INFORMATION PRIVACY ORIENTATION

by

KATHLEEN ERIN GREENAWAY

Volume 1

A thesis submitted to the Department of Management

in conformity with the requirements for the degree

of Doctor of Philosophy

Queen's University

Kingston, Ontario, Canada

December, 2004

Your file Votre référence
ISBN: 0-612-99811-8
Our file Notre référence
ISBN: 0-612-99811-8

ABSTRACT

Information privacy orientation was defined as *the principles, values, decisions rules, policies and desired objectives that organizations adopt to guide them in the collection and use of their customers' personal information* (Greenaway, Cunningham and Chan 2002). I theorized that information privacy orientation is a multidimensional organizational level construct comprising firms' views of their relationships with customers, information management strategy, philosophy with respect to privacy legislation, as well as their actual privacy behaviors.

This exploratory, multiple case study investigated how three Canadian financial institutions implemented their corporate privacy programs in response to the competing pressures of increased technological capacity to exploit customers' personal information, customers' concerns for the privacy of their information, difficult competitive circumstances, and the need to address the requirements of the federal Protection of Information Privacy and Electronic Documents Act (PIPEDA) which came into force in 2001.

There were six research questions that I addressed in this dissertation. I conducted two studies to address these questions. The first study evaluated the privacy policies posted to the websites of ten Canadian financial institutions. The second study involved an intensive, multiple case study of three financial institutions. I interviewed executives and staff, administered a survey, and reviewed privacy related documents. I triangulated this data to assess the different firms' positions on the Information Privacy Orientation Continuum. All six research questions were substantiated.

This research contributes to our understanding of information privacy as an organizational level phenomenon. Specifically, this dissertation explicates the organizational phenomenon of Information Privacy Orientation by extending the Marketing Ethics Continuum (Smith 1995) into the domain of information systems. In addition, it provides several research

instruments developed specifically for IPO investigation. The research also applies two theoretical approaches, the institutional approach and the resource-based view of the firm, to explain similarity and variance in firms' privacy behaviors. In addition, it demonstrates that the IPO Contingency Framework provides a useful device for considering the context for privacy decision-making in firms, which is of relevance to managers and policy-makers. Finally, this research is expected to be useful to managers seeking guidance about the choices they make to protect their customers' information privacy.

ACKNOWLEDGEMENTS

It takes a lifetime to produce a dissertation. Not only does the process feel like it is taking forever, it is in fact the culmination of many processes and the influences of many people that have occurred over the years. Only a few of those years are spent in the actual research activity. This is my modest attempt to do justice to the contributions of the many people who have helped me along the way.

To my parents, Garth and Jean. You instilled in me a respect for education, a love of learning, a belief in the possibility of achieving difficult goals, and the desire to be the best that I could be. Thank you for your love, guidance and fine examples of lives well lived. You support me everyday.

To my sister Carol. A "little" sister could not ask for a better "big" sister. You have been there always. You have shown me how to persevere, how to live and not merely survive, how to come through with panache despite the obstacles. You are a unique individual. I love you and appreciate you always.

To my mother-in-law, Catherine. You have provided me with kindness, love and help whenever I have asked. You cannot imagine how much I appreciated your willingness to drop everything to care for the "grand dogs" so that I could devote myself to whatever turmoil I was wrapped in. You are a strong, able and welcome presence in my life. Thanks for everything.

To my friends who have endured being ignored, having their messages go unanswered for long periods, having plans cancelled or perpetually rescheduled, being subjected to grad student ditherings, blatherings and overall disputatiousness (which masqueraded the insecurity), thank you for hanging in. And especially to Sharon, Tracy and the dearly departed Stephanie. You never questioned my sanity. You always uplifted me (or at least poured me a restorative glass of wine). You have been precious friends in the truest sense. Thank you. You made a difference.

To my professors, colleagues and friends at Queen's School of Business. Thank you for being such a fine collection of human beings. You have earned my gratitude for listening to my tales of woe, for helping me think through what my project was all about, enduring endless rehearsals and rewrites, and for encouraging me in my frequently unorthodox approaches. I am truly privileged to be associated with a group of this calibre. My thanks especially to the MIS area group and the Monsieson/KBE Centre for always being supportive with time, ideas, encouragement and research funds. Thanks to the staff in the PhD Office, especially Teresa Touchette whose ability to stick handle the bureaucratic necessities made my life easier. Special thanks to Linda Freeman for being so kind and helpful over my years at the School and especially in this latter period of high anxiety! And to Anna Dekker as well. You two make me look good. Thank you.

My thanks also to David Lyon and Elia Zuriek, Queen's Department of Sociology, who supported this research through the Globalization of Data Flows project funded by the Social Sciences and Humanities Research Council of Canada.

My committee is a wonderful collection of superb academics who, thankfully, are equally exceptional people. Peggy Cunningham held my hand through difficult times and has been a model of kindness, thoughtfulness and good scholarship. Jane Webster has challenged me to produce really good work and has been willing to endure endless rewrites while I tried to get things right. Her humour, tenacity and exacting standards helped improve this research. Thanks also to Art Cockfield, Queen's Faculty of Law and Mary Culnan, Bentley College, Massachusetts. I could not ask for better, more thoughtful external examiners. Collectively, my committee represented the best possible role models for a newly minted academic. You set a high standard and I can only hope that through my own hard work that I can achieve the same. Thanks for setting me on the right path.

Yolande Chan is a supervisor of extraordinary patience and superb insight. This research has profited from her ability to encourage me to excel, keep me focused on the key issues and yet

provide the freedom to try new approaches. My development as a researcher has been largely due to her efforts to save me from my worst excesses without cramping my sense of adventure! I have learned from her in classes and through collaborations. More importantly, her example of how to live a good life is likely of greatest impact. To my supervisor, mentor and dear friend - my thanks are insufficient payment for a tremendous debt.

To the four companies who provided me with the opportunity to research their privacy initiatives – you made this research possible. I will honour my commitment to respect your desire for anonymity, although that hardly seems fair. You are all fine examples of firms that not only understand that business and the academy may have something to learn from each other, you actually allow the process to happen. Thank you for having the courage of your convictions to allow a scholar-in-training to root around and ask many questions about your firms and your privacy programs. I am grateful for the honesty, openness and patience exhibited by your managers and staff who not only endured the questioning but made helpful comments about the direction the research might take. You know who you are. Thank you.

And to my "family." Macallan and Talisker are my four footed "girls" who have napped under my desk for long hours. You have listened patiently to my lectures as I "thought out loud" and always looked interested. You reminded me to take occasional breaks for walks in the woods to restore my mind to some semblance of balance. Thank you puppies, you are good girls and deserve lots of treats!

Douglas my love – you have always believed in me, even when I doubted. You have always supported me, even when it looked like this process would never end. You have always sustained me, even when my ideas fountain was running dry. Your love, your support, your challenge to me to persevere, and your cheerleading kept me going throughout the classes, exams, papers, comps and now my dissertation. This is not the first graduate degree you have cajoled, pushed, cheered and supported me through (I think we're up to three but who's counting). My completion is as much a testament to your love and patience as it is to my ability to churn out

intelligible prose at midnight. Thank you doesn't begin to address what I feel and what you deserve. Let's start with "I'm back."

And there it is – a lifetime of family and friends, mentors and colleagues, dogs and the best husband you could ask for. That's what it takes to do a dissertation. My name is but a symbol for everyone who has contributed to this effort.

TABLE OF CONTENTS

VOLUME I

Abstract ii
Acknowledgements iv
Table of Contents viii
List of Tables xv
List of Figures xvii

CHAPTER ONE: INTRODUCTION 1
Research Motivation 1
Research Model and Theoretical Base 4
Research Findings and Contribution 6
Dissertation Overview 8

CHAPTER TWO: INFORMATION PRIVACY LITERATURE REVIEW 9
Information Privacy: Consumer Level of Analysis 9
Consumer Attitudes About Privacy 10
Consumer Motivations to Disclose Information 17
Organizational Level Studies 22
Information Privacy as Organizational Liability 23
Information Privacy as An Organizational Decision Outcome 25
Sectoral/National Studies 28
Descriptive Sectoral/National Studies 29
Theory-Based Sectoral/National Studies 33
Chapter Summary 39

CHAPTER THREE: INFORMATION PRIVACY ORIENTATION CONTINGENCY FRAMEWORK 40
Antecedent External Variables 41
National Culture 41
Regulatory Environment 44
Industry Practice 46
Antecedent Internal Variables: Factors that Support the Economic Goals of the Firm 47
Strategic Positioning 47
Market Orientation 49
Availability of Slack Resources 50
Antecedent Internal Variables: Factors that Support Non-Economic Goals of the Firm 52
Organizational Culture 52
Ethical Climate 53
Interfunctional Values 54
Top Management Team Preferences 56
Outcome Variables 58
Social Capital 59
Intellectual Capital 59
Financial Capital 60
Chapter Summary 61

CHAPTER FOUR: FOCAL VARIABLE – INFORMATION PRIVACY ORIENTATION 63
Marketing Ethics Continuum 63
Customer Relationship Stance 66
Buyer Exploitation 67
Buyer Self-Protection 68
Shared Responsibility 68
Consumer Well-Being 69
Customer Information Management Strategy 69
Reduce Costs 72
Minimize Risks 73
Add Value 74
Create New Reality 75
Customer Information Privacy Philosophy 76
Privacy Ignored 77
Privacy as Constraint 78
Privacy as an Exchange 78
Privacy as Opportunity 79
Customer Information Privacy Behaviors 81
Non-Compliance 82
Minimal Compliance 83
Adhering to Codes of Conduct 84
Significantly Enhanced Privacy Offerings 85
Chapter Summary 87

CHAPTER FIVE: COMPETING THEORIES TO EXPLAIN SIMILARITIES AND DIFFERENCES IN INFORMATION PRIVACY ORIENTATION 89
Explaining Similarities: The Institutional Approach (IA) 89
Organizational Goals 90
Sources of Pressure 91
Ability to Respond to Pressure 92
Response Strategies 92
Institutional Approach and Information Privacy Orientation 97
IPO and Organizational Goals 97
IPO and Source of Institutional Pressure 98
IPO and Ability and Willingness to Respond to Pressure 99
IPO and Responses to Pressures 100
Explaining Differences: The Resource-Based View of the Firm (RBV) 101
Resources, Process and Capabilities 102
Resource-Based View and Information Privacy Orientation 108
IPO and Organizational Goals 109
IPO and Resources 110
IPO and Processes 111
IPO and Capabilities 111
Using Competing Theories to Explain Information Privacy Orientation 112
Chapter Summary 114

CHAPTER SIX: RESEARCH METHODOLOGY 115
Ontology, Epistemology and Research Domain 115
Research Methodology Overview 116
Phase One: Privacy Policy Evaluation Study 118
Study Purpose 118

Sample 119
Data Collection 119
Data Analysis 120
Phase Two: Instrument Development and Validation 121
Interview Guides 121
Survey Instrument 122
Pre-Testing the IPO Survey Instrument: IPO Continuum 124
Pre-Testing the IPO Survey Instrument: IPO Typology 125
Pre-Testing the IPO Survey Instrument: Demographic Data 126
IPO Survey On-Line Version 126
Phase Three: Field Research 128
Purpose 128
Recruiting the Research Sites 129
Data Collection 131
Data Analysis 136
Phase Four: Cross-Case Analysis 138
Chapter Summary 139

CHAPTER SEVEN: PHASE ONE – PRIVACY POLICY EVALUATION STUDY 141
Study Purpose 141
Sample 141
Data Collection 143
Data Analysis 144
Detailed Findings 148
Overview 148
Applying the IPO Definition 153
Applying the IPO Continuum 159
Initial Selection of Research Sites 164
Limitations 165
Chapter Summary 166

CHAPTER EIGHT: PILOT STUDY (CASE A) 167
Privacy Program Status: "Managing the Immediate Exposure" 167
First Responses 168
Present Activity 169
Looking Ahead 169
Pilot Study 171
Goal One: Testing Interview Questionnaires' Efficacy 171
Efficacy of Interview Guides 172
Improvements in Process 172
Regional and Branch Versions 173
Recognizing Organizational Idiosyncrasy 173
Goal Two: Validating the IPO Survey Instrument 173
Goal Three: Identifying Key Privacy Documents 174
Goal Four: Expanding My Learning 174
Lessons About Conducting Research 175
Lessons About Privacy as Organizational Activity 179
Goal Five: Assessing Case A's IPO 183
Assessing the Information Privacy Policy 183
Applying the IPO Definition 186
Principles (External) 186

Principles (Internal) 186
Values 188
Policies 189
Objectives 189
Decision Rules 192
Case A's Position on the IPO Continuum 193
Survey Results 193
Customer Relationship Stance (CRS) 196
Customer Information Management Strategy (IMS) 197
Customer Information Privacy Philosophy (PHIL) 199
Customer Information Privacy Behaviors (BHV) 200
Section Summary 202
Theoretical Assessment 204
Institutional Approach 204
Resource-Based View 205
Chapter Summary 206

CHAPTER NINE: CASE B 207
Case B Privacy Program Status: "The Privacy Project is Completed" 208
Privacy Program Context 208
Implementing the Privacy Project 211
Assessing Case B's Privacy Policy 213
Applying the IPO Definition to Case B 216
Principles 216
Values 218
Policies 219
Objectives 220
Decision Rules 223
Case B's Position on the IPO Continuum 225
Survey Results 225
Customer Relationship Stance (CRS) 227
Customer Information Management Strategy (IMS) 229
Customer Information Privacy Philosophy (PHIL) 231
Customer Information Privacy Behaviors (BHV) 233
Repositioning Case B on the IPO Continuum 235
Theoretical Assessment 235
Institutional Approach 235
Resource-Based View 238
Chapter Summary 238

CHAPTER TEN: CASE C 239
Case C Privacy Program Status: "We're compliant – now what?" 240
Initial Privacy Program Implementation 240
Next Steps 242
Assessing Case C's Privacy Policy 246
Applying the IPO Definition to Case C 248
Principles 248
Values 251
Policies 251
Objectives 253
Decision Rules 256

Case C's Position on the IPO Continuum 257
Customer Relationship Stance (CRS) 257
Customer Information Management Strategy (IMS) 259
Customer Information Privacy Philosophy (PHIL) 260
Customer Information Privacy Behaviors (BHV) 262
Theoretical Assessment 263
Institutional Approach 263
Resource-Based View 266
Chapter Summary 267

CHAPTER ELEVEN: CASE D 268
Case D Privacy Program Status: "Let's talk about information management" 269
Privacy as an Information Management Enabler 270
Assessing Case D's Privacy Policy 272
Applying the IPO Definition to Case D 275
Principles 277
Values 277
Policies 277
Objectives 279
Decision Rules 280
Case D's Position on the IPO Continuum 281
Survey Results 282
Customer Relationship Stance (CRS) 293
Customer Information Management Strategy (IMS) 284
Customer Information Privacy Philosophy (PHIL) 286
Customer Information Privacy Behaviors (BHV) 288
Repositioning Case D on the IPO Continuum 289
Theoretical Assessment 291
Institutional Approach 291
Resource-Based View 293
Chapter Summary 294

CHAPTER TWELVE: CROSS-CASE ANALYSIS 296
Placing the Case Studies on the IPO Continuum 297
Customer Relationship Stance (CRS) 298
Customer Information Privacy Philosophy (PHIL) 298
Customer Information Privacy Behavior (BHV) 299
Customer Information Management Strategy (IMS) 300
Institutional Theory and IPO: Explaining Similarities 301
Organizational Goal 302
Source of Pressure 303
Ability and Willingness to Respond to Pressure 306
Response to Pressure 308
Section Summary 310
The Resource-Based View and IPO: Explaining Differences 311
Organizational Goal 312
Resource 314
Process 315
Capability 315
Section Summary 315
Chapter Summary 316

CHAPTER THIRTEEN: CONCLUSIONS 317
Dissertation Findings by Research Question 317
R1: Do Firms Have an Information Privacy Orientation? 317
R2: Is Information Privacy Orientation Constructed as I Have Theorized? 322
R3: Does the Institutional Approach Explain IPO Homogeneity? 327
R4: Does the Resource-Based View Explain IPO Heterogeneity? 329
R5: What is the Effect of the Firm's Context on Its IPO? 331
R6: What is the Effect of IPO on Firm Performance? 334
Section Summary 335
Implications 335
Implications for Researchers 335
Implications for Managers 339
Section Summary 341
Limitations 341
"Positivist" Case Study Assessment 342
"Interpretivist" Case Study Assessment 344
Contributions 345
Chapter Summary 347
Concluding Thoughts 347

REFERENCES 349

VOLUME II
Appendix A: Consumer Level Studies Summary 373
Appendix B: Organizational Level Studies Summary 381
Appendix C: Sectoral/National Studies Summary 385
Appendix D: Background to Information Privacy Principles 391
Appendix E: Differences Between Chartered Banks and Credit Unions 393
Appendix F: Canadian Domestic Banks 395
Appendix G: Top 20 Canadian Credit Unions 397
Appendix H: Research Methods – Validating and Adapting Instruments 400
Appendix H-1: Data Collection Strategy: Interviews (Initial Version) 401
Appendix H-2: Data Collection Strategy (Revised) – Basic Interview for All Participants 405
Appendix H-3: Summary of IPO Guide and IPO Survey Instrument Validation Pre-Test Participants 410
Appendix H-4: IPO Interview Guides: General Content Improvements from Pre-Test 412
Appendix H-5: IPO Interview Guides: Specific Guide Content Improvements from Pre-Test 414
Appendix H-6: IPO Interview Guide: Construction Issues from Pre-Test 417
Appendix H-7: Questionnaire Revisions and Improvements During and After Research Visit (Based on Case A Experience) 418
Appendix H-8: IPO Interview Guides (Examples of Questions) 421
Appendix H-8.1 Basic 421
Appendix H-8.2 Privacy Professionals 425
Appendix H-8.3 IT/Information Management/Information Security Functions 427
Appendix H-9: Draft Initial IPO Survey Instrument for Information Privacy Orientation 428
Appendix H-10: IPO Survey Instrument Construction – Card Sort Description and

Results 433
Appendix H-11: Questionnaire Item Sorting Instructions 446
Appendix H-12: IPO Survey Instrument – Content Improvements from Pre-Test 452
Appendix H-13: Final Version of IPO Survey – Procedure (Paper-and-Pencil Survey) 453
Appendix H-14: Final Version of IPO Survey Instrument 454
Appendix H-15: IPO Survey Instrument – Web-Based Version 467
Appendix I: Research Sites Recruitment 475
Appendix I-1: Request for Participation 476
Appendix I-2: Invitation Letter 479
Appendix I-3: Research Project Summary 480
Appendix I-4: Research Site Requirements 482
Appendix I-5: Confidentiality & Non-Disclosure Agreement 484
Appendix J: Phase One Privacy Policy Evaluation Study – Detailed Findings 491
Appendix J-1: Phase One Privacy Policies Evaluation Study - Evaluation Form 492
Appendix J-1.1 Firm 1 501
Appendix J-1.2 Firm 2 505
Appendix J-1.3 Firm 3 509
Appendix J-1.4 Firm 4 513
Appendix J-1.5 Firm 5 517
Appendix J-1.6 Firm 6 522
Appendix J-1.7 Firm 7 526
Appendix J-1.8 Firm 8 530
Appendix J-1.9 Firm 9 534
Appendix J-1.10 Firm 10 538
Appendix K: Case A (Pilot Study) - Supplementary Information from Case Study Database 542
Appendix K-1: Case A - Research Setting and Site Visit 543
Appendix K-2: Case A – Case A - Interviews 544
Appendix K-3: Case A - Distribution of Completed Surveys 544
Appendix K-4: Case A - Survey Respondent Characteristics 545
Appendix K-5: Case A - Desirable Privacy Documents 546
Appendix K-6: Case A - Frequencies and Means from IPO Survey 547
Appendix L: Case B - Supplementary Information from Case Study Database 551
Appendix L-1: Case B - Research Setting and Site Visit 552
Appendix L-2: Case B - Interviews 556
Appendix L-3: Case B - Distribution of Completed Surveys 556
Appendix L-4: Case B - Survey Respondent Characteristics 557
Appendix L-5: Case B - Privacy Documents 558
Appendix L-6: Case B - Frequencies and Means from IPO Survey 560
Appendix M: Case C - Supplementary Information from Case Study Database 564
Appendix M-1: Case C - Research Setting and Site Visit 565
Appendix M-2: Case C - Interviews 568
Appendix M-3: Case C - Documents 569
Appendix N: Case D - Supplementary Information from Case Study Database 573
Appendix N-1: Case D - Research Setting and Site Visit 574
Appendix N-2: Case D - Interviews 577
Appendix N-3: Case D - Survey Respondent Characteristics 578
Appendix N-4: Case D - Privacy Documents 579
Appendix N-5: Case D - Frequencies and Means from IPO Survey 580

LIST OF TABLES

Volume I
Table 1-1: Summary of Dissertation Findings by Research Question 7

Table 5-1: Institutional Approach and Information Privacy Orientation 98
Table 5-2: A Hierarchy of Corporate Resources 105
Table 5-3: Resource-Based View and Information Privacy Orientation 109
Table 5-4: Competing Theories Summary 113

Table 6-1: Summary of Research Program 117
Table 6-2: Site Visit Schedules 131
Table 6-3: Summary of Data Collection Methods 132
Table 6-4: Summary of Interviews Conducted 133
Table 6-5: Summary of Documents Collected 134
Table 6-6: Summary of IPO Survey Activities by Main Case Site 135
Table 6-7: Summary of Analytical Techniques by Data Collection Method 136

Table 7-1: Selected Canadian Financial Institutions (Alphabetical Order) and Their URLs 142
Table 7-2: Initial Assessment Criteria 146
Table 7-3: IPO Definition Components 147
Table 7-4: Summary of Privacy Policy Comprehensiveness 149
Table 7-5: Summary of Privacy Policy Readability 151
Table 7-6: Summary of Privacy Policy Accessibility 154
Table 7-7: Summary of Comprehensiveness, Readability and Accessibility Scores 155
Table 7-8: Phase One Study – Summary Chart for IPO Definition 156
Table 7-9: Phase One Study – Summary of IPO Definition Scores 160
Table 7-10: Phase One Study – Summary of IPO Continuum Scores 163
Table 7-11: Final Ranking of Potential Research Sites 164
Table 7-12: Research Site Preferences 165

Table 8-1: Case A - Privacy Notice Basic Assessment 184
Table 8-2: Case A - IPO Definition 187
Table 8-3: Case A - IPO Survey Findings 193

Table 9-1: Case B - Privacy Notice Basic Assessment 214
Table 9-2: Case B - IPO Definition 217
Table 9-3: Case B - IPO Survey Findings 226

Table 10-1: Case C - PIPEDA Project Phases 241
Table 10-2: Case C - Classification of Compliance Distinctions of PIPEDA Principles 243
Table 10-3: Case C - Privacy Notice Basic Assessment 247
Table 10-4: Case C - IPO Definition 249
Table 10-5: Case C - IPO Evidence 257

Table 11-1: Case D - Privacy Notice Basic Assessment 273
Table 11-2: Case D - IPO Definition 275
Table 11-3: Case D - IPO Survey Findings 282

Table 12-1: Institutional Approach and IPO 301
Table 12-2: Summary of Evidence for Organizational Goal (IA) 303
Table 12-3: Summary of Evidence for Source of Pressure (IA) 304
Table 12-4: Summary of Evidence for Ability and Willingness to Respond to Pressure (IA) 306
Table 12-5: Summary of Evidence for Responses to Pressure (IA) 309
Table 12-6: Summary of Cross Case Analysis – IPO and the Institutional Approach 310
Table 12-7: Resource-Based View and IPO 312

Table 13-1: Summary of Dissertation Findings and Future Research Opportunities by Research Question 318
Table 13-2: Sub-Construct Definitions (Revised) 326
Table 13-3: Two Approaches to Evaluating Case Studies 342

LIST OF FIGURES

VOLUME I

Figure 1-1: Information Privacy Orientation Continuum (IPOC)(Basic Model) 4

Figure 3-1: Information Privacy Orientation Contingency Framework (IPOCFW) 41

Figure 4-1: Marketing Ethics Continuum 65
Figure 4-2: Information Privacy Orientation Continuum (Overview) 66
Figure 4-3: Customer Relationship Stance 67
Figure 4-4: Strategic Information Alignment (SIA) Framework 71
Figure 4-5: Customer Information Management Strategy 71
Figure 4-6: Customer Information Privacy Philosophy 77
Figure 4-7: Royal Bank Financial Group – Privacy as Business Strategy 80
Figure 4-8: Customer Information Privacy Behaviors 82
Figure 4-9: Information Privacy Orientation Continuum (Detailed) 88

Figure 7-1: Phase One Study – Summary Placement of Ten Financial Institutions on IPO Continuum 161
Figure 7-2: Phase One Study – Summary of Firms' Relative Positioning on IPO Continuum 165

Figure 8-1: Case A's Initial Placement on the IPO Continuum (Based on IPO Survey Results) 194
Figure 8-2: Case A's Final Placement on the IPO Continuum (Based on Triangulated Results) 203

Figure 9-1: Case B's Initial Placement on the IPO Continuum (Based on IPO Survey Results) 227
Figure 9-2: Case B's Final Placement on the IPO Continuum (Based on Triangulated Results) 236

Figure 10-1: Case C's Placement on the IPO Continuum (Based on Interviews and Documents Results) 264

Figure 11-1: Case D's Initial Placement on the IPO Continuum (Based on IPO Survey Results) 283
Figure 11-2: Case D's Final Placement on the IPO Continuum (Based on Triangulated Results) 290

Figure 12-1: Cross Case Analysis – IPO Continuum 297
Figure 12-2: Information Initiative 313

Figure 13-1: Privacy Stages Across the Cases 321
Figure 13-2: Competing IPO Models (1) 323
Figure 13-3: Competing IPO Models (2) 324
Figure 13-4: Complementary Theories to Explain IPO 331

CHAPTER ONE

INTRODUCTION

> *"Anyone who today thinks the privacy issue has peaked is greatly mistaken ... We are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope."*
> (Forrester Research 2001)[1]

This dissertation investigates how firms construct their privacy regimes to balance their profit motivations (which lead them to gather and use customer information in ever increasingly intrusive manners) with their customers' legitimate concerns about the collection, use and, potentially, misuse of their personal information.[2] More specifically, my research examines different firms' *information privacy orientation* (IPO). I define *information privacy orientation* as:

> *The principles, values, decisions rules, policies and desired objectives that organizations adopt to guide them in the collection and use of their customers' personal information* (Greenaway, Cunningham and Chan 2002).

I theorized that IPO is a complex organizational phenomenon comprising firms' views of their relationships with customers, information management strategy, philosophy with respect to privacy legislation, as well as their actual privacy behaviors.

There are four sections to this chapter. First, I explain my research motivation. Next, I introduce the formal model for information privacy orientation, the associated research questions, and the theory underpinning the research. Then I discuss the contributions made by the dissertation and, finally, I provide an overview of the contents of this dissertation document.

Research Motivation

Information privacy, "the ability of the individual to personally control information about oneself" (Stone Gardner, Gueutal & McClure 1983; Westin 1967) is a pivotal social, strategic, legal and ethical issue (Bloom, Milne, and Adler 1994; Cavoukian and Hamilton 2003; Culnan

[1] As quoted in Cavoukian and Hamilton (2002:91).
[2] Employee privacy is an equally important phenomenon but is beyond the scope of this research.

and Armstrong 1999; Milberg, Smith and Burke 2000; Milne 2000; Nakra 2001). This is particularly true for businesses competing in consumer-based industries, such as pharmacies and retail banks, that have access to especially "sensitive" customer information (Cespedes and Smith 1993; Sheehan and Hoy 2000). The exponential growth in the ability of firms to gather, store, merge and process personal information, from a vast array of data collection modes (Culnan and Armstrong 1999) has increased consumers' concerns about privacy (Bordoloi, Mykytyn and Mykytyn 1996; Caudill and Murphy 2000; Smith 1993). Even as consumers desire personalized products and tailor-made services, they are concerned about the information gathering practices that enable such customization (Phelps, Nowak and Ferrell 2000; Sheehan and Hoy 2000). The shift to mobile commerce is expected to exacerbate these privacy challenges (Cavoukian and Hamilton, 2002; Keen and Mackintosh 2001).

There have been numerous studies that examine customers' information privacy attitudes (Culnan 1993; Culnan and Armstrong 1999; Tam, Hui and Tan 2002) and concerns (Hine and Eve 1998; Smith Milberg and Burke 1996; Stewart and Segars 2002). There have also been several sectoral and national studies of privacy policies posted on corporate web sites (i.e., Culnan 1999a, 1999b; FTC 1998, 2000; Geist and Van Loon 2000; Leizerov 2001; Ryker Lafleur, McManis and Cox 2002). Culnan and Bies (1999) propose that consumers invoke a "privacy calculus" to weigh the potential risks and benefits of providing personal information in exchange for economic or social gains. At the same time, Dhillon, Bardacino and Hackey (2002) argue that individuals make "value focused" privacy-based assessments about the firms with which they do business.

Organizations must likewise make decisions about the use of personal information whether as a means to reduce operating costs (Laudon 1996), to respond to evolving social norms (Smith 1989,1993), or to comply with domestic or foreign regulation (Milne 2000). The ability to gather and use information effectively to learn about new and existing customers as well as to leverage this knowledge to change the competitive dynamics of an industry may be an

organization's only sustainable competitive advantage (Day 2001) or key strategic asset (Deshpandé 2001). Gathering relevant, accurate and useful information is getting more difficult given customers' concerns for privacy invasions and misuse of personal information (Hoffman, Novak and Peralta 1999; Phelps, Nowak, and Ferrell 2000.) Firms are increasingly seeking ways to allay these information privacy concerns so that they may reap the benefits of their investments in sophisticated information systems.

Further exacerbating an already challenging environment is the emerging international consensus over what constitutes appropriate privacy practices (Geist 2002) including the broad regulation of information practices of commercial enterprises in many jurisdictions, including Canada. However, with few exceptions (i.e., Bordoloi et al. 1996; Ives and Jarvenpaa 1991; Smith 1989, 1993), there has been limited empirical work examining organizational responses to the customer information privacy challenge (Greenaway, Cunningham and Chan 2003; Milne 2000). In other words, there is as yet no organizational level equivalent "privacy calculus."

At the same time, there is little theory to guide us in understanding organizational information privacy behavior. Ethical theory applied to information privacy has dominated both the IS (i.e., Laudon 1995; Mason 1986; Smith 1993; Smith and Hasnas 1996) and marketing (Caudill and Murphy 2000; Charters 2002; Foxman and Kilcoyne 1993; Hoffman, Novak and Peralta 1999) literatures. However, these theories have largely been used to examine information privacy from the customer perspective and then relate these to organizational actions. Rarely has there been a systematic consideration of both the content and context of firms' specific information privacy policies and behaviors. Further, even where studies have discerned significant similarities and differences in information privacy behaviors among firms within the same sector (such as is offered by the website privacy policy surveys), seldom has any theory been offered to explain the variance. Lastly, few instruments have been created to assist with documenting and analyzing the complexities of information privacy orientation.

It is these several gaps in our understanding that I address through my dissertation research. Hence, the overarching question driving this research has been:

How can we understand the different choices organizations make in the treatment of customer information privacy?

Research Model and Theoretical Base

As will be explained more fully in Chapter Four, I modelled Information Privacy Orientation as a four-tiered continuum. I theorized IPO and developed this model as a first effort to respond to the overarching question identified above. The basic model is shown in Figure 1-1. The first set of research questions investigated in this dissertation were concerned with the construct IPO and its sub-constructs as represented by the IPO Continuum. These questions were:

R1: Do firms have an Information Privacy Orientation?

R2: Is Information Privacy Orientation constructed as I have theorized?

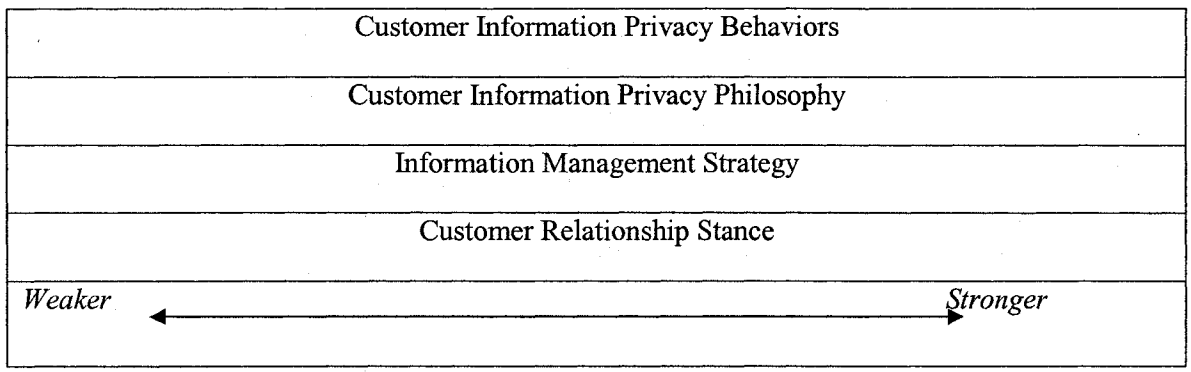


Figure 1-1: Information Privacy Orientation Continuum (IPOC) (Basic Model)

The second set of research questions were concerned with explaining the differences in Information Privacy Orientation among firms in the same industry. As is explained in detail in Chapter Five, I employed the contrasting theories of the Institutional Approach (IA) and the Resource-Based View (RBV) of the firm to explore similarities and differences in IPO among firms. The IA is a paradigm that explains organizational behavior as a function of social pressures to conform in order to ensure firm survival (Scott 2001). Therefore, the IA can be applied to IPO as a way to explain homogeneous orientations across firms. In contrast, the RBV is a paradigm

that seeks to identify the sources for sustainable competitive advantage within firms (Barney 1991). Therefore, the RBV is concerned with explanations of heterogeneous IPO. Hence, the second set of research questions was:

R3: To what extent does the Institutional Approach help us to explain homogeneity in information privacy orientation across firms in the same industry?

R4: To what extent does the Resource-Based View help us to explain heterogeneity in information privacy orientation across firms in the same industry?

I addressed these questions through two studies. The first study evaluated the privacy policies posted to the websites of ten Canadian financial institutions. I documented and analyzed these firms' publicly announced privacy policies and practices. From this sample of 10 banks and credit unions, I selected cases representing the greatest variance in observed privacy policies and behaviors. I successfully recruited three financial institutions to participate in my main study. This second study entailed the intensive analysis of these firms' Information Privacy Orientations by examining and triangulating interview, survey and documentary data.

To truly understand information privacy orientation operating at the organizational level, I determined the need to gain some insight into the different contexts in which firms operate and make decisions. I developed an Information Privacy Orientation Contingency Framework as a way to organize the contextual variables that I have identified as being the most salient as antecedents and outcomes of IPO. I explain this contingency framework in Chapter Three. While the framework was not the focal point of my dissertation research, I gathered contextual information during the course of my fieldwork. As a consequence, I used the following additional questions to guide my research activities in this area:

R5: What is the effect of the firm's overall context (external and internal environment) on its Information Privacy Orientation?
R6: What is the effect of IPO on firm performance?

Given the broad scope of this research, the question became how to understand the contribution of the various components? Pettigrew (1987:657-8) offered an analytical framework comprising context, content and process as a vehicle for studying organizational change. Context

(the what question) includes the "outer" (social, political, economic, competitive) and "inner" (structure, culture, political context) environments. Content (the why question) means the specific aspects of change that are the object of investigation. Process (the how question) refers to the "actions, reactions and interactions" among the corporate players involved with marshalling the change effort. To the extent that implementing information privacy policies and practices represents a more or less deliberate organizational change process, I believe that my dissertation research addresses Pettigrew's questions in the following ways. The Information Privacy Orientation Continuum responds to the "content" question while the "context" and "process" questions are addressed by my Information Privacy Orientation Contingency Framework.

Research Findings and Contribution

As noted above, I addressed six research questions in this exploration of information privacy orientation. I was able to demonstrate support for all six questions as identified in Table 1-1. (See Chapter Thirteen for a detailed discussion of these findings.)

This research contributes to our understanding of information privacy as an organizational level phenomenon, an under researched area in this domain. More specifically, this dissertation explicates the organizational phenomenon of Information Privacy Orientation by extending the Marketing Ethics Continuum (Smith 1995) into information privacy, information systems, and marketing research. In addition, it provides several research instruments developed specifically for IPO investigation. The research also affords insight into the reasons for similarity and variance in firms' privacy behaviors through the application of two theoretical approaches, the institutional approach and the resource-based view of the firm, that are underutilized in MIS research. In addition, I demonstrate that the IPO Contingency Framework provides a useful device for considering the context for privacy decision-making in firms. Finally, this research is expected to be useful to managers seeking guidance about the choices they make in their privacy

regimes as well as public policy makers interested in understanding how Canada's innovative model for privacy legislation has been implemented in different firms.

Table 1-1: Summary of Dissertation Findings by Research Question

Research Question	Finding
R1: Do firms have an Information Privacy Orientation?	• Demonstrated. • Phase One – Privacy Policy Evaluation Study: ten firms displayed different approaches to customer information privacy. • Phase Three – Field Research (Case Studies): four firms displayed variance in "principles, values, decisions rules, policies and desired objectives."
R2: Is Information Privacy Orientation constructed as I have theorized?	• Partly demonstrated. • Evidence of customer relationship stance, information management strategy, privacy philosophy, privacy behaviors.
R3: To what extent does the Institutional Approach help us to explain homogeneity in information privacy orientation across firms in the same industry?	• Demonstrated. • The Institutional Approach (organizational goals, sources of pressure, ability and willingness to respond to pressure, and response strategies) can be applied to explain IPO in firms within the same industry.
R4: To what extent does the Resource-Based View help us to explain heterogeneity in information privacy orientation across firms in the same industry?	• Partly demonstrated. • Case D presented evidence to suggest that RBV might be useful to explain differences in IPO in firms in the same industry.
R5: What is the effect of the firm's overall context (external and internal environment) on its Information Privacy Orientation?	• Not specifically tested in the thesis research. • Data emerged to support a relationship between antecedent variables and IPO.
R6: What is the effect of IPO on firm performance?	• Not specifically tested in the thesis research. • Data emerged to support a relationship between IPO and outcomes.

Dissertation Overview

This dissertation is organized as follows. Chapters Two, Three and Four collectively move from a general to a specific consideration of information privacy as an organizational phenomenon. Chapter Two examines key information privacy literature by level of analysis – customer, organization, and national/sectoral – and identifies some of the gaps in our understanding. Chapter Three provides an approach to addressing the organizational level gaps by providing the Information Privacy Orientation Contingency Framework. Chapter Four provides further focus through a detailed explanation of the Information Privacy Orientation Continuum by anchoring it within the literature, and defining the individual continuum layers. Chapters Five and Six address the theories and methods that underpinned the research into the IPO construct. Chapter Five explores the application of contrasting theory bases as potential explanations for similarity and differences among different firms' IPO. Chapter Six describes the research methods and analytical approaches I employed. Chapters Seven through Eleven inclusively describe the studies I conducted to answer the research questions. Chapter Seven reports on the Privacy Policy Evaluation Study. Chapter Eight (Case A) describes the pilot case study (through which I tested my research instruments). Chapters Nine, Ten and Eleven report the findings of the within-case analyses from the three separate cases, B,C and D repectively. Chapters Twelve and Thirteen conclude the dissertation. Chapter Twelve reports the outcomes of the cross-case analysis of findings. Chapter Thirteen discusses the findings and future research opportunities arising from this research, describes the limitations, and outlines the contributions of this dissertation.

CHAPTER TWO

INFORMATION PRIVACY LITERATURE REVIEW

Information Privacy has been investigated by researchers within the traditions of information systems (i.e., Chan 2003; Dinev and Hart 2003; George 1996; Ives and Jarvenpaa 1991; Smith 1993; Smith, Milberg and Burke 1996; Stewart and Segars 2002; Webster 1998), marketing (i.e., Culnan 1993; Phelps, Nowak and Ferrell 2000; Greenaway, Cunningham and Chan 2002), organizational behavior (i.e., Culnan and Armstrong 1999; Milberg et al 1995; Milberg et al 2000; Stone et al 1990) and ethics/social responsibility (i.e., Caudill and Murphy 2000; Dhillon, Bardacino and Hackney 2002; Gattiker and Kelley 1999; Mason 1986; Smith and Hasnas 1996). However, a discipline based approach is not a particularly useful manner in which to organize the literature mainly because the issue of consumer information privacy cuts across functions in firms and, therefore, requires a more holistic or integrated treatment.

The approach I take in this chapter is to examine information privacy as a business issue (Cavoukian and Hamilton 2003) that has three useful levels of analysis – customer, organizational and sectoral/national. I will review samples from the empirical literature within each of these categories and demonstrate where it supports my research and where significant gaps exist. Note that in the succeeding chapter of this dissertation, I offer a contingency framework for considering both the environmental pressures that appear to inform an organization's privacy regime as well as its likely outcomes. Reference to both this contingency framework and the focal variable, Information Privacy Orientation (explained in Chapter Four), is made throughout this literature review.

Information Privacy: Consumer Level of Analysis

The empirical research into consumers information privacy has been conducted largely by marketing and IS researchers. A main focus of this research has been the investigation of consumer attitudes about privacy (i.e., Culnan 1993; Culnan and Armstrong 1999; Tam, Hui and

Tan 2002) in including their concern for privacy risk through disclosure of personal information (Milne and Culnan 2004; Miyazaki and Fernandez 2000); about privacy violating behaviors by organizations (i.e., Hine and Eve 1998; Smith, Milberg and Burke 1996; Stewart and Segars 2002); and the tradeoffs consumers are prepared to make to receive benefits from providing personal information to companies (i.e., Dinev and Hart 2003; Hann, Hui, Lee and Png 2002; Phelps, Nowak and Ferrell 2000; Sheehan and Hoy 2000). Consistent across these studies is the question of what firms ought to do to increase customer comfort with providing personal information. Increasingly, these studies are concerned with customer information privacy within the online environment (i.e., Dinevand Hart 2003; Hann et al 2002; Tam et al 2002), although a substantial body of work considers privacy in the offline world (Culnan 1993; Culnan and Armstrong 1999, Smith et al 1996; Hine and Eve 1998, Phelps et al 2000). The selection of research setting (i.e. offline or online) is largely the result of the time of data collection (pre or post introduction of publicly accessible Internet).

In this chapter, I review two groups of consumer level studies in order to provide an examination of what we have learned about customers and information privacy and how these findings may inform organizational action. The first group of studies is concerned with consumer attitudes to information privacy while the second addresses consumer motivations to share information. Note that details about the individual studies are contained in Appendix A: Consumer Level Studies Summary.

Consumer Attitudes About Privacy

Two studies by Culnan (Culnan 1993; Culnan and Armstrong 1999) address the important role of control in shaping consumer attitudes about information sharing. The first study (Culnan 1993) was a pre-Internet examination of the role of perceived control in shoppers'

attitudes to secondary information use[1]. The study looked at how *individual concerns for privacy*, *attitudes toward direct marketing*, and *previous negative experience* affected customers' *sensitivity to secondary information use.*[2] The study found that respondents who did not equate privacy with a loss of control, who viewed shopping by mail as beneficial, and saw themselves as possessing the ability to cope with unwanted mail had a more positive attitude (or less sensitive attitude) towards secondary information use. Clearly, perceptions of control were fundamental to shoppers' attitudes to secondary use of personal information.

The second study (Culnan and Armstrong 1999) assessed the degree to which customers would or would not provide personal information under the conditions that they were or were not explicitly advised that FIP would be used. In a secondary analysis of public opinion survey data, the researchers found that when people were *advised explicitly that F.I.P* would be used, only *prior experience* distinguished individuals who were willing to be profiled from those who were unwilling. When respondents were *not told explicitly* that fair information principles would be observed, both *privacy concerns* and *prior experience* distinguished between those willing and unwilling to be profiled.

Culnan (1993) used Categorization Theory - (Dutton and Jackson 1987) – does the customer view secondary use as a threat or opportunity - to explain the differences in response. This theory argues that individuals characterize issues as gain-loss, positive-negative and controllable-uncontrollable (357). Culnan and Armstrong (1999) applied Procedural Fairness theory (Lind and Tyler 1989) – does the customer perceive how they are being treated as fair – to explain why customers would or would not share information. Both studies address perceptions of control but the two theory bases offer different avenues for ongoing investigation and as such support my research from different perspectives.

---

[1] "Secondary information use" is one of several practices that are collectively referred to as "fair information principles or practices" (FIP). See Appendix D for information about FIP.
[2] Note that italicized words or phrases indicate a specific variable or key theme used in a study (unless otherwise indicated).

First, the assertion of the importance of control in consumers' perceptions of privacy issues supports my contention that a distinguishing characteristic among firms with stronger information privacy orientations is their willingness to share or cede control to customers (i.e. they differ in privacy behaviors[3]). Second, both theory bases are useful. Categorization theory comes from the strategic management literature and helps us to understand how managers perceive and act on critical issues. This theory is useful in addressing top management team privacy preferences[4] and the development of a firm's privacy philosophy.[5] Procedural fairness (based on organizational justice theory) is grounded in the organizational behavior literature and has been applied primarily to employee research. However, its innovative use with customers helps us to think about the balance that firms may be attempting to strike between their interests and those of their customers[6] that I assert express themselves in the customer relationship stance[7]. Both theories are useful in considering how an organization might construct and evaluate its privacy policies from the perspective of the goals it wants to achieve. In other words, what is the alignment between a firm's desire to achieve certain goals through its privacy activities and the likelihood that these goals will be interpreted by customers in the manner intended? Third, both studies demonstrate that customers are able to make decisions about the cost-benefit of providing versus withholding personal information, and that they will default to apposition of unwillingness to share if their concerns for control are not addressed. This supports my contention that organizational approaches to information privacy are recognized and acted upon by customers and therefore need to be deliberately considered in the development of a firm's information privacy regime.

---

[3] Variation in privacy behaviors appears as the fourth layer of the Information Privacy Orientation continuum. See Chapter Four.
[4] Top management preferences appear as an internal environment antecedent variable in the Information Privacy Orientation contingency framework. See Chapter Three.
[5] Privacy Philosophy appears as the third layer of the Information Privacy Orientation continuum. See Chapter Four.
[6] Economic versus non-economic goals frame the internal environment antecedent variables in the contingency framework. See Chapter Four.
[7] Customer Relationship Stance appears as the foundational tier of the Information Privacy Orientation continuum. See Chapter Three.

Smith, Milberg and Burke (1996) developed and validated an instrument to measure the primary dimensions of individuals' concerns about organizational privacy practices. The authors successfully challenged the prevailing wisdom that information privacy was a unidimensional construct (either I am or am not concerned for privacy). They demonstrated that the construct *concern for privacy* is multidimensional comprising four central dimensions (190) – *collection*, *errors*, *unauthorized secondary use*, and *improper access*.

Stewart and Segars (2002) further refined and tested the CFIP instrument. They theorized that "CFIP represents a cognitive state (or perception) [by consumers] about *corporate practice and control* of that practice (38) (my emphasis). Stewart and Segars argued that despite offering a welcome multidimensional view of consumer information privacy, the CFIP construct was misspecified when modeled as a first order factor model. Their study demonstrated that CFIP was more correctly modeled as a second order factor model. The improved model comprises the four distinct factors derived by Smith et al as well as "the structure of the interrelationships among those factors" (39). They demonstrated that the paths connecting the second order factor CFIP to the four first order dimensions were significant and provided a more parsimonious explanation.

These studies are important for three reasons. First, they help to build a cumulative tradition within the information privacy research stream. Second, they provide a validated CFIP instrument that helps both researchers and practitioners to understand the complexity of consumers' concerns for their privacy. Of most interest for my research is the researchers' point that while the CFIP instrument provides useful guidance about consumer attitudes towards the use by firms of personal information, it points to the lack of understanding that we have about firms' attitudes to privacy. Indeed, the Stewart and Segars (2002:46) specifically admonish that the "use of CFIP as a metric of corporate practice or managers attitudes towards information use may be inappropriate."

Sheehan and Hoy (2000) agreed with the findings of previous research that demonstrated that consumers' privacy concerns are multidimensional but argued that framing these dimensions

simply in terms of the FIP was of limited value in the age of the Internet. Their critique included the overemphasis on monetary exchange and treating all information as equivalent. As a result of these concerns, the researchers developed an expanded model of *consumer privacy concern* that included three additional dimensions that expressed the "complex contextual nature of privacy"– *information sensitivity, familiarity with entity,* and *compensation for information provided* (63). The researchers recategorized privacy concerns within a three factor model that included *control over collection and usage of information, short term transactional relationship* and *established long term relationship*. Sheehan and Hoy (2000:71) found that "what information is collected in what manner by which entity to be used for what purpose influences people's privacy concerns."

Apart from the insights about the complexity of consumer privacy concern, this study provides important support for my contention that there are opportunities for firms to differentiate themselves from their competitors by going beyond mere compliance with the prevailing social norm or regulatory regime[8]. Firms that embrace the notion that customers have varying sensitivities to privacy based on the types of information gathered might be able to provide specific inducements for sharing. Sheehan and Hoy's (2000) construct *familiarity* addressed privacy concerns with firms with which consumers had different levels of awareness and relationships. They found that consumers were more likely to have high privacy concerns when receiving unsolicited email from unknown firms and low privacy concerns when receiving email from firms with which they currently did business. The challenge for firms is how they establish relations new, prospective customers and their attendant high privacy concerns as well as maintain existing relations with current customers. My research into Information Privacy Orientation should assist with illustrating how certain firms address (or not) this challenge.

Dinev and Hart (2003) specifically examined the role of tradeoffs in an online environment. The researchers used the "consumer privacy calculus" (Culnan and Bies 2003; Laufer and Wolfe 1977) as a theoretical framework and tested a model of *Internet use* (the

[8] Privacy Philosophy is the third layer of the Information Privacy Orientation continuum.

likelihood of engaging in e-commerce transactions) based on its theorized association with *perceptions of vulnerability, ability to control, privacy concerns, trust,* and *interest*. They found that privacy concerns were strongly, directly and negatively related to Internet use. The greater the consumers' concerns for how their personal information is gathered and (mis)used, the less likely they are to engage in transactions on the Internet. In addition, they found that perceptions of vulnerability was related negatively to trust and positively to privacy concerns while perceptions of the ability to control one's personal information positively influenced trust while diminishing privacy concerns.

This study reinforces two important lessons for firms. First, firms need to understand the complex and multidimensional nature of consumer privacy concerns and the different ways these concerns influence consumer behavior. Second, organizations must tailor their efforts to address the specific concerns in meaningful ways in order to reduce the negative and enhance the positive. The authors suggest that it is "not sufficient ... to only target consumers' interests (i.e. user-friendly and attractive websites, lucrative marketing incentives, etc.) to disclose personal information ... businesses need to focus on building trust" (23).

In one of the few non-U.S. based consumer studies, Hine and Eve (1998) conducted a qualitative investigation into the "construction of privacy infringement – the ways in which representations of the self, representations of the data using organization, and the technology combine" (254). Consistent with previous research (Culnan 1993; Smith et al 1996), the authors found "no single set of factors that consumers identified as privacy infringement" (260). Rather, they discerned five factors that contributed to the construction of privacy infringement - the *visibility of the mediating technology,* the *legitimacy of motives for information requests, the intrusion/disruption of* [customers'] *legitimate activities, imbalances of power and control,* and the *social context.* The perceptions of privacy infringement by customers was neither isolated nor static. Rather, respondents constructed their perceptions of firms' data collection activities within a larger view of an emerging technological society in which personal control over information is

largely a matter of trust, both in the uses of technology and the organizations that deploy them. Interestingly, privacy infringement, as a specific concern that might prevent or constrain customers in their shopping behaviors, was "rarely independently raised" (254) by the different study participants. However, the researchers found that when prompted, "concerns about privacy were widespread" and the interviewees articulated their concerns in repertoires of benefit, risk, trust and control.

This research is important for my dissertation for the following reasons. First, the research approach provided the opportunity for customers to talk about their issues rather than have researchers derive them from other researchers' literature reviews. This provides an important "reality check", especially for those of us who are immersed in the subject. The experience that respondents needed prompting to address privacy specifically may have a variety of explanations but the obvious one that privacy is not the top of mind concern cannot be ignored and has interesting implications for firm behavior. Second, the five factors demonstrate both the temptations for firms to engage in privacy violating behaviors with the excuse that "what customers don't know doesn't seem to bother them" as well as the consequences of lacking sensitivity to customers concerns that they not be taken for granted or assumed to be incompetent to understand firm behaviors. This plainly articulates the privacy paradox with which firms must struggle to find their niche. Finally, Hine and Eves (1998) employed both a research methodology (multiple qualitative methods) and an analytical strategy (content analysis) that clearly lend themselves to moving below the surface of constructs and exhuming interesting findings. I will be using qualitative methods and content analysis in my research and it is encouraging to see them employed by others to such good effect.

In summary, research has demonstrated that customers' information privacy concerns are multifaceted. Important themes include the need for customers to have control over their information, the importance that they be treated fairly, the value of preserving existing commercial relationships, and the willingness of customers not to transact business because of

privacy concerns. The next group of consumer studies suggests that customers can be motivated to disclose information (overcome privacy concerns) given appropriate organizational action.

Consumer Motivations to Disclose Information

Several studies have attempted to shed some light on what motivates consumers to give up their privacy by sharing personal information with businesses. Dhillon et al (2002) applied Keeney's (1992) value thinking approach – what are the values or principles that customers bring to their decisions – and applied the approach to a consideration of customers' privacy concerns when engaging in internet commerce. The value thinking approach is thought to help decision-makers, in this case customers, make decisions based on what is truly important to them as opposed to what appears to be the available alternatives. From the interviews conducted in the U.S. and the U.K., the researchers were able to identify 28 clusters of objectives that were classified by whether they were *fundamental privacy objectives* (i.e., maximize shopper ability to control personal data) or *means related objectives* (i.e., decrease customer responsibility for privacy issues).

This preliminary research provides another template from which to consider the development of a firm's privacy goals. While Dhillon et al. established that the "overall objective" is to "Maximize Internet Commerce Privacy" there are eight supporting fundamental objectives. Interestingly, these objectives include "maximize reputation of the firm" by emphasizing trust[9] and "maximize expectation of shopping privately" to ensure the creation of a norm of privacy protection (708). These statements illustrate that organisations need to be aware that customers have privacy preferences that are an expression of values, not simply media induced paranoia. This study, therefore, is useful in providing an approach to discussing with the research sites what their customers' privacy values are and how they are being met by the firms' specific privacy activities. I would expect that the there will be a range of responses depending on

[9] Trust and Reputation are argued to be part of the social capital outcome included in the Information Privacy Orientation contingency framework. See page 59.

whether or not the firms have investigated their customers values and whether they consider responding to customer values as a legitimate objective for their privacy activities.

A recent study by Tam et al (2002) combined expectancy theory (Stone and Stone 1990) with extrinsic/intrinsic consumer value theory (Davis, Bagozzi and Warshaw 1992) to develop a framework of seven "disclosure motivators." Expectancy theory suggests that individuals strive to maximize positive outcomes (like receiving benefits) and minimize negative activities (like privacy invasions). Consumer value theory argues that individuals are motivated by extrinsic or instrumental stimuli (such as a coupon to receive a discount) and intrinsic stimuli (such that the shopping experience is an end in itself). The researchers found that *monetary savings*, *time savings* (extrinsic/instrumental) and *pleasure* (intrinsic) were the most likely motivators for disclosing personal information.

This research takes an interesting approach to thinking about customers shopping on the Internet. It does not address privacy specifically and none of the statements used in the questionnaire deals with any of the privacy, security, and confidentiality concerns (Rindfleisch 1997) that other literature suggests serve as barriers or de-motivators for customers. In my view, this is a problematic omission. The authors assert that as competition heats up for customer information, firms are using a combination of motivators to induce disclosure (Tam et al 2002:18). However, the study missed the opportunity to assess the direct appeal of privacy statements and security protocols to "motivate" disclosure. It would be interesting to have this study replicated with the addition of "motivators" that address privacy and security issues.

However, this study provides the basis for discussing the concepts of disclosure motivation and, hence, the potential role for information privacy behaviors as motivators. What motivators are firms employing? Are customers responding? How do these motivators, for example, reflect a firm's Customer Relationship Stance or support its Information Management

Strategy[10]? As well, the study provides a framework for adding additional motivators that specifically address privacy concerns (how could privacy behaviors be used as motivators? Are they intrinsic or extrinsic)?

Another study examined the question of *motivation to disclose* by calculating the dollar value of privacy protection. Hann et al (2002) invoke traditional "rational economic man" theory to argue that customers will willingly disclose (forgo privacy) if the price is right. The price may be monetary reward or time savings (similar to extrinsic motivators) influenced by individual characteristics. Their experiment found privacy concerns generally outweighed economic incentives. While time savings were significant, the real effect was that firms need to offer "substantial monetary incentives" (ranging from $ U.S.15.46 to $ U.S.49.78)(6) depending on the privacy policy under consideration. Websites that offered *reviews for error, restrictions against secondary use* or promised *no secondary use* were ranked higher by respondents than those that did not offer these protections. The combined costs to forgo these privacy protections ranged up to $105.57 U.S. Interestingly, there was no statistically significant effect for individual differences.

For my purposes, the actual cost estimates are of less importance than the magnitude of concern they reflect. The "customers" in this experiment required a tangible and substantial financial incentive to forgo their privacy through disclosure. This suggests that there is an economic incentive for firms to engage in surreptitious information gathering in order to avoid the costs that may be associated with "motivating" customers to disclose. On the other hand, firms may find it cheaper to not engage in privacy violating behaviors and instead spend their energies on devising useful information strategies that deliver specific information that has been willingly (and accurately) disclosed by customers. Non-academic researchers have found that on-line "misrepresentation" is rampant (BCG, etc).

[10] Both Customer Relationship Stance and Information Management Strategy are layers of the Information Privacy Orientation continuum.

Phelps, Nowak and Ferrell (2000) applied Social Contract Theory (Dunfee, Smith and Ross 1999) to an examination of the *willingness to provide information.* Social Contract Theory suggests that consumers are able to exercise some control over the collection and use of their information in order to minimize the risk of being harmed (29) through the exercise of an implied "social contract." The researchers developed a conceptual model that comprised four input factors (type of information required, amount of information control offered, potential consequences and benefits, consumer characteristics), outcomes (beliefs regarding marketers' information practices, overall concern regarding the ways companies use personal information) and future outcomes (behavioral and future attitudinal responses).

Phelps et al (2000) found that *willingness to provide information* depended on the *type of information* being sought. Respondents were more willing to provide demographic and lifestyle information and less willing to provide financial and personally identifiable information. Furthermore, the *level of concern* with corporate use of customer information was high (87% of respondents were either "very concerned" or "somewhat concerned"). This concern for privacy was also related to *perceptions of information behaviors* by firms. The very concerned respondents (45% of sample) were most likely to disapprove of secondary use of personal information, support constraints (regulatory or voluntary) on firms' information practices, and take action to prevent privacy invasions (e.g., request to be placed on do not call/mail list).

Importantly for my research are two particular findings from the Phelps et al (2000) research. First, was the role of *personal interest* in the willingness to share. Customers did not like receiving unsolicited catalogs and mailings because they regarded this action as intrusive largely because the material did not correspond to their interests and because they did not appreciate receiving mailings from companies with which they had not previously done business. Second, was the finding that consumers' control over their information was positively related to *purchase intentions* and that purchase intentions were negatively related to requests for "sensitive" information such as financial or personally identifying information. This supports my

contention (expressed within the contingency framework) that there are outcomes attached to firms' information privacy behaviors, for example, intellectual capital (actual useful information about customers) and financial capital (customers will spend more with firms that they perceive have "better" privacy behaviors than those that have "poorer" privacy behaviors).

Ranganathan and Ganapathy (2002) took a different approach to the question of how privacy concerns influenced *consumers' purchase intentions*. These researchers examined what features or characteristics of websites were most important to consumers. They found that the relative importance of the four main characteristics of websites were *security, privacy, design,* and *content*. What is particularly interesting about these findings is that the "security" feature of greatest value to the sample was the ability to access an alternate payment mode. This has been shown in other studies to be an important aspect of the "security" principles within the FIP for privacy. Furthermore, the highest item in the privacy factor "*hesitation in sharing personal information over the web*" followed by "*gathering of personal information*" suggests that the respondents understood that privacy violation requires two participants – one to provide (share) personal information and one to collect (gather) it. This insight should lead organizations to consider what exactly they think they are accomplishing with their information collection procedures, especially given the evidence that consumers frequently are less than truthful in their personal information disclosure (Graphic, Visualization, and Usability Centre 1998; Greenman 1999.) This supports my contention that there is a link between information gathering and privacy protecting behaviors to desired outcomes (whether privacy enhancing or violating). Certainly, the finding that security and privacy had predictive power for customer purchase intention supports the inclusion in my contingency framework of the outcome categories of social, intellectual and financial capital.

In summary, consumer motivation to provide information has also been investigated and we are beginning to understand the complexity of its construction. Notions of personal values and personal interest, intrinsic versus extrinsic motivations, actual monetary value for personal

information, as well as the influence of website design are important issues for customers that organizations should consider as they craft information privacy policies. Interestingly, as the next section demonstrates, organizational level studies have not generally taken consumer privacy concerns as their starting point.

Organizational Level Studies

Goldstein and Nolan (1975), in a Harvard Business Review article, warned that privacy would be a significant challenge for companies and governments in the years ahead. The authors took a fairly narrow view of what constituted privacy and argued that activities such as allowing customers and employees ("data subjects") to view their own information and request corrections had "little to do with privacy per se" but reflected an attempt to address perceptions of power imbalances between individuals and "remote, domineering and unconcerned" large organizations (66). Despite this arguably condescending view, Goldstein and Nolan advised organizations to deal with privacy as part of a corporate social responsibility program for the pragmatic reason that

> Informing subjects will demonstrate a company's awareness and concern for the privacy of its data subjects and may also be of significant help later in obtaining data and the authorization to use it (69).

Since that time, some limited work on information privacy at the organizational level has been done, primarily by IS researchers. This research largely treats information privacy as an organizational concern within broader contexts such as global IT management (Ives and Jarvenpaa 1991) or ethics/social responsibility (Straub and Collins 1990). Most researchers assert a narrow perspective of privacy as a source of liability (Bordoloi, Mykytyn and Mykytyn 1996) or having to do more with security than privacy (Srivatava and Mock 2000). Few authors examine privacy within specific firms as a business issue requiring organizational action (Cadogan 2001; Smith 1993) despite calls for such investigations (i.e., Chan 2003; Milne 2000).

In this section, I review selections from this research to provide a base for understanding what little we know about the construction of privacy as an organizational concern and to demonstrate both the need for my research and the legitimacy of my approach. Given the limited empirical research at the organizational level of analysis, I will include conceptual and discussion pieces for the sake of thoroughness. Note that details about the individual articles are contained in Appendix B: Organizational Level Studies Summary.

Information Privacy as Organizational Liability

Research into "global IT" has become increasingly important as firms expand operations beyond their domestic borders. In general, the overall theme has been to regard privacy as a source of liability. An example of this thread in the IS literature is Ives and Jarvenpaa's (1991) research in which "international data sharing" was identified as one of the key issues for global IT management. Of particular concern to the managers they interviewed for this research was *transborder dataflows* (TDFs), the "movement of machine-readable data for processing, storage, or retrieval across national boundaries" (Chandran et al 1987). While acknowledging that "global customer/consumers" and firms to serve them (airlines, hotels, rental car and credit card companies) are driving the need for global IT, data flows are discussed primarily from the perspective of internal firm operations including payroll and personnel systems. Ives and Jarvenpaa (1991:44) focus on data standardization (after Keen 1897) and managers are simply advised to "understand your responsibilities, limitations, and exposures vis à vis TDF and privacy laws."

The theme of privacy as a source of liability for firms is echoed in other work. Straub and Collins (1990:144) discussed three sources of *information liability* including "how to collect and disseminate information on individuals while respecting individual rights to privacy." Privacy can be violated through security breaches, inaccurate data collection and inappropriate disclosure. The authors suggest that managers take action through *security* (i.e., access controls,

cryptography, employee training), *stewardship* (lifecycle of information approach) and *informed consent* by data subjects. Bordoloi et al (1996) provided an overview of the broad legal issues involved with *inaccurate data* and emphasized the importance of verifying potentially damaging information. From a risk management perspective, the article reinforced the need for firms to follow strict practices to ensure that information is entered correctly into databases and to verify information before it is acted upon (as a fair information practice approach would require.)

Srivatava and Mock (2000) developed a framework for providing audit opinions on transaction assurances for electronic commerce. They offered a framework for audit firms to use to provide independent third party assurance "to reassure consumers who are fearful of providing credit card numbers to complete transactions (12)." The authors suggest that there are four "categories of assertion" important for web assurance – *soundness of business practices*, *ensuring transaction integrity*, *offering information protection*, and *compliance with legal requirements*. The information protection category generally follows fair information practice concerns including reference to ensuring that there is no unauthorized access to customer data and no improper use.

Approaching organizational level information privacy as an issue of liability is severely limited in its utility. Ives and Jarvenpaa's (1991) efforts reflect, perhaps, the limited understanding of privacy issues by U.S. managers at that time. Certainly, their research predates the European Data Directive. However, ghettoizing information privacy as simply an issue of TDFs with employee information suggests a limiting view of the role of information systems in the revenue generating functions of global firms, especially the capture and manipulation of customer information. The exhortations to appropriate behavior by both Ives and Jarvenpaa (1991) and Straub and Collins (1990) while useful, do not reveal an understanding of the depth of organizational information privacy challenge. Similarly, the legal approach suggested by authors such as Bordoloi et al (1996) leaves little room for discussions about larger organizational issues. The narrowness of this stance reduces information privacy to an exercise in minimizing the risk

of being sued as opposed to minimizing the risk of harming customers, rather than maximizing the value of the information while minimizing the privacy concerns. Srivatava and Mock (2000) also assume a limited perspective, and as a result, the reader is left with many questions. For example, have all the potential risks been captured? From whose perspective? What types of improper uses could occur beyond the defined transaction relationship and what should the organization do to prevent them?

Information Privacy as An Organizational Decision Outcome

The last studies I will review in this section adopt the perspective of information privacy as the outcome of purposeful organizational decision-making. Perhaps the most widely known study of information privacy at the organizational level was conducted by Smith in the late 1980's. Smith's (1990, 1993) exploratory case study of the information privacy policies and activities of seven firms examined two important questions. First, how were information privacy policies developed in these firms? Second, how well did these polices address social concerns and expectations concerning information privacy? Smith found that none of the firms in the study was proactive in adopting information privacy policies and that there was no internally derived reason to be so. Rather, all firms experienced a period of "drift" during which time the absence of an explicit legislated privacy framework permitted unfocussed and, in some cases, abusive treatment of customer information. The threat of legislative action spurred the insurance and credit card firms to make some efforts to institute privacy policies, more or less in line with fair information practices. The banks did not perceive a similar threat and so did not engage to the same extent in developing privacy policies for their organizations. Smith called for additional research to be done to support theory development in information privacy.

Smith's work makes four important contributions that provide a strong platform on which to base research into the study of the development and implementation of information privacy orientation in firms. First, he established that it is possible to observe information privacy policy

development in organizations. Second, Smith identified that different functional units experienced the development and implementation of information privacy policies in different ways. Third, Smith showed that information privacy was an expression of organizational values encapsulated in the raison d'etre for policies (a fear of negative publicity or legislative action), their development (what was covered by policy or not, and who was organizationally responsible), and their implementation (the explicit versus implicit policies and practices that were promulgated in the firms). Last, Smith revealed how firms had not made the connection between their privacy behaviors and their customers' concerns for improved privacy protection.

The commercial world has changed considerably since Smith undertook his research. The broad adoption of the Internet as a commercial medium and the increasing use of wireless technologies have multiplied the opportunities for firms to collect increasingly personal data (Keen and Macintosh, 2001) as well as increasing amounts of data (Culnan and Armstrong 1999). Inexpensive data storage coupled with high speed communication networks boosts the rates by which organisations can gather, use, reuse and act upon customer information (Cavoukian and Hamilton 2003). This has exacerbated what Smith (1993:105) characterized as "a disparity between society's concerns about privacy and industry's response." The imposition of regulatory privacy regimes also complicates organizational decision making. As a consequence, there is a need to reexamine the construction of privacy regimes in organizations, which is at the heart of my proposed research.[11]

A more recent study addressed specifically the impact of the Internet on firms' information privacy behaviors (Cadogan 2001). Her multiple case study examined the privacy activities of three major online presences – Online Privacy Alliance (an industry organization devoted to privacy issues), Amazon.com (a retailer of a large variety of consumer products) and Dell Computer Corporation (a retailer of "high ticket" computers and peripherals). Of most

[11] I corresponded with Dr. Smith and asked specifically if he thought that there was a need to continue organizational level studies. His email response to me indicated that there was a need to understand processes of decision making about privacy in firms beyond "narrow" legal issues (21/06/2002).

interest to my research is that in addition to using an adapted version of the Culnan analytical instrument and subjecting the firms' policies to readability analysis, the researcher contacted the representatives named on the websites for follow-up questions. The findings suggest that while all three organizations professed a keen interest in consumer privacy, their policies revealed different approaches that were more or less "readable" and , therefore, intelligible to customers.

This study makes three useful contributions. First, it is the only recently conducted study of which I am aware that asks the responsible firms to elaborate on their policies' contents and their organizational approach. In this way it looks behind the privacy policy to address issues of intention and implementation. Secondly, concern for the readability of policies suggests that the presentation of policies requires organizational thought if the policies are to be understood by customers and to enable customers to exercise choice, correct errors, etc. The important point of consideration here is to ask ourselves if the readability level of a privacy policy is a meaningful clue to a firm's intentions? Third, and most importantly for my research, Cadogan's commentary suggests that different firms have different characterizations of both their responsibility to customers in terms of privacy and willingness to share control over the information customers provide to companies.

For example, Cadogan characterizes Dell Computer's approach as "a partnership with both Dell and the customer taking appropriate action (2001:240) characterized by Dell's pledge to "help the consumer maintain control over [the] individual's personal data on the Internet") (Cadogan, 2001:238). Dell has partnered with the National Consumers League (NCL) to develop the "Consumers Guide for Internet Safety, Privacy and Security" (234), allows outside organizations to scrutinize its privacy program and recommend actions to improve security and privacy (232), and provides information on its website about the use of privacy enhancing technologies, such as anonymizers, to provide customers with privacy protection options (235). Furthermore, the researcher's comments about the openness of Dell staff to discussing their privacy behaviors suggested that the firm had nothing to hide and was "walking the talk" about

being proactive on privacy issues. I interpret this as an example of a firm that is trying to do more than merely "comply" with the U.S. social and regulatory norms for privacy. Both the differences in Dell's behavior and philosophies are consistent with my theory of Information Privacy Orientation.

In summary, information privacy as an organizational level phenomena has been under-researched and confined to treatment largely as an issue of liability. The multi-dimensionality of customer information privacy that was demonstrated in the previous section of this chapter, does not seem to be reflected in organizational level studies, with rare exception. What has been researched suggests that the phenomenon is rich and varied among firms and industries but as many questions are raised as are answered. As a result, there are many gaps in our understanding. Of particular interest is the need to understand the content of organizational decision-making (my proposed information privacy orientation construct) as well as the context and process which make up the decision-making environment (my proposed contingency framework). In the final section of this chapter, I review a sample of the literature that addresses information privacy at the sectoral/national level of analysis.

Sectoral/National Studies

A major contribution to our general understanding of information privacy has come from the study of privacy policies and statements posted on websites. These studies were conducted at the supra-organizational level of analysis including sectoral (industry) and national (jurisdictional) efforts. *Privacy Policies* refer to "a comprehensive description of a company's web site information practices that is located in one place on the site and may be reached by clicking on an icon or hyperlink," (FTC 1998) while a *privacy practice* is "a discrete statement that describes a particular practice regarding consumers' personal information" (Leizerov 2001). With one exception, all of the studies reviewed in this section fall within the tradition of evaluative research (Patton 1990) that is generally, although not exclusively, concerned more

with describing the extent to which organizational actions meet requirements or expectations than with hypothesis testing or theorizing. The website studies to be discussed below are primarily of this ilk – there is little theory that underpins much the work. Most of these studies are descriptive. They examine the extent to which privacy policies posted on web sites meet some predefined standard, for example the U.S. FTC's fair information principles (FTC 1998, 2000; Culnan 1999a), or the Organization for Economic Cooperation and Development's (OECD) privacy principles (Livingston 2002). Another feature of the research is that it combines nationally based (i.e., exclusively U.S. or Canadian) with sectoral analysis (i.e., what is the relative performance of financial versus entertainment website policies). One study examines information privacy as a national cultural phenomenon. Note that the details about the specific studies are contained in Appendix C: Sectoral/National Level Studies Summary.

There are two categories of national/sectoral evaluative studies that I will discuss. In the first category are those studies that strictly report whether or not privacy policies appear on websites and the extent to which these policy statements comply with the some standard such as basic FIP. These studies primarily identify and count the features of website privacy policies. In the second category are studies that attempt a more sophisticated analysis of the policies and statements by theorizing firm behaviors beyond simple compliance.

Descriptive Sectoral/National Studies

Likely the most well known website policy studies within the descriptive studies category are those that have been carried out under the auspices of the U.S. Federal Trade Commission (FTC)[12]. The FTC considers the privacy practices of notice, choice, access and security as the main mechanisms for providing consumers with the information they need to choose appropriately among the online presences with which they do business. The FTC's 2000 study

[12] The FTC has regulatory authority for enforcing U.S. federal privacy statutes (for firms under their jurisdiction). These statutes include the Gramm-Leach-Bliley privacy law for financial institutions, as well federal antitrust and consumer protection laws. The FTC characterizes its role primarily as curbing actions by business that undermine consumers' abilities to make informed choices in the marketplace (FTC, 2000).

was concerned with consumer-oriented (i.e. "B to C") sites only. The study examined the 100 "Most Popular" and 335 randomly selected websites. Only 45% of the most popular sites and 20% of the randomly selected sites addressed all four features of FIP. In addition, only 45% of the most popular sites and 8% of the randomly selected group displayed a web seal indicating membership in a privacy organization (i.e., BBB Online, TRUSTe, VeriSign, WebTrust) requiring adherence to a set of privacy policies (FTC 2000). However, these results indicated a marked improvement over the 1998 study that found that 97% of the websites surveyed collected personal information but only 14% had any privacy information posted (FTC 1998).

In 1999, the Georgetown Internet Privacy Policy Project (GIPP) surveyed 361 websites randomly selected from the top 7500 URLs surfed by consumers in January 1999. The study found that while 92.8% of the sites collected at least one piece of personally identifiable information, 34% had no privacy policy posted and only 14% had all elements of their version of Fair Information Practices of notice, choice, access, security and contact information (Culnan 1999a). Lastly, a study of the top 100 U.S. websites was conducted, again in 1999, for the Online Privacy Alliance (OPA) by Culnan (the lead investigator for GIPP). The purpose for the research was to address compliance with the OPA's industry guidelines for commercial websites, not the FTC's requirements. The study showed that 99% of sites collected some personal information, 93% posted some privacy statements while 81% posted privacy policies. However, only 22% of the sampled sites addressed all four of the FTC's fair information practices (Culnan 1999b).

Ryker, Lafleur, McManis and Cox (2002) reported on another FIP compliance website study that used the same instrument as that used in the FTC studies. This study was different in three ways. First, the sample was small and selective. The sites under scrutiny were those firms listed in the Fortune magazine's "e-50" as of September 2000. The second important difference, therefore, was that this study examined both "business to customer" (B to C) websites (the exclusive focus of previous studies) and "business to business" (B to B) websites. Third, the

content analysis conducted in the study categorized compliance in two ways, by individual fair information practice and overall compliance.

The results for both categories of firms showed that despite Fortune's glowing assessment that "[t]hese companies get it, they understand the profundity of the Internet and its power to change business" (Chen 1999:141), these firms did not "get" privacy very well. Overall, only two of 35 B to C websites fully complied with all four F.I.P, 22 had policies in partial compliance while 11 did not comply with even one FIP requirement. The F.I. P of notice was the practice best addressed by the B to C firms with 30 firms' "notice" policies fully compliant. "Choice" was fully complied with by 15 firms while another 19 were partially compliant. The "Access" practice was the weakest area for compliance with six firms fully compliant. Lastly, despite public concerns for "Security," only 19 of the examined policies were fully compliant by addressing both the security of information in process (i.e., credit card information to purchase an item) and security of information within the firm itself (i.e., firm's storage system cannot be accessed by unauthorized users). The results for the B to B websites (15 firms) were even worse. Only three (20%) of these firms had posted a privacy statement and none was fully compliant. This was an interesting, and very disturbing finding. It suggests that B to B firms did not feel pressure to address consumer privacy issues even if they might be in a position to have access to this information in the course of working with B to C firms.

The sole Canadian based evaluative study was conducted in 2000 (Geist and Van Loon 2000). Two hundred and fifty nine sites were studied of which 194 were Canadian in origin, 42 were "dual-origin" (hosted outside Canada but with significant Canadian content) and 23 were "foreign" sites that, while lacking Canadian specific content were deemed of sufficient interest to warrant inclusion. The survey divided sites into five broad categories to facilitate comparison – e-commerce, sensitive information, services, culture and government and Canadian media. Geist and Van Loon (2000) found that 41% of all sites and 50% of Canadian sites lacked a privacy policy while 58% of all sites collected personal information without advising customers. Many

sites were not compliant with the then-proposed federal privacy legislation (then called Bill C-6, now known as PIPEDA). Forty-six percent of sites lacked explanations for the purpose of collecting information; 94% did not explain data retention policies; and 40% did not communicate the firms' intentions with respect to sharing or selling customer information with third parties. Firms within the "sensitive information" category performed the best of the five categories while the Canadian media group performed the worst. Interestingly, the data on the use of web seal programs showed that there was both a low uptake (10% of Canadian sites) and no dominant program (six programs were identified).

The last descriptive study I will review was also a "B to C" website review conducted by Miyazaki and Fernandez (2000). This effort was different from previous studies in two important ways. First, the researchers explicitly distinguished between privacy policies and security policies. Second, they were interested in determining whether and how firms' policies addressed consumer privacy concerns. Three consumer privacy concerns were identified – *online customer identification*, *unsolicited customer contacts*, and *customer information dissemination*. Three company "responses" to these concerns were identified – *technology to secure transactions*, *guarantees against credit card fraud*, and *alternate payment capabilities*. The results indicated that firms were more likely to have security statements (78.5%) than privacy statements (49.8%). Of the sites with privacy statements, 28% addressed online customer identification, 40.3% unsolicited customer contacts, and 34.8% customer information dissemination. Of the sites with security statements, 65%.5 indicated that they used secured transaction systems, 7.5% guaranteed reimbursement of unauthorized charges, and 54.9% provided alternate payment methods.

These descriptive studies are useful for three reasons. First, these studies document policies and thus provide a base line with which to compare future studies. Second, they illustrate differences in national experiences. Canadian and U.S. privacy behaviors appear to be different and thus warrant separate examination. Third, they demonstrate that there are differences in privacy behaviors across industries. This suggests that there is a need to examine privacy

behaviors by industry or sector in order to understand the reasons for the observed differences. However, as with the majority of evaluative studies, the lack of theory on which to base explanations for observed differences is problematic.

In summary, the descriptive evaluative studies have indicated low but improving corporate privacy policy behaviors as expressed through posted policies and statements. Policies for both B to C and B to B firms could be greatly improved. Canadian firms appeared to be as non-compliant as their U.S. counterparts, if in different ways. These studies indicate a range of privacy behaviors both between jurisdictions and across sectors. However, they do not provide insight into the underlying reasons for the variance. The next set of studies I review offers more scope for this understanding.

Theory-Based Sectoral/National Studies

The second group of sectoral/national evaluative studies move beyond merely cataloguing policies and measuring compliance. These studies invoke a variety of theories to explain the privacy behaviors that are represented by the posted policies.

Earp, Antón and Jarvinen (2002) applied Goals-Based Requirements Analysis to a case study of 23 healthcare web sites' privacy policies. Goals-Based Requirements Analysis argues that information systems are designed purposefully to meet certain specific organizational goals and objectives. The purpose of the study was to test the applicability of a previously developed conceptual framework incorporating five perspectives that influence the development of privacy policies. These perspectives were argued to include *legal constraints*, *technical measures*, *business rules*, *social norms* and *contractual norms.* A taxonomy of privacy goals was articulated to guide interpretation of the statements. The taxonomy includes *privacy policies*, *privacy protection goals* and *privacy goal obstacles*.

The results of the case study were that 46% of goal statements supported the social perspective, 23% the technical perspective, 20% the contractual perspective, 9% the business

perspective and 3% the legal perspective. One interesting finding was that technical goal statements were almost evenly split between protection statements and vulnerability statements. The authors argue that this is to be expected given the role that technology plays both in protecting privacy through such things as encryption algorithms, and violating privacy through the automated gathering and storing of personally identifiable information.

This study is important for three reasons. First, it makes an important move away merely from counting the features of privacy statements toward an articulation of privacy protecting and privacy violating behaviors as organizational activities. Second, it acknowledges that organizations have multiple perspectives on privacy as an organizational issue. The use of the goal-based approach brings added insight – the various statements say something about what a firm appears to be trying to accomplish. Third, by dealing exclusively with a single industry (healthcare) in a single jurisdiction (U.S.), we learn that firms make different decisions even when in a regulated environment[13]. This is an important point given my desire to address a single industry in Canada. I incorporated aspects of the Goals Based Requirements analytical approach in my research, as will be described in Chapter Six: Research Methods.

Privacy issues at the sectoral or national level of analysis has been the subject of recent dissertation research. While these studies dealt exclusively with U.S.-based commercial interests, they add to our understanding in several areas by moving beyond description to attempting to offer additional insight by either meshing policy evaluation with previously existing research (i.e. Smith, Milberg and Burke 1996 concern for information privacy instrument) (Alexander 2001) or theorizing about what evaluations say about how privacy issues are played out on the Internet (Leizerov 2001 – conflict institutionalization study).

Alexander (2001) re-evaluated the 335 high traffic commercial Internet sites that had been examined by Culnan in her studies for the FTC and the OPA (Culnan 1999a, 1999b). The

[13] Healthcare is one U.S. industry that has sectoral privacy legislation (Health Information and Personal Privacy Act, HIPPA) governing its information gathering and privacy activities

research aimed to consider how companies address consumers' information privacy concerns through their privacy policies. The study's most important contribution is the development of the "privacy consciousness matrix" which is conceptualized as "incorporating *accessibility, participation, choice, security, enforcement,* and *error correction concepts*" (30). It is theorized as the gap that exists between customers' *information privacy concerns* and the *FIP* implemented by firms. This study offers an interesting perspective that suggests that firms, and indeed sectors, can be differentiated on the basis of their privacy behaviors, and that these behaviors represent at some level an expression of a particular perspective on privacy. However, despite the interesting concept of the privacy consciousness matrix, the study largely explores FIP implementation across industries and says little about the reasons for firms or sector behaviors.

Livingston (2002) modified the FTC/Culnan questionnaire in a study of national/sectoral compliance with the OECD's privacy principles (OECD 1980). This study sought to identify privacy trends across the small sample as well as to assess the extent to which these sites might be found to be *confusing* to Internet users. The matter of confusion was thought to contribute to Internet users' privacy concerns. Livingston found that there was a great diversity of privacy practices engaged in by the firms whose sites were evaluated as well as great variance in the *comprehensiveness* and the *clarity* of the policies. None of the websites included in the study clearly (i.e. unambiguously) met the totality of the OECD requirements. The majority of the policies were inadequate in both substance and clarity. This study demonstrated that there is variance in how firms express their privacy behaviors and that this may be a source for differentiation.

Leizerov's (2001) holistic case study examined the privacy polices posted to a sample of U.S. websites. This study continues within the evaluative research tradition but uses the language of conflict management as a theoretical lens. The purpose of the research was to investigate the extent to which the conflict of interest between companies and individuals over how personal information is treated has become institutionalized. *Conflict institutionalization* is described as a

"system comprised of rules (norms or laws) that bind (social bonds) the parties' actions and an agency (governmental or non-governmental) that monitors them" (1). Within the U.S., the overarching "rules" are the FIP and the main "agency" is the FTC. However, the actual conflict is played out or "institutionalized through binding social norms" such as privacy behaviors to build trust, and "a pattern of collective action" such as the creation of industry oversight agencies (i.e., Truste and BBBonline) that offers the various parties incentives and mechanisms through which conflicts may be resolved thus avoiding "non-legitimate (extreme) conflict" (47), tighter legislation or online shopper boycotts. The conflict is characterized as a *conflict of interest* - firms' interests in maximizing economic outcomes conflict with customers' interests in maintaining privacy (25). This is an important theoretical point that I use to underpin my contingency framework.

Leizerov's research was extensive and I will highlight only those aspects of most salience to my research. The sample was drawn from the "most popular" category used in the previously discussed FTC studies augmented with companies participating in either of the Truste or BBBonline privacy web seal programs. The institutionalization of the conflict was assessed by analyzing six different variables - *compliance with regulations, attitude of compliance with regulations*, i*ntrusiveness of data collection, integrity, trust building through responsible privacy practices, and transparency and competition for customers*. These variables are reflected to varying degrees in both my contingency framework and the Information Privacy Orientation continuum.

Among his various findings, Leizerov demonstrated industry differences for all four aspects of social bonds. Further, he found statistically significant differences among sites that were not members of a web seal program, those who were members of Truste and those who were members of BBBonline. Overall, members of the BBBonline program were in greater compliance with FIP and displayed a better "attitude to compliance" than the Truste members. Furthermore, the BBBonline members displayed greater efforts at "building of social bonds" than

Truste members. Interestingly, the research showed that many non-members displayed higher compliance and greater social bond concerns than did members of the Truste web seal program! Lastly, the researcher examined whether there was a discernible difference between privacy policies exhibiting more concern for adhering to rules or for building trust. Interestingly, Leizerov found a high correlation between compliance with institutionalizing rules and greater concern for trust building measures.

This dissertation makes many contributions to the national/sectoral studies research stream. First, by considering the messages and motivations behind the features of posted privacy policies, he has demonstrated that when parsed carefully, privacy policies reveal important information. Second, he shows that industry effects are important. This means that we can expect that firms within a given industry will display privacy policies that will likely be comparable on many measures. The relative importance of the differences in approach, therefore, call for careful consideration. Third, this work shows that the building of trust with customers is not simply a question of asserting "trust is important" but of behaving in several ways that appear to be both consistent and mutually reinforcing. Fourth, the finding of the high correlation between rules compliance and trust-building raises interesting questions. This finding is perhaps not surprising in a self-regulated context. Firms that choose to engage in privacy behaviors such as complying with FIP or joining a web seal program are more highly engaged in privacy matters than those who do not comply, do not join an industry group, etc. However, would this finding be the same in a regulated environment? When the minimum acceptable behaviors are defined by law, firms can exercise choice about the extent to which they build upon this legal "floor" and they surely have specific reasons for doing this (or not). Hence, my investigation into compliance versus other motivations appears justified in the Canadian context.

The final sectoral/national level study I will discuss departs from the previously reviewed studies in that it does not involve reviewing policies on web sites. Rather, Milberg, Burke, Smith and Kallman (1995) surveyed members of an international association from nine different

countries. The purpose of their research was to examine the relationship among *nationality*, *cultural values* (based on Hofstede's (1984) cultural differences) and the *nature* and *level of privacy concerns* and how these factors influenced the *regulatory scheme* preferred by managers. They found that the overall level of information privacy concern varied across nationalities but that there was no difference among the relative importance of issues or among the level of information privacy concern and cultural values. However, significant differences among cultural values and type of regulatory scheme as well as among level of information privacy concern and regulatory scheme were observed in the research. (The significance of this research is discussed more thoroughly in the following chapter on the contingency framework).

In summary, these national/sectoral privacy studies based largely on the categorization and analysis of privacy policies and statements posted on websites have provided important insight into information privacy trends across industries. While caution must be exercised in comparing among these studies given that they track firms in different jurisdictions, have different purposes, designs and sample frames, define FIP differently, and use different variables and definitions, three tentative conclusions can be drawn. First, privacy behaviors differ among industries and firms. Second, we are beginning to glimpse the outlines of some of the ways to explain these differences. Third, there is some indication that firms may have privacy philosophies that are manifested in privacy behaviors.

However, these studies are not without their limitations. First, counts of policies do not explain firm behavior (Milne and Culnan 2002). Second, the predominantly U.S. basis for the studies is not helpful in understanding firm behavior in other jurisdictions. Describing the frequency of compliance with FIP on U.S. sites does little to explain the behaviors of Canadian firms required to comply with the 10 principles of the federal PIPEDA legislation (explained in Appendix D: Background to Information Privacy Principles). The Geist and Van Loon (2000) study makes a particularly important contribution as a result. A third problem is that the emphasis on the online privacy experience denies the myriad ways available to firms to track customer

behavior in more "traditional" exchanges such as using scanning technology (Culnan and Bies 1999). In other words, to truly understand privacy behaviors of firms, we must consider the totality of their customer information collection apparatus across their "clicks and bricks" scope of operations. In addition, the cross-sectional nature of the research overall leaves us uncertain as to the changes in policies, if any, of individual firms. Finally, with rare exception, the studies treat all firms the same, as simply announcers of policies rather than implementers of strategies. I believe that this is a demonstrably inadequate approach to understanding a phenomenon as complex as information privacy.

Chapter Summary

In this chapter I reviewed literature on information privacy according to three levels of analysis. Consumer information privacy has been investigated extensively and we are beginning to understand the complexity of its construction. Control, procedural fairness, information sensitivity, trust and personal experience combine with the knowledge of different information privacy violating practices to form a potent stew of expectations that organizations should heed. Furthermore, we have extensive evidence of variation in firm activity based on several studies have been conducted at the sectoral/national level of analysis. However, little work has been done to get behind firms' policies to understand the range of motivations, circumstances and objectives that make up the answer to the basic research questions of why firms behave they way they do and how these behaviors are manifested in firm outcomes. In other words, our understanding of information privacy at the organizational level is inadequate. A conceptual approach to addressing this gap is the Information Privacy Orientation contingency framework that is the subject of the next chapter of this dissertation.

CHAPTER THREE

INFORMATION PRIVACY ORIENTATION CONTINGENCY FRAMEWORK

In Chapter Two, I reviewed selected information privacy literature by level of analysis, and argued for the necessity of conducting systematic research into information privacy as an organizational phenomenon. I further suggested that this systematic analysis must consider the context within which different organizations exist. In this chapter I present my Information Privacy Orientation Contingency Framework (IPOCFW) as illustrated in Figure 3-1.[1] The IPOCFW organizes a series of variables that I believe represent the larger organizational context within which my focal variable, Information Privacy Orientation, is situated. These variables are derived from various business research literatures and appear either to influence or be a consequence of Information Privacy Orientation (IPO). Note I include this framework to assist both the reader and me to understand the organizational context for IPO. I did not investigate this framework specifically as part of my dissertation research.

In this chapter, I review the external variables (national culture, regulatory environment and industry practice) that I argue influence the firm's decision to implement a privacy program. Next, I review two sets of internal variables: those that support the achievement of the firm's economic mission (strategic positioning, market orientation, and slack resource availability), and those that support other goals (organizational culture, ethical climate, interfunctional values, and top management preferences). Last, I discuss the formation of social, intellectual and financial capital, which I contend are important outcome variables related to information privacy orientation.

---

[1] I draw the readers' attention to the direction of the arrows in this framework. My reading of the literature suggests that this is a legitimate ordering of the variables for exploratory purposes. However, a plausible alternate reading would reverse the logical flow with the proposed "outcome" variables influencing Information Privacy Orientation and the left-hand (internal variables) serving as the consequences of privacy orientation. I remain open-minded about the issue of directionality.

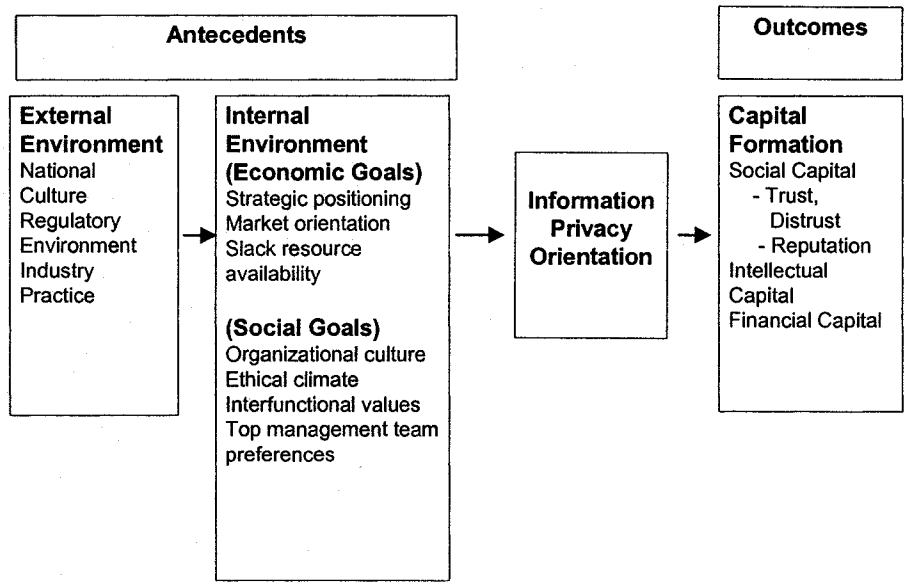


Figure 3-1: Information Privacy Orientation Contingency Framework (IPOCFW)

Antecedent External Variables

The impact of the external environment on firm behavior is well documented (Porter 1980; Day and Wensley 1988; Kotler 1994). I believe three of these are most salient to the development of Information Privacy Orientation – national culture, regulatory environment and industry practice.

National Culture

National culture would appear to have an independent effect on decision-making, irrespective of regulatory regime. I argue that consumer actions represent, at least to some extent, an expression of a national culture. For example, the US (Cesepedes and Smith 1993; Culnan 1993; Hart and Dinev 2002; Phelps, Nowak and Ferell 2000; Sheehan and Hoy 2000) and UK (Long, Hogg, Hartley and Angold 1999) consumer preference for maintaining control over their personally identifiable information exemplifies a cultural preference. Americans are seen to be more trusting of business and less of government for information privacy protection when

compared with their European counterparts. This leads to approaches that in the US emphasize reactive regulations providing for market remedies (consumers armed with information choose which firms they will deal with), while the EU approach emphasizes broadly applicable proactive regulation that reinforces information privacy rights (Walczuch and Steeghs 2001).

Milberg et al. (2000) studied the link between national cultural values, regulatory approaches and managers' regulatory preferences in a survey of internal systems auditors representing different national cultures, industries, organizational types and responsibility levels. They found that the regulatory approach adopted by a country was affected by cultural values (as defined by Hofstede 1991) as well as by the concerns for information privacy expressed within the population. This research pre-dated significant changes in privacy regulation in the EU, Canada and the US (from whence the majority of the survey sample was drawn).

Blodgett, Ly, Rose and Scott (2001) studied the impact of national culture on ethical sensitivity in a study of American and Taiwanese sales agents. The dimensions examined in the study were based on Hofstede's (1980, 1991) cultural diversity measures[2], specifically: (1) power distance, (2) uncertainty avoidance, (3) individualism versus collectivism, (4) masculinity versus femininity, and (5) long- versus short-term orientation. The focus of the study was the identification of the differences in ethical sensitivity to different stakeholders – colleagues, the

---

[2]The original four dimensions of national culture are defined as follows:

a) Power distance – The extent to which there is an acceptance of an inequality of power between individuals within a given culture.
b) Uncertainty avoidance – The extent to which the unknown represents a threat to cultural members.
c) Individualism versus collectivism – The extent to which cultural members are concerned only for themselves and their immediate families (individualism) or are more concerned for a larger social group which protects them in exchange for member loyalty.
d) Masculinity versus femininity - The social norms in which there are defined gender roles. In masculine cultures, men are supposed to be behave aggressively and toughly and be concerned mostly with material pursuits, while women are supposed to be modest and tender and concerned mostly with the quality of life. In feminine cultures, men and women both pursue quality of life over material possessions as a definition of success.

An additional dimension was added after the original four dimensions were defined in Hofstede's initial studies:

e) Long-term versus short-term orientation – The temporal orientations in which cultural members seek future rewards through behaviours that emphasize thrift and perseverance (long-term) while short-term orientations are concerned with past or present actions. Cultural members emphasize behaviours that respect tradition and comply with socially-defined obligations.

company, competitors and customers. Of importance to my research is the finding that while both nationalities were equally sensitive to customer interests, they differed in their sensitivity to the interests of the company, competitors and colleagues. These findings suggest that the national culture of organizational members influences the firm's priorities when weighing the interests of competing stakeholders.

A different study suggests that national culture may not be a useful approach to understanding ethical behavior. Singhapakdi, Marta, Rao and Cicic (2001) compared the responses of American and Australian marketers to a series of marketing ethics scenarios. Australian and American culture are very similar according to Hofstede's national culture typologies and, therefore, one would have expected very similar responses to ethical scenarios. Instead, the study revealed that in the comparison of the contribution of different moral philosophies – idealism and relativism – there were significant differences between the two groups of marketers. Despite finding a similarity between corporate ethical values (the groups would agree on whether or not their respective companies behaved ethically), there were marked differences in personal moral philosophies. Australian marketing professionals were significantly more idealistic and relativistic than their American counterparts.

These findings present two important issues for privacy researchers. First, can we continue to rely on existing instruments to adequately capture the role of national culture when investigating its impact on information privacy orientation? Could attitudes about information privacy in themselves require definition along cultural lines? How do we determine the ethical stance represented by a national culture? Caudill and Murphy (2000:16) theorize an Ethical Responsibility Continuum as a way to map seven different ethical theories to privacy policies at the corporate and public policy levels (US and EU). It would be interesting to extend this to an empirical examination of the privacy regulatory environment in other countries. Second, if information privacy attitudes within different jurisdictions are culturally-based, what then ought

to be the response of global enterprises operating across multiple jurisdictions? And how should competing ethical stances (perhaps reflected within national cultures) be reconciled?

Regulatory Environment

The regulatory environment varies considerably across nations, and is particularly important when dealing with issues such as information privacy (Milberg et al. 2000). Bennett (1992) proposed a typology of privacy regimes based upon the extent to which government intrudes into whether and how firms manage information privacy. The typology spans a spectrum from lower involvement (Self Help, Voluntary Control) through to medium involvement (Data Commissioner) to higher involvement (Registration, Licensing).

The need for the largely "self help, voluntary control" jurisdictions, such as the USA, to create special responses to foreign privacy initiatives[3] indicates that the regulatory environment acts as an important impetus for organizational action by firms. Walczuch and Steeghs (2001) demonstrated that complying with the EU Directive was of greater or lesser difficulty and expense for affected firms in different countries. Interviews were conducted with the personnel responsible for implementing data protection legislation in 23 multinationals located in Europe. The results indicated that German-based firms (which were used to working within a rigorous national privacy regime) found implementing the EU Directive easier and less costly than firms based in countries that had a weaker or no privacy regime prior to the EU Directive.

Smith's (1993) research into the US circumstances of the late 1980s (voluntary control) found that none of the seven firms in his study was proactive in adopting information privacy policies and that there was no internally derived reason to do so. Rather, all firms experienced a period of "drift" during which time the absence of an explicit legislated privacy framework permitted unfocussed – and in some cases abusive – treatment of customer information. Industries responded differentially to the threat of legislative action. Firms that were not threatened by

[3] For example, the development of "Safe Harbor" designations for the US firms in response to the European Data Directive.

potential legislative action seemed to ignore a growing consumer trend towards a preference for individual information privacy. This would seem to suggest that firms will only respond to government threats to intervene. But, if this is indeed the case, firms within any single jurisdiction would have identical attitudes and behaviors with regard to the treatment of personal information. This is far from true, as witnessed by the variance in US firms' conduct. Some US firms are working at least to appear "privacy friendly" and 391 have voluntarily entered the US Department of Commerce's "Safe Harbor" in order to comply with the European Union's much tougher privacy standards (DOC 2003). Others are exploiting their clients' personal information (FTC 2003).

Canada has a more specific and stricter information privacy regulatory environment than does the US. The passage of PIPEDA required action by all Canadian firms in three waves of compliance. The first wave required all firms designated as "federal works" (that is firms subject to regulation by the federal government) to comply with the federal privacy legislation on January 1, 2001. This first wave included *inter alia* federally chartered financial institutions (banks, insurance companies, provincial credit union centrals), transportation companies (airlines, inter-provincial trucking, railways), and firms engaged in inter-provincial trade and commerce (Perrin, Black, Flaherty and Rankin 2001). The second wave, effective January 2002, applied to the personal health information collected and used by the organizations subject to the organizations already required to comply with the law. The third wave, effective January 1, 2004, required all other commercial enterprises to comply either with the federal statute or substantively equivalent provincial legislation.[4]

With the implementation of PIPEDA in Canada, we can observe compliance variance within and across industries. While other firms will have to comply eventually, some are responding to this challenge well in advance of the legal requirements. The point is that in all

[4] Quebec has had private sector privacy legislation since 1993. This legislation has been deemed substantively equivalent since the time of the initial promulgation of the federal PIPEDA.

three regulatory circumstances – pre-PIPEDA, first wave PIPEDA compliance and second wave PIPEDA compliance – we can observe differences in firms' privacy behaviors. The question is, why are there differences? What has been impact of the different regulatory environments on these behaviors?

Industry Practice

Smith (1995:90) argued that "industry practice" was a valid "benchmark ...for evaluating marketing practices [as] business norms." This echoes Berger and Luckman's (1971) contention that, over time, industries develop a set of common understandings or expectations of how things are done. The extent to which firms observe and replicate the practices of others is well documented (DiMaggio and Powell 1983; Scott 1987).

Dobbin et al.'s (1993) and Edelman's (1992) examinations of collective responses to legislation in the US are particularly instructive. These studies demonstrated the tendency of organizations to respond to new demands by altering organizational structures to implement new initiatives. A comprehensive privacy survey carried out in 1992 (Equifax 1992) found that organizations were unwilling to implement information privacy policies in the absence of a clear industry consensus. This sentiment was echoed by many of the managers interviewed by Smith (1993).

Similarly, the influence of memberships in trade associations and other business organizations would be expected to influence a firm's information privacy orientation. The environmental literature suggests that the adoption of voluntary codes of conduct is influenced by industry membership. Prakash (2000) employed the lenses of club theory, stakeholder theory, institutional theory and corporate social performance to examine the adoption of the Responsible Care Program by members of the Chemical Manufacturers' Association (CMA). This case study demonstrated the importance of membership within a trade association for the dissemination of new environmental practices within individual firms (adherence to the six codes of conduct under

the program) as well as the establishment of new communication and knowledge transfer practices across the industry.

The role that industry practice plays in the formation of a firm's information privacy orientation has not been explored. I contend that there will be important industry effects contributing to the formation of information privacy orientation. In particular, the role that leading firms play, both within their industry associations and as overall business leaders, to characterize and shape the debate over information privacy is likely to be important.

In summary, I argue that national culture, regulatory environment, and industry practices are important antecedent external variables to the development of a firm's information privacy orientation. However, the relative strength of these variables requires examination, as does the extent to which these variables interact.

Antecedent Internal Variables:
Factors that Support the Economic Goals of the Firm

The proposed internal variables are divided into two groups. The first group of variables comprises those that support the economic mission of the firm – strategic positioning, market orientation, and availability of slack resources. The second group is composed of those variables that are involved with other, non-economic, aspects of the firm including organizational culture, ethical climate, interfunctional values and top management team preferences. These variables are discussed below.

Strategic Positioning

It is anticipated that a firm's strategic positioning will significantly affect its privacy orientation given that strategy can be considered a guide to managerial decision-making, including resource allocation (Bower 1970) and priority setting (Mintzberg 1998). Porter (1985) proposed a basic typology of strategies that have become a generally accepted nomenclature for

distinguishing how firms compete. A cost leadership strategy is internally focused and emphasizes activities to reduce costs across the organization, while a differentiation strategy is more externally oriented and emphasizes tailoring products and services to customer needs. Porter's focus strategy is a hybrid in that it obliges an organization to select a segment to serve and then to align internal resources to pursue either cost leadership or differentiation. Miles and Snow's (1978) typology of strategic orientations (defenders, analysts and prospectors) reflects Porter's generic strategies to the extent that defenders tend to seek rents by minimizing costs, analyzers operate as fast second entrants into emerging markets and prospectors lead their industries in the discovery, development and deployment of new products and services that often redefine competition within the industry. The strategic orientation typology has been used to demonstrate how firms, for example, differ in their IT deployment (Sabherwhal and Chan 2001).

Similarly, I would expect that defenders, analyzers and prospectors would employ different logics in developing their information privacy orientations. Empirical evidence supports the suggestion that prospector firms, by "placing greater strategic emphasis on product-market development than on domain defense" will engage privacy through "externally rather than internally derived actions" (Chattopadhyay, Glick and Huber 2001). Furthermore, Aragón-Correa (1998) demonstrated that prospector firms were more likely to incorporate pollution prevention strategies than other strategic types. I suggest that defender firms would not engage in privacy behaviors beyond meeting basic legal requirements in order to minimize adding to their costs. Analyzers would be more likely to imitate privacy behaviors if leading firms were so engaged or if the analyzer firms could initiate a niche strategy by engaging privacy behaviors. Lastly, prospector firms could either pursue enhanced privacy behaviors or not depending on how they conceptualized the basis for their leadership position. The question is how and to what extent would their current or future position be undermined by not engaging in privacy behaviors?

Market Orientation

Kohli and Jaworski's (1990) initial conceptualization of market orientation focused on the organization-wide gathering, disseminating, and responding to customer information. Clearly, this places market orientation as a central concern to our understanding of the development of a firm's information privacy orientation. An alternate perspective is offered by Narver and Slater (1990) who characterize market orientation as a type of culture — a culture that creates behaviors resulting in superior value for customers. Market orientation's behavioral dimensions (customer, competitor, inter-functional co-ordination), and decision criteria (role of time and profit motivation), are particularly relevant to my model. I expect to find that market orientation contributes fundamentally to the formation of a firm's customer relationship stance, and, hence, its information privacy orientation. In addition, market orientation may offer an important source for variation among firms given that the construct "can be viewed as ... continuous" in that organizations will exhibit different degrees of market orientation based on the extent to which they engage the "different ... activities associated with market orientation" (Kumar, Subramanian and Yauger 1998:204).

I am unaware of any studies that have linked market orientation to privacy practices. Furthermore, I suggest that the effects of market orientation may be equivocal. The literature establishes that different customers have different privacy needs and therefore, the collection, use and reuse of customer information, as a part of the market orientation intelligence gathering activity, will need to reflect this concern. Kumar et al. (1998) argue that a market oriented firm understands that there are several alternatives available to them to satisfy customer needs and deliver superior customer value. In other words, not engaging in privacy violating behaviors may constitute as legitimate an expression of market orientation as does extensive customer profiling based on intrusive data collection practices. In industries where customers have high privacy concerns, organizations with high levels of market orientation will be sensitive to this concern

and are likely to have stronger privacy orientations. However, if customer concern for privacy appears ambivalent or low, firms with high market orientation may focus on the outcomes of having more complete information to better serve customers or overcome their competitors. This focus may lead them to adopt a weaker information privacy orientation. Thus, while I suggest that market orientation is linked to information privacy orientation, the type and direction of the linkage is ambiguous.

Availability of Slack Resources

Firms are also expected to evaluate how they respond to privacy pressures based on the availability of slack resources. Slack resources are defined as "the supply of uncommitted resources" (Cyert and March 1963:54) and as the "pool of resources in an organization that is in excess of the minimum necessary to produce a given level of organizational output" that is usually measured "using standard financial data reported for a firm as a whole" (Nohria and Gulati 1996:1246, 1252.) The availability of slack resources assists firms to cope with environmental jolts (Meyer 1982) and to support innovation, experimentation and risk-taking (March 1991). Importantly, the availability of slack resources is in the eye of the managers who control how resources are used in firms.

I borrow from the corporate environmentalism ("green") literature to illustrate the potential effect of this variable on information privacy orientation. Bowen (2002) showed how the perception of the availability of slack resources affected organizational decisions to pursue more or less costly and disruptive environmental initiatives. Bowen distinguished between the availability of financial and non-financial slack and showed how the two forms of slack differentially affected firm environmental activity. The unavailability of slack caused firms to engage in either materials reduction strategies (i.e., recycling programs) or "buffering" activities (similar to Oliver's decoupling approach).These behaviors could be seen as the equivalent of non or minimal compliance – that is, weak privacy orientation. The availability of either financial

slack or non-financial slack (such as managerial time) contributed to the development of new environmental initiatives, including new technology developments or engagement with stakeholders. In other words, the availability of slack provides firms with the choice of whether or not to engage new initiatives. In information privacy orientation terms, this translates to a range of orientation strengths from minimal (the firm chooses to use slack for other purposes) to strong (the firm chooses to invest in information privacy initiatives).

I would expect that firms that have experienced poor economic performance would be less likely to display high privacy orientation than firms with positive economic performance. Poor economic performance would lead firms to have fewer available resources for experimentation. As a result, these firms would either not comply with legislative requirements or would comply minimally, thus displaying a weak privacy orientation at best. On the other hand, firms with available slack resources gained from good economic performance would at least have the option of choosing to apply some of their slack resources to the pursuit of higher information privacy orientation if they perceived a benefit would accrue from the higher levels of behavior (for example, achieving greater social capital).

In summary, I argue that variables that operate in support of a firm's economic mission (strategic orientation, market orientation, and availability of slack resources) are important antecedent internal variables to the development of a firm's information privacy orientation. However, the relative strength of these variables requires examination as well as the extent to which these variables interact.

In the next section of this chapter, I discuss the variables that support the achievement of other firm objectives and their relationships to the development of information privacy orientation.

Antecedent Internal Variables:

Factors that Support Non-Economic Goals of the Firm

I argue that there are four additional Antecedent Internal Variables that influence the development of a firm's Information Privacy Orientation. These variables (organizational culture, ethical climate, interfunctional values, and top management team preferences) are distinguished by their role in supporting a firm's broader, not necessarily economic, goals.

Organizational Culture

Organizational culture can be defined as the symbols, language, narratives, practices (Trice and Beyer 1993) and values (Hofstede et al. 1990) that define "how things are done" (Pheysey 1993) in particular organizations. Organizational culture has long been recognized as a factor influencing the sense-making, decision-making and behaviors of people working in organizations (Akaah 1993; Ferrell and Skinner 1988; Victor and Cullen 1987). More practically, it can be seen to constitute the acceptable approach to problem solving (Christensen and Gordon 1999).

Hofstede et al.'s (1990) specific investigations into the dimensions of organizational culture revealed six culture dimensions. The first dimension distinguished between concerns for means (process orientation) versus goals (results orientations). The second dimension contrasted concern for people (employee oriented) against concern for the immediate task (job-oriented). The third dimension addressed issues of identification – whether employees derived their identification primarily from the organization (parochial) or from their specific job (professional). The fourth dimension considered the differential effects of the organization's communications climate (after Poole 1985), whether open or closed. The fifth dimension deals with whether there is tight or loose management control about such things as norms for dress and deportment. The final dimension addresses the cultural orientation to customers. Does the organizational culture encourage market-driven behavior (pragmatic) or rule enforcement behavior (normative)? This

latter dimension is particularly interesting for my research given the items included in the survey instrument. These included statements such as the company was "pragmatic, not dogmatic in matters of ethics;" that there was a "major emphasis on meeting customer needs;" and that "results were more important than procedures" (303). These items directly examine issues related to the organization's emphasis on addressing customer concerns, which I argue is an important aspect of information privacy orientation (customer relationship stance layer).

Organizational culture provides a means to examine information privacy formation through an appreciation for "what really matters" in a firm versus a superficial characterization of culture contained in slogans, logos and "successories" art (Kilmann 1985). Hofstede's characteristics as briefly outlined above provide the basic tools for considering what are the larger "character traits" of a firm and how these distinct combinations of traits lead to a "personality" that contributes differentially to the formation of Information Privacy Orientation. Of interest to me would be to research the different contributions to the formation of IPO by firms exhibiting a combination of the dimensions of means, people, organizational affiliation, open communication, tight management control, and normative customer orientation in contrast to those displaying cultures based on goals, tasks, job identification, closed communication, loose management control, and pragmatic customer orientation.

Ethical Climate

Ethical climate is defined as the "shared perceptions of what is ethically correct behavior and how ethical issues should be handled" (Victor and Cullen 1987). The ethical climate construct has been variously described as a unidimensional continuum (Cohen 1995a, 1995b) or as a multidimensional construct (Fritzsche 2000; Weber 1993; Winbush, Shepard and Markham 1997). Victor and Cullen (1987) offered an ethical climate typology based on ethical theory (egoism, utilitarianism, and deontology), ethical standards (self-interest, caring, and principled) and locus of analysis (individual, local and cosmopolitan). This typology has been modified over

time but the existence of multiple ethical climates has been at least partially validated (Fritzsche 2000).[5]

To the extent that information privacy is considered an ethical issue (Caudill and Murphy 2000; Mason 1986; Milne 2000; Laudon 1995) we would expect the strength of information privacy orientation to vary with different ethical climates. Fritzsche (2000) suggests that there are six identifiably different climates. A "caring climate" is characterized by concern for others while an "efficiency" climate emphasizes performance of work as paramount. A "laws and codes" climate emphasizes following externally derived rules, laws and codes of conduct whereas as a "rules and procedures" climate emphasizes internally based modes of operation. An "independence" climate operates on the basis of individuals placing more value on their personal moral beliefs than on organizational norms. Finally, a "company" climate emphasizes concern for the organization (i.e., profitability) over personal ethical beliefs.

The variety in ethical climates is expected to differentially influence the formation of information privacy orientation. Given the multidimensionality of the ethical climate construct, it is difficult to argue for specific relationships between the different climates and information privacy orientation. Similar to market orientation, I suspect that the linkages are ambiguous.

Interfunctional Values

The location of the Information Privacy responsibility within the organization will likely influence the firm's information privacy orientation through two different influence patterns. First is the influence exerted by the norms and values of the responsible occupational group. This speaks to the existence and potential strength of organizational subcultures. While organizations may have an overall culture that most members are aware of and perhaps subscribe to, many also

[5] Winbush et al. (1997) combined ethical climate with Ouchi's (1980) governance typologies (market, bureaucracy, and clans) in a study of employees in a large retail company using the revised 36 item Ethical Climate Questionnaire (ECQ) (Cullen, Victor and Bronson, 1993). Three of the ethical climate factors (law and rules, independence, and instrumental) were strongly supported while a fourth (service) was also in evidence. Fritzsche (2000) studied managers in a high technology firm using a vignette study of ethical decisions as well as a revised version of the ECQ.

have subcultures that lay a greater or lesser claim of loyalty on their members (Trice and Beyer 1993). Subcultures consist of "distinctive clusters of ideologies, cultural forms, and other practices that identifiable groups of people in an organization exhibit" (Trice and Beyer 1993: 174). Second is the influence of the responsible group within the organization as a whole. Different functional areas will exercise different levels of influence over key decisions involving the selection of issues for attention and the deployment of resources that are important to the overall functioning of the overall organization (Day 1997; Homburg, Workman and Krohmer 1999; Pfeffer 1992). Furthermore, these groups have their organizational agendas, interests and needs (March and Simon 1959) that produce a "logic of action" (Bacharach, Bamberger and Sonnenstahl 1996:477). This logic of action is defined as the "implicit relationship between means and ends underlying the specific actions, policies and activities of organizational members" (478). I would expect that the functional unit given responsibility for implementing the firm's privacy initiatives would bring its own particular views and priorities to the issue.

Understanding the functional group responsible for the firm's privacy program is important to this research for three reasons. First, Smith (1993) identified that different functional units experienced the development and implementation of privacy policies in different ways. Second, the different values that are based in the identity of occupational groups might dictate different approaches to handling information privacy issues in the firm. Buenger, Daft, Conlon and Austin (1996) used the Quinn and Rohrbaugh (1983) competing values framework to demonstrate that different units within an organization pursue four sets of competing values simultaneously - control versus flexibility and internal versus external focus. These dimensions are either more or less emphasized in the most likely functional groups to assume responsibility for the firm's information privacy programs – marketing, IT and legal. Third, the relative influence of a particular subunit in an organization has been empirically verified,[6] supporting my

[6] For example, Homburg, Workman and Krohmer (1999) studied the relative influence of marketing departments in firms in three different industry sectors. They found that in addition to "traditional"

contention that the location of the responsibility for the firm's privacy function may be an important signal as to the importance that the firm accords to privacy as an issue requiring attention and resources. This will also likely influence the formation of the firm's information privacy formation.

Top Management Team Preferences

The top management team (TMT), is defined as the Chief Executive Officer and his or her direct reports. The TMT is a form of "dominant coalition" with a key responsibility for setting the firm's strategy and allocating the resources to implement that strategy (Cyert and March 1963). Part of the TMT's strategy-setting mandate involves the identification and selection of the issues most likely to affect the firm's ability to execute its strategy successfully (Hambrick 1989). Strategic decisions are characterized by their degree of complexity (affecting significant aspects of the firm's activities), ambiguity (uncertainty about what the impact is likely to be positively or negatively) and the amount of resources required to address the issue (the greater the resource stake, the more significant the issue) (Mason and Mitroff 1981). The strategic management literature emphasizes the importance of non-economic factors in decision-making by TMTs, characterizing the approach as the "outcome of behavioral factors rather than a mechanical quest for economic optimization" (Hambrick and Mason 1984:194) that are better characterized within a social model of decision-making rather than an economic one (Pfeffer 1997).

The selection by the TMT of information privacy as a strategic issue can be examined from three perspectives. First is the traditional "threats versus opportunities" approach (Jackson and Dutton 1988). In this tradition, a firm distinguishes between an opportunity which is defined as "a *positive* situation in which *gain* is likely and over which [the firm] has a fair amount of *control*" versus a threat which is defined as "a negative situation in which loss is likely and over which [the firm] has little control" (Dutton and Jackson 1987:80 emphasis in the original).

---

concerns (i.e., advertising messages, customer satisfaction measurement), the marketing groups exercised considerable influence in strategic decision-making beyond that of other functional groups.

Chattopadhyay, Glick and Huber's (2001) research has shown that issues categorized as threats are more likely to incite organizational action than were those issues perceived as opportunities. Second, TMTs may categorize the information privacy issue in terms of organizational identity and image. Goia and Thomas (1996) studied issue interpretation among executives in US colleges and universities. They found that the executives interpreted change as issues of identity or image with strategic or political implications. Identity was defined as the "features of the organization that members perceive ostensibly as central, enduring and distinctive in character that contribute to how they define the organization and their identity with it" (372). Image was defined as the "perceptions of how external constituents view the organization" (372). *Strategic* issues were characterized as "identifying and pursuing initiatives that would convey the desired future image" while *political* issues required "managing competing interests and preferences [within the organization]" (373). Thus, strategic issues required external "image" management while political issues called for internal "identity" management.

Third, an innovation can be viewed as any change in "policy, structure, method or process, product or market opportunity" usually requiring sponsorship by top management in order to secure necessary resources and counter internal resistance (Nohria and Gulati 1996:1251). A useful further distinction is Daft's (1978) characterization of innovations as technical or administrative. Technical innovations "pertain to products and services, as well as production processes and operations related to the *central activities of the organization*" while administrative innovations "pertain to changes in the organization structure and the people who populate the organizations" which "originate more in the *peripheral administrative core*" (Bantel and Jackson 1989:108, my emphasis).

The classification of the information privacy issue by top management has interesting implications for my research and raises a few questions. What is the specific threat or opportunity to the firm? Is the issue one of image or identity? What type of losses would the firm be concerned with - financial, informational, or reputational? Do TMTs classify information privacy

as a strategic issue or tactical issue? Would changes be characterized as technical or administrative innovations? And what actions would be attached to the different characterizations?

In summary, I have argued that four antecedent internal environmental variables – organizational culture, ethical climate, interfunctional values and top management team preferences – will influence the formation and strength of a firm's information privacy orientation. In the concluding section of this chapter, I discuss the variables that I propose are the outcomes of a firm's Information Privacy Orientation.

Outcome Variables

If we accept that different organizations will exhibit different information privacy orientations, we can expect that there will be a variety of outcomes, intentional and otherwise, related to these differences. As the study by Earp et al. (2002) suggested, firms may organize their privacy activities to achieve a variety of goals. For example, we could argue that organizations that strive harder to protect customer privacy do so because they believe that they will enjoy greater gains than those that do not expend this effort. These "gains" can be captured as a series of performance measures. Performance measures provide a way to evaluate an organization's success in implementing its strategies (Kaplan and Norton 1996). I suggest that information privacy orientation will contribute to organizational performance, as measured by its social capital, intellectual capital and financial capital. Just as organizations will vary in their information privacy orientations, they will also vary in the emphasis they place on these various outcomes. However, I propose that organizations with the strongest levels of information privacy orientation will have superior long term performance on all three performance measures.

Social Capital

An organization's social capital is defined as its potentially beneficial relationships with external parties (Burt 1992; Coleman 1990) including customers and other stakeholders. Granovetter (1985) stressed that economic action is not independent of the organization's social relationships. In an era of increasing competition between networks, enhancing the scope of an organization's relationships and the knowledge and perspectives gained as a result of these relationships is increasingly important (Gulati, Nohria, and Zaheer 2000). Social capital, also termed relational capital, has been shown to be a source of competitive advantage (Dyer and Singh 1998; Hitt, Dacin, Levitas, Arregele and Borza 2000). I expect two important aspects of a firm's social capital – trust and reputation – would be related to the strength of its information privacy orientation. I argue that information privacy orientation as expressed through the behaviors of firms will affect customer trust and, potentially, distrust in them. Further, with regards to reputation considerations, I expect that a firm's information privacy orientation, as expressed through its privacy behaviors, will form part of a customer's judgment of the firm's social reputation. In addition, I argue that a stronger information privacy orientation will enhance a firm's reputation and should, therefore, lead to stronger relationships with customers and other key stakeholders.

Intellectual Capital

Intellectual capital is a key non-financial performance measure that is indicative of an organization's actual knowledge and its learning capability (Nahapiet and Ghoshal 1998). This ability to gather and use information effectively to learn about new and existing customers, channel members and partners, as well as to leverage this knowledge to drive markets into new forms, may be an organization's only sustainable competitive advantage (Day 2001) or key strategic asset (Deshpandé 2001). Furthermore, Itami (1987) notes that "a superior ability to *acquire, understand and disseminate relevant information* about markets satisfies the conditions

for a true core competency" (my emphasis). Slater and Narver (2000) demonstrated that intelligence gathering that focused on "customers' expressed and latent needs" (121) was associated with delivering superior customer value.

I propose that information privacy orientation supports the development of organizational intellectual capital in three ways. First, respecting customer privacy and following fair information practices legitimizes future requests for additional information and therefore provides customers with a reason to share important information. This enhances organizational ability to acquire appropriate types of information. Second, repeated successful interactions with customers will increase organizational customer knowledge, thereby increasing the understanding of customer needs and wants. Third, attention to privacy issues should create the circumstances in which customers willingly share specific kinds of requested information. This should increase the relevancy of the information provided.

Financial Capital

Traditionally, firm performance measures have primarily reflected an interest in financial results. Key outcomes of interest include profitability, return on assets and return on investment. Sveiby (1997) argues that financial measures remain important to organizations because financial capital is "visible," and that there are well-established rules regarding its calculation and interpretation. These established rules and interpretations assist stakeholders in comparing performance within and across industries. We expect that customers will be more willing to transact business with firms with strong information privacy orientations than with firms with weak information privacy orientations. For example, the Royal Bank claims

> that 7 percent of a customer's buying decision relates to privacy issues. Using that and other assumptions, Mr. Cullen [former Chief Privacy Officer] said RBC's privacy policies were responsible for $700 million worth of consumer banking business. (NYT 2003)

Furthermore, if, as Day (2001) suggests, information competency is a key asset leading to sustainable competitive advantage, financial capital will be enhanced for firms with strong

information privacy orientations.

However, implementing strong privacy policies in organizations will likely result in additional costs. For example, creating a "culture of privacy" might include establishing a senior position with corporate-wide responsibility, training employees, and conducting periodic privacy audits (Culnan and Bies 1999). It might also entail participating in third party assurance programs (Caudill and Murphy 2000), upgrading websites and business processes, and communicating the claim that the organization has a privacy-friendly orientation. These expenditures could be significant, especially for transnational and global firms that have to coordinate privacy policies across jurisdictions and locations. Furthermore, strong privacy policies may require that certain opportunities are forgone (such as not selling customer information and not engaging in alliances with potential partner firms that do not share the same information privacy orientation). Disclosure costs associated with keeping customers informed of the use of their information may also be higher.

In summary, I argue that Information Privacy Orientation contributes to three different firm outcomes – social capital, intellectual capital and financial capital. However, the relative strength of these variables requires examination as well as the extent to which these variables interact.

Chapter Summary

In this chapter, I presented a contingency framework that organizes the variables that I argue comprise the larger organizational context in which Information Privacy Orientation is situated in firms. I discussed the antecedent external variables (national culture, regulatory environment, and industry practices) and the antecedent internal variables. These internal variables were divided into two groups – those that support economic goals (strategic orientation, market orientation, and availability of slack resources) and those that support other firm goals (organizational culture, ethical climate, interfunctional values and top management team

preferences). Finally, I argued that the likely outcomes of the firm's Information Privacy Orientation will be the formation of different types of capital, including social capital (trust and reputation), intellectual capital and financial capital.

I believe that the Information Privacy Orientation Contingency Framework serves as a useful guide to the consideration of the key contextual aspects of the firms that were investigated in the course of this research. While the emphasis of my dissertation was the specific development of the Information Privacy Orientation construct, the framework supports the predictive and nomological validity of my research. The framework helps to situate IPO as an organizational concern. The next chapter addresses specifically the IPO construct that I suggest mediates the relationships between the antecedent and outcome variables in the contingency framework. The IPO was the focal construct of this dissertation research.

CHAPTER FOUR

FOCAL VARIABLE - INFORMATION PRIVACY ORIENTATION

The preceding chapters have addressed some of the broad issues of customer information privacy including a review of selected literature and the introduction of a contingency framework to conceptualize the pressures that likely inform organizational privacy decision-making. In this chapter, I turn my attention to the central issue of my dissertation research - the definition and explication of the focal variable Information Privacy Orientation.

Recall that I defined the **Information Privacy Orientation** (IPO) construct in Chapter One as:

> *The principles, values, decisions rules, policies and desired objectives that organizations adopt to guide them in the collection and use of their customers' personal information* (Greenaway et al. 2002).

I theorize that information privacy orientation will be weaker or stronger based on the relationships among, and variation in, each of its four sub-constructs, namely customer relationship stance, customer information management strategy, customer information privacy philosophy and customer information privacy behaviors. These sub-constructs collectively form IPO and are represented in the IPO Continuum. In the next section, I explain the underpinning of the continuum – Smith's (1995) Marketing Ethics continuum. Then I define and discuss each of the four sub-constructs of Information Privacy Orientation and their organizational ramifications.

Marketing Ethics Continuum

Before explaining the Marketing Ethics continuum, it is appropriate for me to discuss briefly the application of ethical theory to information privacy. In his overview for a special issue of the *Journal of Public Policy and Marketing* devoted to privacy and ethical issues in database and interactive marketing, Milne (2000:3) argues that ethical theories are "useful for explaining

differences in corporate ... business policies." Ethical theories such as Utilitarianism[1], Kantianism[2], and Stakeholder Theory[3] have been applied to customer information privacy (Charters 2002; Foxman and Kilcoyne 1993; Hoffman et al. 1999; Laudon 1995; Smith and Hasnas 1999). Caudill and Murphy (2000) provides a comprehensive review of their applicability.

Social contract theory (Hoffman et al 1999), social exchange theory (Culnan 1995) and the more recently articulated "Integrative Social Contracts Theory" (Dunfee et al. 1999) are particularly useful for considerations of information privacy in two ways. First, these theories argue that social contract obligations are unspecified and, thus, cannot be enforced through legal means (Blau 1964 as quoted in Hoffman et al 1999:133). This suggests that how firms treat customer information privacy can be considered in more than merely legal compliance terms. Second, these theories argue that obligations stem from the conflict that exists between firms and their customers (Hoffman et al 1999). Information privacy, with its concerns for control over the collection and use of personally identifiable information, is characterized as a source of conflict between firms and their customers. The exchange based ethical theories argue that firms make choices about how they manage this conflict.

Consistent with these theories, I contend that organizations choose, consciously or otherwise, whose interests will primarily be served by the capture and use of customers' personal information. This calculation involves making decisions about the fundamental tradeoffs between the interests of the organization and those of its customers. I have adapted the "Marketing Ethics Continuum" developed by Smith (1995) as a foundation for this perspective. Figure 4-1 illustrates the Marketing Ethics Continuum. While Smith did not specifically identify social

---

[1] Utilitarianism is an ethical theory that "considers [the] consequences for everyone affected" by an act and balances the "harm and the good expected to result from [that] act" (Foxman and Kilcoyne 1993:110).
[2] Kantianism is an ethical theory that "individuals should act in a manner that treats other individuals as an end and never as a means only" (Charters 2002:249).
[3] Stakeholder Theory is an ethical theory that argues that "those who have an interest in or are affected by the organization have a stake in its decisions" (Caudill and Murphy 2000:15).

exchange or social contract theory as the ethical underpinning for the continuum, he adopts the language of these ethical theories by characterizing consumer-producer relations as a conflict.

• Producer interests favored • Consumer interests less favored				• Producer interests less favored • Consumer interests more favored
←				→
Caveat Emptor	**Industry Practice**	**Ethics Codes**	**Consumer Sovereignty**	**Caveat Venditor**

Figure 4-1: Marketing Ethics Continuum

(Adapted from N.C. Smith 1995:89)

The poles of Smith's continuum are anchored by different philosophies about whose interests are to be served – those of the producers or the consumers? At one end are firms that follow a "Caveat Emptor" philosophy – it is up to buyers to protect themselves in the marketplace. Producer interests are paramount. At the other extreme are firms that believe "Caveat Venditor" - firms are entirely responsible for consumer well being and must prove the merits of their offerings). In this instance, consumer interests are paramount. Between these extremes lie firms that are guided by Industry Practice, Ethics Codes and Consumer Sovereignty based on a perspective that consumers and firms are jointly responsible for their commercial relationships.

The Information Privacy Orientation Continuum adapts and extends Smith's (1995) marketing ethics continuum in four ways. First, the caveat emptor anchor is expanded to include a perspective that acknowledges that some firms operate in a more predatory mode than merely making buyers fend for themselves. Second, the "Industry Practice" and "Ethics Codes" categories are collapsed into a single category. Third, the continuum is specifically applied to a consideration of information privacy. Fourth, the continuum was theorized as comprising four

layers that conceptualize the producer-consumer tradeoffs in terms of a customer relationship stance and information management strategy that inform an organization's privacy philosophy which, in turn, is manifested in its privacy behaviors. Collectively, these four sub-constructs contribute the vertical logic for the IPO Continuum. Figure 4-2 illustrates the Information Privacy Orientation Continuum.

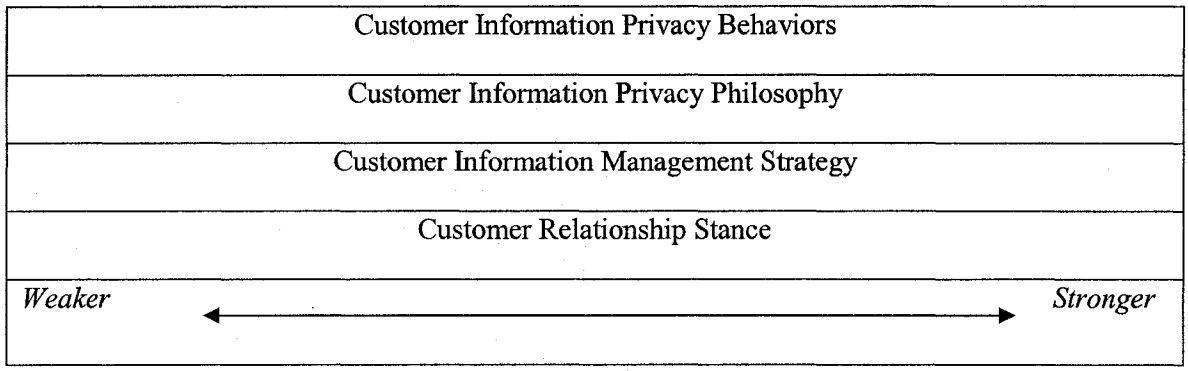


Figure 4-2: Information Privacy Orientation Continuum (Overview)

Note that in the following discussion of the sub-constructs of IPO, there are four strength categories that proceed from left (weaker) to right (stronger). The effect is cumulative across the categories, that is, a firm would not be identified as having a strong privacy orientation if it did not meet the minimum laws or norms applicable to its particular jurisdictional or industry circumstances. These categories form the horizontal logic of the information privacy orientation continuum.

In the next section of this chapter, I will discuss the sub-constructs of Information Privacy Orientation. I begin with the sub-construct Customer Relationship Stance that I argue is the fundamental base upon which an organization shapes its approach to customer information privacy.

Customer Relationship Stance

I define **customer relationship stance** as:

The organizations' predominant characterization of its relationship to its customers based on the definition of its obligations to its customers.

I contend that organizations' customer relationship stances underpin their information privacy orientations. These stances derive from organizations' conceptualizations of the obligations they owe their customers as suggested by Smith (1995). The four categories of Customer Relationship Stance that I theorize exist across organizations are illustrated in Figure 4-3. A firm's customer relationship stance may contribute to a weaker or stronger IPO based on its desire to exploit or assist its customers.

Buyer Exploitation	Buyer self-protection	Shared Responsibility	Consumer Well-being
Organization exists to exploit its customers	Customers are obligated to protect themselves in transactions with the organization	Organization and customers share responsibility for consumer well-being	Organization is obligated to promote consumer well-being
Weaker ◄——————————————————————► *Stronger*			

Figure 4-3: Customer Relationship Stance

Buyer Exploitation

The extreme left end of the continuum is occupied by organizations that believe customers exist solely to be exploited. The tradeoff made here completely favors organizational interests. Organizations assume and exploit an information asymmetry – customers are not necessarily aware that they are being exploited. This is a weak position on the IPO continuum because it suggests that customer information can be used without regard for customer preferences. This represents a violation of every tenet of information privacy that has been previously discussed such as Fair Information Principles. For example, the "notice" principle requires that customers are advised of corporate practices regardless of whether or not the practices would be considered privacy beneficial to customers.

Buyer Self-Protection

This stance conceptualizes the tradeoff between firms and customers as one in which organizational interests remain paramount but also in which customers are seen to be ultimately responsible for protecting themselves in the marketplace. This tradeoff assumes that customers have some knowledge that they need to protect themselves and that they are in a position to do so. However, organizations continue to exploit information asymmetries, justifying their behaviors by invoking the nostrum of "buyer beware." Again, this represents a weak privacy position although somewhat stronger than the buyer exploitation position. At least the buyer self protection position acknowledges, in however limited fashion, that customers have some interest in protecting their privacy. As well, customers will have some "negative power" in that they can withdraw from the marketplace. The weakness of the position, similar to the previous one, is that customers are left on their own to protect their personal information. Both the buyer exploitation and buyer self protection positions represent "relationships" in which firms assume power, and abuse it, by emphasizing their interests over those of their customers.

Shared Responsibility

This stance characterizes the commercial relationship as one of mutual interest and obligation. Tradeoffs do not favor one group over another but are played out in a model of mutual adjustment. Organizations believe they and their consumers bear a joint responsibility for marketplace behavior. Attempts will be made by organizations to bridge information gaps but with the recognition that customers will seek their own answers. This position represents a stronger IPO than the previous two positions for the following reasons. First, this position acknowledges specifically that there is a power relationship between firms and their customers and that firms should take care to ensure that customers are able to participate in the marketplace not simply be exploited by that marketplace (Caudill and Murphy 2000; Hoffman et al. 1999). Second, the position argues for customer ability to exercise agency. Customers are not merely

targets for exploitation but carriers of information that firms value. Customers have more "positive" power because they can negotiate, at least to some extent, the terms of access to and use of their information.

Consumer Well-Being

At the extreme right end of the continuum are organizations that believe consumer well-being is paramount. Tradeoffs are made in the interests of the customer over the organization. In other words, organizations explicitly work to promote consumer well being even if this means they "leave money on the table." I argue that this position represents the strongest IPO for two reasons. First, this position permits customers to exert positive power (make personal information disclosure choices with full information). Second, firms assist their customers by not pursuing privacy violating activities in the first place and by anticipating customer information privacy preferences in the design and development of customer facing activities.

Customer Information Management Strategy

I define **customer information management strategy** as:

The organization's predominant strategy with respect to its objectives for gathering and using customer information.

A firm's information management strategy may contribute to a weaker or stronger IPO based on whether the firm is attempting to manage information or to manage with information.

Information is the lifeblood of organizations and customer information is of particular value (Day 2001; Deshpandé 2001; Itami 1987). Most organizations have an approach to their "information resource" that is more or less explicit and more or less supports their activities (Marchand 1998). The information management strategy sub-construct addresses the fundamental organizational question "what do we want to do with the information we gather?" (Davenport and Prusak 1997:xii). This question is particularly relevant when considering the collection, use and reuse of customer information. What is the main focus of the use to which organizations put the

vast amount of transactional and personally identifying information they collect about their customers?

I adapted Marchand's (1998) characterization of the strategic uses of information in the pursuit of business value to the information management strategy layer of the IPO Continuum. Note that Marchand (1998:6) created a strategic information alignment (SIA) framework (Figure 4-4) to assist firms to map the relative emphasis placed on the four different approaches to "using information for business advantage" (232).[4] I have adapted the SIA framework by considering each of these approaches as individual information management strategies occupying discrete positions on the Information Privacy Orientation continuum.

I recognize the intuitive validity of Marchand's approach which underscores that firms pursue these different strategies simultaneously, and to greater or lesser degrees, depending on their business strategies. However, I argue that the treatment of customer information can be characterized according to a *predominant* information management strategy that answers Davenport and Prusak's fundamental question. Note also that I adopt Marchand's (1998:23) distinctions between "management *of* information" strategies (reduce costs, minimize risk) and "management *with* information" strategies (add value, create new reality). Figure 4-5 summarizes this layer of the continuum.

[4] Firms complete surveys to establish an information management profile (where 1 = weak to non-existent practices in support of a strategy and 7 = the strategy as a key focus of organizational activity) based on the relative importance of each strategy to their businesses (233). This diagnostic tool was developed by Marchand to use in a large sample survey of the information strategies of leading European firms.

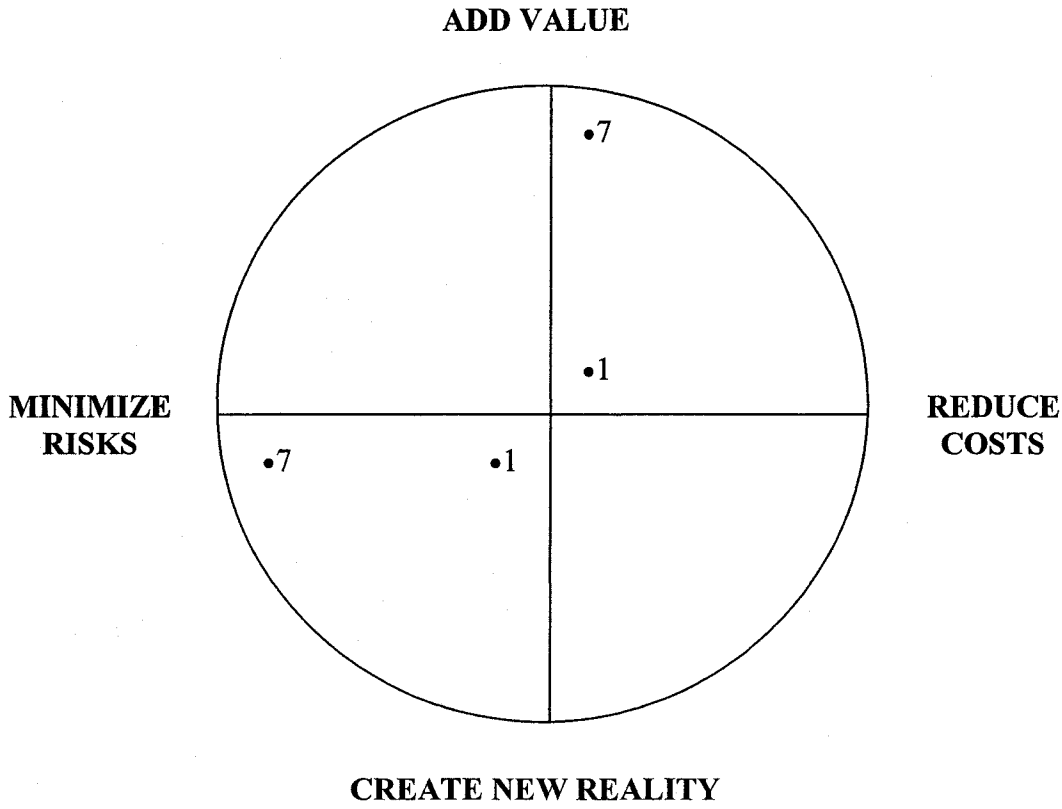


Figure 4-4: Strategic Information Alignment (SIA) Framework

(Adapted from Marchand 1998:232)

Management of information strategies *Management with information strategies*

Reduce Costs	Minimize Risks	Add Value	Create new reality
Information is managed to reduce operational costs	Information is managed to minimize *inter alia* market, legal, and security risks	Organizations use information to add value to products and services	Organizations use information to innovate products and services
Weaker ⟷ *Stronger*			

Figure 4-5: Customer Information Management Strategy

Reduce Costs

Most firms desire to be cost efficient but not all firms have this as the main objective for their information management strategy. I argue that firms on the extreme left hand of the information privacy orientation continuum view customer information as a resource owned by the firm with its primary value as a means to achieving operational efficiency in business processes. A cost reduction approach to customer information would dictate that firms gather all the information they can on customers in order to better target their marketing offers, thus reducing waste in their operations. Greater customer information could also assist firms to better "mass customize" their customer operations which could lower the costs both to produce products and to service customers. A cost reduction focused information management strategy represents a weak information privacy orientation for four reasons. First, the organization's focus is on its own needs and not necessarily those of its customers. Cost focused firms would be likely to interpret incorporating privacy considerations into their information resource strategies as an imposition that would result in little direct benefit to them. Second, customer privacy preferences would be seen to impose costs (Caudill and Murphy 2000; Culnan and Bies 1999) that the firm would prefer to avoid. Third, privacy considerations could also be seen as costly because they may prevent the firm from behaving in cost efficient ways. For example, having to request consent to gather and to reuse information imposes privacy-based operating costs that firms may not be able to recover. Fourth, these firms would be the least likely to expend resources educating themselves or their customers about information privacy. Rather these firms would be more likely to exploit their customers' ignorance of the firms' information management strategy and its implications for their information privacy. In other words, information privacy would not be seen as a desirable means of achieving cost reduction goals and therefore privacy considerations would not be readily incorporated into these firms' information management strategies.

Minimize Risks

Risk management is a traditional concern of most firms (Hamilton 1998) and a particular theme in the privacy literature (Bordoloi et al. 1996; Srivatava & Mock 2000). With this information management strategy, the different functional areas of the firm gather and use information to protect the firm from various categories of risks. For example, a Treasury department functions to "risk manage" investment exposure while an Accounting department uses information to account for and protect against mismanagement of a firm's assets. I argue that there are several different kinds of risks involved with customer information. First, there is *market risk* which can be characterized as the risks involved with not gathering sufficient customer information or of gathering information of insufficient value for effective decision-making thus rendering the firm vulnerable to customer churn and market share losses. *Legal risk* includes the risk of regulatory action stemming either from not complying with various statutes to protect privacy (such as PIPEDA) or, paradoxically, not complying with "legal privacy violation" requirements to report on certain types of financial transactions (such as money laundering statutes). Customer information also involves *security risks* including the risk of firms' systems being hacked by outsiders and customers' information being stolen, or unauthorized employees accessing customer files for inappropriate activities.

A risk management focused information management strategy represents a relatively weak information privacy orientation. Similar to the cost reduction focus, a risk management focus emphasizes the firms' needs over those of their customers. Second, a risk management approach tends to be a fragmented not an integrated strategy relying on different functions to concern themselves with managing the risks as they see them. This could lead to organizations not adopting a consistent, enterprise-wide approach to managing customers' information which would increase the likelihood of privacy violations. Third, a risk management focus concerned primarily with security (i.e., secure socket layers, separate servers, encryption, etc.) is a necessary

but insufficient approach to information privacy. Firms can have very secure systems and violate their customers' privacy if they neglect to implement the important policies that can guide the collection and use of personally identifiable information.

Despite these concerns, the risk management information management strategy represents a stronger position on the information privacy orientation continuum than does the cost reduction position in two important ways. First, firms in this position are more likely to regard the implementation of privacy measures more as a legitimate risk mitigation investment rather than an imposed cost. This argues for a greater willingness to consider incorporating privacy into their information management strategies. Second, even if information privacy is construed more as a security issue requiring a technological solution rather than a customer preference issue requiring broader organizational attention, this demonstrates some limited concern for customer privacy as part of an information management strategy. For example, investments to secure customer information as a risk management tool to prevent identity theft moves these organizations into a somewhat stronger information privacy orientation than firms that might not make these investments in order to maximize cost reductions.

Add Value

The add value strategy emphasizes the use of detailed customer information to better serve customers and, thereby, increase their satisfaction with the firms with which they do business. Increased customer satisfaction is accomplished by collecting detailed customer information in order to tailor service delivery to customer requirements, providing customer feedback opportunities and acting on the information, and by setting and meeting high customer service standards (Horovitz 1998:41).

This strategy occupies a stronger position on the information privacy orientation continuum for two primary reasons. First, an add value strategy focuses on discovering and satisfying customer preferences including their stated likes and dislikes through the deployment

of information systems for detailed information collection. Presumably customer privacy preferences are included in this exercise as they may constitute an important customer concern. Second, the strategy requires a disciplined approach to information collection and use to achieve specific purposes, both organizational (improve service delivery) and customer-focused (improve customer satisfaction). For example, firms operating with this information resource are challenged to maintain accurate (correct and timely) information on their customers. The application of fair information principles, with their emphasis on accuracy and consent, would be a useful approach for firms pursuing a value-add information management strategy.

Create New Reality

This information management strategy represents firms' desires to use information, such as competitive intelligence on social and political trends, or detailed customer information, to "innovate or create new realities – [to] attract new customers, invent new products, provide different services and use emerging technologies" (Marchand 1998:27). This approach is adopted by firms that seek to use information as a strategic differentiator. Not only do these firms seek to maximize customer satisfaction through the use of detailed customer information (as in the add value information management strategy) but they attempt to integrate information management across their organizations and effectively deploy supporting technologies. Information privacy challenges firms using a create new reality approach to differentiate by operating both *within* the constraints imposed by social norms or legislation as well as *beyond* what competitors offer in terms of privacy safeguards including privacy policies and technologies.

The create new reality information management strategy represents the strongest information privacy orientation for three reasons. First, the emphasis on scanning the environment for intelligence on social and political trends suggests that these organizations have an awareness that extends beyond their immediate concerns into the future. Forward-looking, externally focused firms use information to differentiate for innovation rather than to merely

support ongoing business processes (Marchand 1998:11). Understanding what information to collect (and not to collect), organizing the firm to appropriately gather and share the information, and analyzing and applying the information for its intended and declared purposes is not only the best process for innovating with information (Deschamps 1998), but it describes a strong discipline for privacy based innovation (Cavoukian and Hamilton 2003; Heart and Stroke Foundation 2003; Wright 2003).

Second, the use of technology to assist customers with their information needs with respect to buying, obtaining service or adapting their use of products or services to evolving needs (Horovitz 1998:57) can be a powerful source of differentiation. Technology can assist customers to manage their privacy preferences and not simply rely on the firms' word that they are protected. Third, firms can differentiate by proactively addressing privacy issues in order to translate customer satisfaction (the goal of the add-value strategy) to customer loyalty. By anticipating concerns and educating customers about information privacy, by opening the privacy conversation itself and not waiting for customers to ask, by clearly articulating the organization's privacy position and practices, and by offering customer driven privacy solutions, a small number of firms may be able to claim a differentiated position based on their information management strategy.

Customer Information Privacy Philosophy

I define **customer information privacy philosophy** as:

> *The organization's predominant philosophy about the role and impact that customer information privacy norms and laws have on the firm's ability to carry out its business.*

A firm's customer information privacy philosophy will contribute to a weaker or stronger IPO based on the extent to which customer information privacy norms and laws are viewed as a constraint or opportunity for the business.

I contend that organizations have customer information privacy philosophies, explicit or implicit, and that these philosophies are informed by both their customer relationship stances and their information management strategies. These privacy philosophies are anchored at four points on the information privacy orientation continuum as illustrated in Figure 4-6 and explained below.

Privacy Ignored	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
Firms lack awareness or concern for privacy laws or norms	Privacy laws/norms viewed as constraint on ability to maximize shareholder value	Privacy laws/norms viewed as necessary to ensure ongoing transactions with customers	Privacy regime within firm as platform for strategic differentiation
Weaker ◄——————————————————————► *Stronger*			

Figure 4-6: Customer Information Privacy Philosophy

Privacy Ignored

This philosophy anchors the continuum at the left. Organizations that exist simply to exploit their customers are unlikely to be aware of or care that there are norms or rules about customer information privacy. Their philosophy will be that privacy is something to be ignored or that it is too difficult to provide to be worth the effort. These firms certainly would not see customer information privacy as an opportunity. An illustration of this privacy philosophy is the statement made in 1999 by Scott McNealy, CEO of Sun Microsystems, to the effect that "You have no privacy. Get over it." This is the weakest customer information privacy philosophy simply because it fails to acknowledge growing social and regulatory realities – privacy matters to customers, is being legislated by governments (or self-regulated), and there are expectations that organizations must meet to be considered legitimate in the marketplace. As I indicated in Chapter Two, customers are concerned about the privacy of their personal information and they are making these concerns felt in the legislature and in the marketplace.

Privacy as Constraint

Organizations occupying this position view their customers as shouldering the entire responsibility for protecting their privacy interests. These organizations would engage in rhetoric that reflects an overriding concern for shareholder value as the dominant legitimate outcome for firm activities (Friedman 1970) while ignoring other stakeholder groups as legitimate claimants for organizational concern. Privacy norms or legislation would be viewed as limitations on organizational freedom of activity. An example of this privacy philosophy is the position adopted by the Canadian Federation of Independent Business (CFIB) in its submission commenting on the proposed Ontario private sector privacy legislation. The CFIB argued that "Consumers who may feel that their information is not used in an appropriate way always have the option of voting with their feet." (CFIB 2002)

This is a modestly stronger position on the IPO for two reasons. First, the position acknowledges that there are constraints on organizational information activities. Firms are not entirely free to engage in activities without regard for their customers. Second, as a result of acknowledging the constraints, firms will likely curb information privacy violating activities to avoid action by organizations or persons that could damage the firms' reputation with key audiences. However, this remains a relatively weak position because it does not give priority to customers who, it can be argued, "own" the information that the firms want to use in order to make their profits and satisfy their shareholders.

Privacy as an Exchange

This position invokes social exchange theory (Homans 1961) and is anchored by the Joint Responsibility ethical stance at the center of the continuum. In this position, customers knowingly provide personal information to complete transactions so that organizations will use the data to better tailor products and services (the add value information strategy). I would expect these organizations to claim to balance shareholder and customer interests. Privacy norms or laws may

be viewed by these organizations as necessary vehicles for the facilitation of transactions. An example of this privacy philosophy is the position adopted by the Canadian Marketing Association (CMA),

> In 1993, CMA was one of the first major business associations to impose a mandatory Privacy Code on its membership. The primary purpose of the Association's Code is to give consumers control of their personal information and to make the process of gathering and using customer information by marketers more transparent (CMA 2002).

This represents stronger IPO for two reasons. First, it acknowledges that customers have information and that the information is owned by and ought to be controlled by customers. Customers should also derive some benefit from disclosing this information. Second, the information is acknowledged to be of value to organizations (otherwise, why bother to collect it) rather than pretending otherwise. However, this value is mutually beneficial – the gathering organization can use the information to provide products and services that better respond to customer preferences and, it is hoped, sell more products and services. Customers receive better value from gaining access to goods and services that better address their needs and wants. For many companies, this customer information privacy philosophy position is as strong as it need be, especially if they are dealing with information that is considered less sensitive (i.e., not financial or medical information). However, this is not the strongest position as it does not place customers at the top of the priority list as is done by firms occupying the last category of this customer information privacy philosophy.

Privacy as Opportunity

The other extreme of the continuum is reflected by organizations seeking to fulfill mixed obligations to a variety of stakeholders but that view customers as paramount in the overall calculus, and whose information strategy is to create new realities through innovative products and services. Privacy norms or laws would be viewed as the platform from which firms could both promote customer well-being but also potentially differentiate themselves from competitors that have a more constrained privacy philosophy. I would expect that this philosophy would be

adopted by organizations who regard information privacy as a key enabler of a network of complex relationships over time. This philosophy appears to be exemplified by the Royal Bank of Canada. Their former Chief Privacy Officer indicated in a presentation at the Privacy 2001 Conference (Columbus, Ohio) that privacy was part of the firm's business strategy and that the regulatory requirements were only the starting point for privacy in the firm. The PowerPoint Slide illustrating this strategic posture appears as Figure 4-7. Note that "Regulatory/Legislation" is coupled with the "10 Principles of Privacy" and "RBFG Privacy Policies" as the base of the strategic pyramid. "Customer preference and choice" was the next layer and "Differentiation" formed the peak.

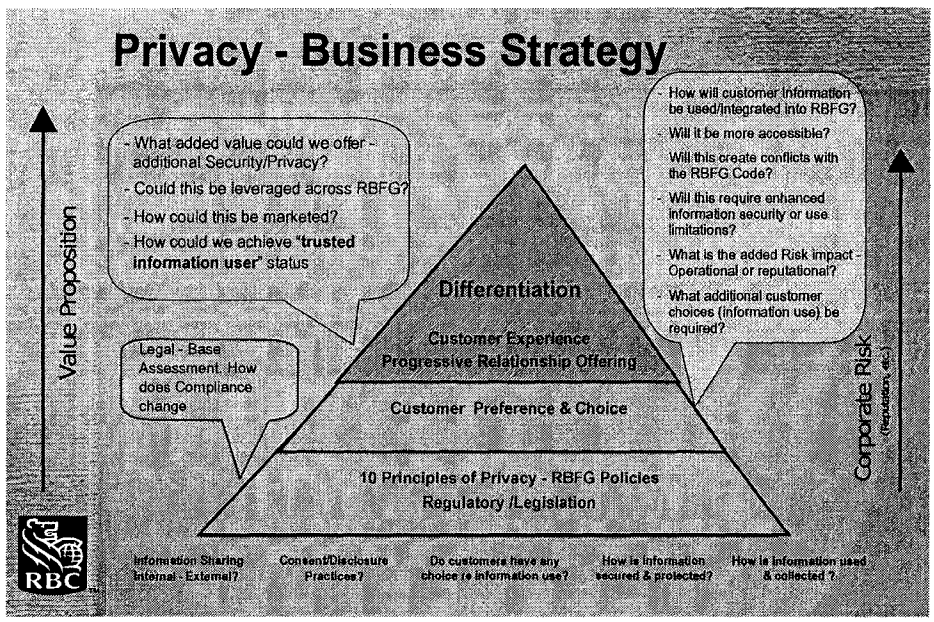


Figure 4-7: Royal Bank Financial Group – Privacy as Business Strategy

"Privacy as opportunity" is arguably the strongest category on this layer of the IPO continuum. However, and as with the other extreme right hand positions, I would expect few firms to attempt to operate in this manner. It is likely difficult and costly to build privacy into a firm's operations to the extent that this philosophy demands and for many firms, this would be an unnecessary goal.

Customer Information Privacy Behaviors

I define **customer information privacy behaviors** as:

The organization's publicly visible and internal information privacy activities.

A firm's privacy behaviors both contribute to and reflect a weaker or stronger IPO based on the extent to which behaviors affect its customers' abilities to exercise control over their personal information and be treated fairly by the organization as it collects and uses customer information.

I contend that organizations will engage in privacy violating, protecting or enhancing behaviors as public manifestations of their customer relationship stances, information management strategies and customer information privacy philosophies. Two primary characteristics differentiate among the privacy practices – control and procedural justice. *Control* over the collection, use and reuse of personal information has been demonstrated to be an important aspect of the "privacy calculus" that customers engage in when evaluating firms from a privacy perspective (Culnan and Armstrong 1999; Laufer and Wolfe 1977). I argue that the degree to which customers are able to retain control over their personal information characterizes the firm's strength of information privacy orientation by distinguishing among those firms that control the information (weak) and those firms that assist customers in protecting their personal information (strong).

Procedural justice, as it has been employed within the organization behavior field, involves the perception by employees that they have been treated fairly in a process, regardless of the actual outcome of the process (Greenberg 1990). Some privacy researchers argue that procedural justice is similarly important in the information privacy relationship between customers and firms (Culnan and Armstrong 1999; Culnan and Bies 2003). Procedural justice, with its concerns for fairness, transparency and accountability for one's actions, is an important source of providing customers with tangible (actual processes) and psychological benefits (confidence, trust) that translate into greater willingness to transact business (Culnan and Bies

2003). Procedural justice can likewise serve as a means of characterizing the strength of firms' IPO. Consistent with the approach taken to exemplify the Customer Relationship Stance, Information Management Strategy, and the Customer Information Privacy Philosophy dimensions of the continuum, I will discuss this sub-construct within four categories as illustrated below in Figure 4-8.

Non Compliant with Privacy Laws or Norms *No control, no justice*	Minimally Compliant with Laws or Norms *Sufficient control, justice provisions to comply with laws, norms*	Embracing of Professional or Trade Group Codes *Control, justice provisions tied to benefits*	Offering Significantly Enhanced Privacy Protections *Significantly enhanced privacy protections*
Firms seize control of customer information; no accessible procedural justice. No privacy references discernible.	Customers wrestle with firms for control; minimal justice provisions discernible. Legal compliance appeals.	Firms and customers share control; procedural justice as required within codes. Privacy actions appeal to trading information to obtain benefits.	Firms help customers maintain control; expanded justice provisions. Privacy actions specifically and directly address customer control, justice issues and address trust and other relationship values.
Weaker ←			→ *Stronger*

Figure 4-8: Customer Information Privacy Behaviors

Non-Compliance

I argue that these firms will exhibit no privacy behaviors publicly whether or not they are in legislated (non-compliant with privacy laws) or non-legislated environments (non-compliant with social norms). Consistent with an exploitive customer relationship stance, a cost reduction information management strategy, and a customer information privacy philosophy that ignores laws and norms, firms in this position would be expected to not comply with privacy statutes or social trends. Organizations may be non-compliant for reasons of ignorance of legal requirements, inability to meet requirements for technical reasons, cost reasons, or willful disregard of regulatory requirements. In the case in which there is no or little legal requirement

for organizational privacy behaviors, firms may not be "compliant" with customer privacy concerns due to ignorance of these concerns, a lack of concern for customer desires for greater privacy, or willful exploitation through deliberate privacy violating behaviors. In these situations, privacy protecting behaviors are absent and privacy violating behaviors are likely invisible to customers and casual observers.

I would expect such organizations would not exhibit privacy behaviors (i.e., not display a privacy policy on a website, not provide detailed information to customers about the organization's use of personal information when requested, or misrepresent the extent to which they violate customer privacy). In these cases, the firms seize control of customer information and provide no avenues for the expression of customer preferences (no control) or for recourse (no procedural justice). This position represents the weakest strength of IPO simply because no privacy behaviors are evident.

Minimal Compliance

I argue that firms occupying this privacy behavior category leave customers to fend for themselves, use information to minimize risks, and see privacy norms and laws as a constraint on their activities. These firms will engage in as few privacy behaviors as they need to avoid legal action but they are not going to be seen as privacy leaders (nor do they aspire to that status).

Responding to the minimum requirements of government regulation is considered to be a key driver of an organization's privacy behaviors (Milberg et al. 2000; Milne 2000). Depending on the jurisdiction, this can mean a high level of mandatory privacy protecting behaviors (as required by the European Data Protection Directive or Canada's Personal Information Protection and Electronic Documents Act). Other jurisdictions may require little of firms (such as in many of the U.S. commercial and industrial sectors). In a legal environment that requires little of firms in the way of providing information privacy to customers, firms would respond in accordance with the basic industry practice (if one had emerged) such as posting privacy policies, even if these did

not meet all requirements of FIP. For example, only 20% of the websites studied for the U.S. Federal Trade Commission Report on Internet Commerce broadly adhered to Fair Information Principles although most of the websites had posted some type of privacy notice (FTC 2000). Geist and Van Loon's (2000) study of Canadian websites found that 41% of the sites lacked a privacy policy and of those with policies, many lacked comprehensiveness (i.e., 94% lacked policies on data retention). These studies illustrate how firms wrestle with their customers for control over customer information and provide the minimum level of justice considerations necessary to avoid legal problems. Minimal compliance is, by definition, somewhat stronger than no compliance on the IPO continuum. However, it remains a weak position because it continues to characterize privacy as a problem to be minimized rather than as an opportunity to serve customers and, potentially, distinguish the organization.

Adhering to Codes of Conduct

Firms occupying this position on the continuum recognize a shared responsibility for customer well being, pursue an add value information management strategy and regard privacy laws and norms as the basis for establishing good exchange relations with their customers. These firms adhere to particular privacy codes that are voluntarily implemented, including industry and professional codes, and that exceed the minimum legal or social norms requirements.

McDonald (2000) suggests that codes of conduct are particularly effective for instilling ethical sensibilities throughout organizations. For example, many Canadian companies had voluntarily implemented the Canadian Standards Association (CSA) Model Privacy Code well in advance of the federal government's legislation (Perrin et al. 2001), placing them further along the privacy continuum than those organizations that had not. In addition, leading industry organizations including the Canadian Information Processing Society (CIPS) and the Canadian Marketing Association (CMA) had privacy policies that required member adherence in advance of the federal legislation. However, just as the Generally Accepted Accounting Principles

(GAAP) are open to interpretation, so are the 10 privacy principles that are at the core of the PIPEDA. The PIPEDA has been described as a "flexible framework" within which firms shape their individual privacy policies (Gustavson 2003; Wright 2003). Different firms are likely to engage in different behaviors even within the scope of the federal law. However, I would expect that the organizations would meet the higher standard of a code in order to maintain membership in an industry group (CMA 2002).

In jurisdictions with modest legal requirements, I would expect some firms would attempt to distinguish themselves by affiliating with a stricter privacy regime. For example, the U.S. Department of Commerce has negotiated an agreement with the European Commission for a "Safe Harbor" for U.S. companies with respect to the collection and use of personally identifiable customer and employee information. As of December 2004, 625 U.S. corporations had registered with the Department of Commerce. A review of the list reveals that a variety of firms have taken advantage of this protection including such well known global operators as IBM and Procter & Gamble. In addition, firms such as Enterprise Car Rental that transact business with European tourists visiting the U.S. for holidays have entered the "Safe Harbor." However, the list includes many less well known organizations and it may be fair to interpret some behaviors as pre-emptive positioning by certain firms to appear more privacy oriented than others. In these cases, I would argue that control over information is shared between firms and their customers and that justice considerations are expanded to incorporate a broader range of opportunities for customers to select how their information is used.

Significantly Enhanced Privacy Offerings

Consistent with a customer relationship stance that places a positive obligation on firms to work for their customers' well being, an information management strategy that attempts to create innovative products and services, and a philosophy that sees privacy as a source of competitive differentiation, firms occupying this position are most likely to offer significantly

enhanced privacy behaviors as part of their business strategy. These behaviors would include actions that deliberately enhance customer information privacy and that set an organization apart from its peer group. Some of these behaviors may be visible to customers. For example, the Royal Bank offers privacy and security enhancing software to its Internet banking customers (Middlemiss, 2001).

However, other behaviors might be less visible to outsiders including the appointment of senior influential personnel responsible for privacy programs (rather than mid-level managers); the use of privacy impact statements as part of business cases; extensive training for employees; and periodic audits (Culnan and Bies 1999). Clarke (1999) further suggests that these types of organizations, in their quest to move beyond the perceived inadequacies of a fair information practices approach to privacy, will provide public justification for privacy invasiveness; offer anonymous, pseudonymous and identifiable options for electronic and mobile commerce transactions; and offer customers choices of modes of identification and authentication. Again, the Royal Bank offers an example in which it "delayed the rollout of wireless banking until it found a Nokia phone with a chip allowing customers to encrypt passwords and other information." (New York Times June 3, 2002). While arguably more an issue of security at a technical level (i.e. enabling similar levels of transaction protection as obtainable in a "wired" environment), this willingness to postpone commercial activity in order to benefit customers suggests that there are firms that are willing to make tradeoffs to the benefit of their customers.

This position represents the strongest of the categories of privacy behaviors on the IPO continuum because it offers the greatest protection to consumers by placing them firmly in control of their information and offering significant procedural safeguards. Few firms are expected to attempt this positioning not only for cost and other organizational considerations but because it may not be what their customers want or need. The paradox of this position is that customers need to be educated and willing to involve themselves in their information privacy protection. Not all customer are likely to be so inclined and therefore, firms will have to

determine what makes the most sense for them over time and as they gain experience with customers and privacy.

As a result, I expect to find that an organization's place on the information privacy orientation continuum will be dynamic, reflecting ongoing changes in consumer privacy expectations, technological advances (both in terms of privacy invasiveness and privacy protection) as well as organizations' responses to evolving legal and competitive challenges. However, given a position in which not meeting statutory obligations or addressing social demands for privacy action occupies the left hand anchor of the continuum (and depending on the regulatory regime), we can distinguish among firms with weak, moderate and strong information privacy orientations based on their privacy practices. The detailed Information Privacy Orientation Continuum is shown as Figure 4-9.

Chapter Summary

In this chapter, I have presented the focal variable, Information Privacy Orientation, and represented it as a four tiered continuum that adapts the Marketing Ethics Continuum (Smith 1995). I argued that firms have distinct information privacy orientations based on combinations of four sub-constructs: customer relationship stances, customer information management strategies, customer information privacy philosophies, and customer information privacy behaviors. Depending on where firms fall on the continuum, they can be classified as weaker or stronger in their information privacy orientation. The question is why would certain firms in the same industry operating within a consistent regulatory framework have different privacy behaviors? In other words, what explanation exists for why some firms follow similar privacy behaviors while others exhibit distinctly different behaviors? I will argue in Chapter Five that these similarities and differences can be explained when considered through the theoretical lenses of the Institutional Approach (IA) versus the Resource-Based View (RBV) of the firm.

Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
Customer Information Privacy Behavior			
No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
Customer Information Privacy Philosophy			
Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
Customer Information Management Strategy			
Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
Customer Relationship Stance			
Weaker	←	→	*Stronger*

Figure 4-9: Information Privacy Orientation Continuum (Detailed)

CHAPTER FIVE

COMPETING THEORIES TO EXPLAIN SIMILARITIES AND DIFFERENCES IN INFORMATION PRIVACY ORIENTATION

To this point, I have discussed a conceptual approach to considering Information Privacy Orientation. In this chapter, I comprehensively review the two theoretical lenses I use to explain the observed similarities and differences in Information Privacy Orientation that I found in my research. As I identified in Chapter One, I adopted an initial posture that placed the Institutional Approach (IA) and the Resource-Based View (RBV) of the firm as competing explanations for IPO. I justified this approach based both on the exploratory nature of the present research as well as the fundamentally different perspectives on firms' behaviors afforded by these theories. I do not claim to offer an overarching theory of information privacy. My goal is more humble. I suggest only that similarities in IPO among firms may be explained using an Institutional theory lens while the RBV lends itself to analysis of differences in IPO.

There are three sections to this chapter. The first section provides an overview of the IA and then uses it to explain homogenous IPO. The second section details the relevant aspects of RBV and then applies the theory to explanations of heterogeneous IPO. The concluding section synthesizes these two opposing views into a comprehensive framework for assessing IPO across a sample of firms.

Explaining Similarities: The Institutional Approach (IA)

Institutional theory is part of a stream of research that examines the relationship between organizations and their environments particularly with respect to the non-economic means by which firms secure their survival. The institutional tradition (Hannan and Freeman, 1989) sees organizations, not solely as rational, efficiency-seeking entities but as social, political and cultural ones (Scott 2001). This is not to say that institutional theory does not accommodate rationality. Rather, and in contrast to economic models of organizational behavior, rationality is located, not

within organizations themselves, but within their environments (DiMaggio and Powell, 1983; Pfeffer, 1997; Tolbert and Zucker, 1996). Furthermore, the rationality is one of conformance to social norms in a search for legitimacy rather than conformance to a rent seeking model of economic behaviour. Meyer and Rowan (1977:343) in their seminal article on institutions argued that

> Many of the positions, policies, programs and procedures of modern organizations are enforced by public opinion, by the views of important constituents, ...by social prestige, by the laws ...Such elements of formal structure are manifestations of powerful institutional rules which function as highly rationalized myths that are binding on particular organizations.

In other words, the Institutional Approach argues that organizational survival may depend more on conforming to the norms of external groups and less on succeeding as efficient producers of goods and services (DiMaggio and Powell 1983).

There are four aspects of the institutional approach that apply to my dissertation research. I argue that the formation of information privacy orientation in most organizations is primarily a response to external pressures or "institutional" forces. Therefore, it is necessary to examine the aspects of institutional theory that address pressures and responses. The theoretical elements of greatest interests are organizational goals, the sources for pressures to act, the ability to act, and response strategies. I discuss each of these elements in turn and then provide an examination of how the Institutional Approach can be applied to understanding information privacy orientation.

Organizational Goals

In its initial formulation, institutional theory suggested that organizations existed merely to survive. That is, the actions taken by firms were directly related to concerns for maintaining the existence of the firm. Over time, the institutional approach has evolved and now assumes that the overriding organizational goal is to achieve legitimacy as a means of ensuring survival. *Legitimacy* is defined as

> A generalized perception or assumption that the actions of an entity are desirable, proper or appropriate within some socially constructed system of norms, values, beliefs and definitions (Suchman 1995: 574).

The IA literature identifies several forms of legitimacy. *Pragmatic legitimacy* refers to short term, self-interested perceptions by external audiences (such as customers) that suggest a transactions oriented focus on legitimacy ("the organization is legitimate because it has met my immediate, transaction needs as a customer"). In contrast, *social legitimacy* (as characterized by Handelman and Arnold 1999) or *moral legitimacy* (Suchman 1995) refers to perceptions grounded in a longer term, pro-social logic that consider actions in light of their impact on concerns for community and society. This form of legitimacy might be expressed in more general terms by customers such as "the organization is legitimate because it is a good corporate citizen." Ruef and Scott (1997) argue for distinctions between managerial and technical legitimacy. *Managerial legitimacy* is "normative support for organizational mechanisms" such the key back-office functions including human resources, accounting, finance and IT/IS. In contrast, *technical legitimacy* is concerned with the core activity of the firm, arguably those most concerned with its direct economic activities of the firm, such as manufacturing, marketing, and sales.[1]

Sources of Pressure

Oliver (1991:160) offers a framework for considering the source of pressures that incorporates five institutional factors operating as antecedents to strategic responses. In other words, there are five questions that drive organizational responses and each question has related predictive dimensions. These factors are cause, constituents, content, control, and context. *Cause* refers to the reasons why the organization perceives pressures to conform. The predictive dimensions are whether the firm seeks legitimacy or efficiency. *Constituents* addresses who is pressuring the organization. The predictive dimensions include whether there is a multiplicity of

[1] These latter definitions are adapted from Ruef and Scott (1997:883). Their study focused on hospitals which have typically well-defined managerial (non-medical) and technical (medical) functions. The adaptation I have made roughly conforms to Porter's (1985) value chain distinction between a firm's primary and support activities.

demands from constituents and the extent of the firm's dependence on the various constituents. *Content* describes what actual norms the firm is being pressured to adopt. In this case, the predictive dimensions are whether or not the imposed norms are consonant with achieving prevailing organizational goals. *Control* refers to how the pressures are being brought to bear on the affected organization. The distinctions between legal coercion versus voluntary adoption are the predictive dimensions of control. Lastly, *context* describes the where, the environment from which emanates the pressures on the firm. For this dimension, Oliver assigns the predictors of environmental uncertainty and environmental interconnectedness.

Ability to Respond to Pressure

Organizational ability to respond to externally based pressures depends on the degree to which organizations are embedded within in their social networks coupled with their ability and willingness to exercise agency. *Social embeddedness* refers to the extent to which organisations are linked within larger networks, both economic and social (Dacin, Ventresca and Beal 1999). These networks, comprised of other organizations (including competitors, regulators, customers and similar stakeholders) act as enablers for and constraints on organizational activity (Orlikowski and Barley 2001). However, organizations are not passive victims of their environment (Pfeffer 1997) because they can exercise agency. *Agency* is the extent to which organizations are able and willing to operate beyond the norms and restrictions contained within their networks. Organizations can choose, albeit to greater or lesser extents, whether or not to engage their environments and respond to pressures (Scott 2001).

Response Strategies

An important strand in Institutional theory has suggested a passive response mechanism in which firms imitated the actions of similar organizations in response to external pressures. Berger and Luckman (1971) contended that, over time, industries develop a set of common understandings or expectations of how things are done. "Isomorphism" is defined by DiMaggio

and Powell (1983:149) as "a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions." More specifically, "mimetic isomorphism" is an organizational phenomenon of imitation in which firms deliberately implement the policies, programs, technologies and practices that they observe being carried out by others and that, rightly or wrongly, they perceive to be successful (Scott 1987). Empirical studies have verified the existence and strength of organizational imitation as a response to environmental pressures. Organizations mimic the strategic and structural choices of others (Scott 1995; Pfeffer 1997; Tolbert and Zucker 1996). Imitation influences the adoption of codes of ethics (Weaver, Trevino and Cochran 1999), intra-industry patterns of political donations (Mizruchi, 1989), and the likelihood and level of philanthropic activity (Galakiewiscz and Wasserman, 1989).

Notwithstanding the empirical evidence in support of the isomorphic tendencies of organizations, several authors (Goodstein 1994; Oliver 1991; Perrow 1985) argued that this approach was "oversocialized", too static and, hence, limiting. It did not account for heterogeneity in observed organizational responses, nor for the exercise of agency and the pursuit of discrete organizational interests. Oliver (1997) combined institutional and resource-dependence theories[2] to develop a repertoire of five strategies from which organizations choose to respond to institutional pressures. The responses are based on how organizations manage their "technical activities" (the activities used to derive economic returns) versus the institutional environment (Meyer and Rowan 1977). Frequently at issue is the need to separate or "decouple" the two sets of discrete, if complementary activities, in order to manage environmental demands while preserving the integrity of the technical core (Meyer and Rowan 1977).

[2] Resource-dependence theory is not the same as the resource-based view of the firm. Resource-dependence theory (Pfeffer and Salancik, 1978) argues that organizations exist within and depend upon uncertain external environments for their survival. The "dependence" involves needing economic and other resources from the external environment in order to continue operating. Power relationships are an important aspect of the theory such that "organizations tend to comply with the demands of those interests in their environment which have relatively more power" (Pfeffer 1987:26-7 as quoted in Pfeffer 1997:63). An explanation of the resource-based view of the firm appears later in this chapter.

Oliver theorized that the strategies can be conceptualized as a continuum ranging from most passive (acquiesce to pressure) to most active (manipulate the circumstances to seize control). *Acquiescence* permits organizations to conform through imitation of model organizations (in the hopes of gaining in legitimacy or additional resources) or compliance to the pressure in order to reduce the likelihood of negative responses. *Compromise* as a strategy involves three processes in which organizations more actively address the frequently competing demands of various stakeholders. Organizations attempt to achieve a balance among these competing interests, or try to pacify constituents through accommodation, or they may bargain to reduce the extent of demands. *Avoidance* strategies were originally described by Oliver (1991:154) as attempts to "preclude the necessity of conformity" by concealing non-conforming activities, decoupling the actual activities (non-conforming technical core) from symbolic ones (representations of conformity), or exiting the industry. *Defiance* as a strategy moves us to the point on the continuum where organizations begin to actively and publicly resist, to greater or lesser degrees, these environmental pressures by ignoring, challenging or attacking the rules or the organizations associated with the rules. *Manipulation* is the strategy employed by organizations that want to seize control of their environment through co-opting, influencing or control activities.

The existence of a range of strategic responses to external threats has been empirically verified. For example, two studies of the response by firms to institutional pressures to address work-family issues demonstrated that firms choose from a menu of responses. Goodstein (1994) confirmed the utility of the Oliver typology. On the one hand, firms that perceived strong institutional pressures for addressing work-family issues and perceived positive benefits from providing child care and low costs of provision were likely to adopt an acquiescence response (offer at least one child care and one flexible benefit option to employees). In contrast, firms that perceived a weak pressure and considered the consequences as negative were more likely to enact a defiance response (not providing any childcare or flexible benefit). Ingram and Simons (1995)

replicated and extended this research. They found improved support for the importance of goal congruence and that distinctions could be made between symbolic and substantive compliance with work-family norms.

The strategies of acquiescence and manipulation are the two most associated with the pursuit of organizational legitimacy (Scott 2001). According to Scott (2001), acquiescence through conformity, or "isomorphic mimetism" (DiMaggio and Powell, 1983) is the most frequently researched aspect of the five institutional responses. Studies of the phenomenon have included examinations of the transition to the multidivisional form (MDF) within certain industries (Fligstein, 1985), homogenization of workplace practices (Baron, Dobbing and Jennings, 1986), adoption of more formal, more systematic, more logical and more analytical approaches to decision-making (Langley, 1989), intra-industry patterns of political donations (Mizruchi, 1989), likelihood and level of philanthropic activity (Galakiewiscz and Wasserman, 1989), diversification into new markets (Haveman, 1993), and corporate acquisition activities (Haunschild, 1993).

The importance of mimetic activities to supporting organizational survival through the achievement of legitimacy has likewise been demonstrated empirically. Baum and Oliver (1991) concluded that replicating institutional norms was positively related to the likelihood of the survival of childcare centers, partly as a result of perceived legitimacy. Deephouse (1996) studied financial institutions and determined that the both the media and regulatory agencies rated banks that followed similar asset management strategies as more legitimate than those which appeared to "deviate from normal behavior" (1033).

In a study that directly examined the impact of the source for institutional pressure on firms' responses, Ang and Cummings (1997) reviewed the outsourcing decisions of a sample of 385 banks of various asset sizes. They found first, that firms' decisions to outsource their IS functions were influenced by whether the pressure came from federal regulators or competitive peers; and second, that the size of the bank affected the response to competitive pressures. The

"acquiescence" strategy was most likely to be invoked in the face of regulatory pressure in order for firms to achieve "certainty, stability and predictability" in their environments (249). A broader range of responses was employed in response to competitive pressures.

The manipulation response strategy typically involves organizational efforts to forge links to powerful groups or individuals in order to expand the range of options. Impression management theory (from social psychology) was used in two different studies of manipulation strategies. Elsbach and Kramer (1996) showed how organizations attempt to bridge the gap between perceived assaults on organizations' external identities (as constructed by others through vehicles such as business rankings) and their internal identities (as generally subscribed to by organizational members). Likewise, Elsbach and Sutton (1992) studied the actions of two interest groups that used "illegitimate tactics to gain recognition and achieve goals" (702). In both studies, the legitimacy of other groups was "borrowed" in order to support the efforts of the focal organizations, clearly manipulation strategies.

While Oliver's typology has been well-received, there have been calls to refine the repertoire of responses to capture the behaviors of firms that behave proactively (Cashore and Vertinsky 2000). In their study of the responses by forestry firms to policy demands for sustainable development programs, Cashore and Vertinsky argue for a "proactive category" in which firms are "more advanced than societal pressure, leading the way with innovation and proaction" (4). This category of response is demonstrated in their case studies to be important to firms seeking competitive advantage from their environmental initiatives. I argue that this proactive response does not fit within the institutional approach as it suggests a deliberate strategy that leads firms away from established norms. I pursue the theoretical reasons for non-institutional behavior in the section on Resource-Based Theory, later in this chapter.

Institutional Approach and Information Privacy Orientation

In this section, I apply the elements of the Institutional Approach as described above to Information Privacy Orientation to demonstrate this theory's applicability to my dissertation research. Recall that I indicated that I expected that the IPO continuum would be dynamic, reflecting organizational responses to changes in regulations, consumer privacy expectations, technological advances, and competitors' moves. These changes make predictions of specific organizational responses problematic. Furthermore, there are instances in which the element in question may be ambivalent in its contribution to the explanation. For example, the roles played by social embeddedness versus agency in the firms' ability and willingness to respond to external pressures can be argued to be ambivalent. However, I suggest that the Institutional Approach provides a broad basket within which to locate the explanations for Information Privacy Orientation that reflect the similarities in approaches across firms within the same industry. Table 5-1: Institutional Approach and Information Privacy Orientation summarizes these arguments which are explained below.

IPO and Organizational Goals

Recall that the organizational goal within the Institutional Approach involves the search for legitimacy as a means to secure organizational survival. I contend that organizations that are weaker in IPO are more concerned with seeking pragmatic and managerial forms of legitimacy than those with moderate IPO who are pursuing social and technical legitimacy. Pragmatic legitimacy in IPO terms will involve appeals to conformity to the legal environment (basic legal compliance) by making the minimum changes necessary to minimize potential legal problems. These changes will be made in the firm's back office operations to demonstrate compliance while attempting to mitigate the impact on firms' key activities. Firms further along the IPO continuum

would be expected to seek social legitimacy by appealing to perceived norms about information privacy and emphasizing changes to the firms' technical core to substantiate these claims.

Table 5-1: Institutional Approach and Information Privacy Orientation

Element	Institutional Approach	Information Privacy Orientation Application	
		Weaker IPO	***Stronger IPO***
Organizational Goal	Survival through the search for legitimacy	• Pragmatic • Managerial	• Social • Technical
Source of pressure	• Cause (threat) • Constituency • Content • Control • Context	• Efficiency • Dependence • Constraint • Coercion • Uncertainty	• Legitimacy • Multiplicity • Consistency • Diffusion • Interconnectedness
Ability and willingness to respond to pressure	Influence of social network	Embeddedness	Agency
Responses to pressures	• Acquiescence • Manipulation	• Acquiescence (compliance with legal model) • Imitation of minimalist organizations	• Manipulation (impression management) • Imitation of benchmark organizations

IPO and Source of Institutional Pressure

Oliver (1991) identified five sources of institutional pressure – cause, constituents content, control and context. I have modified this typology to regard "cause" as the nature of the perceived threat to the organization. In other words, is the pressure seen to be a threat to firm legitimacy or efficiency? I argue that weaker IPO is a response to one set of pressures made up of efficiency, dependence, constraint, coercion and uncertainty concerns. Stronger IPO is made up of the combined pressures of legitimacy, multiplicity, consistency, diffusion and interconnectedness. In the case of weaker IPO, firms will perceive privacy as a threat to their ability to pursue their economic activities (efficiency) unless they conform with privacy norms (legal or social). In addition, they will perceive that they are dependent on the legal system to legitimate their claims to conformity, will view the norms as constraints on their organizational

activities, perceive any required changes as coercive, and will perceive the information privacy issue as contributing to the environmental uncertainty in which they operate. In other words, weaker IPO will attach to firms that see information privacy as a threat to their organization.

In contrast, I argue that stronger IPO attaches to firms that apply a different logic to how they perceive the external pressures to conform to privacy norms. These firms perceive the privacy issue as an opportunity to reinforce their legitimacy. In addition, they will argue that a multiplicity of constituents (e.g., customers, regulators, privacy advocates) need to be satisfied, that pursuing information privacy beyond minimum legal compliance is consistent with their firms' culture and goals, and that their privacy practices are not solely a response to legal "coercion" but to several points of pressure. Lastly, these firms are likely to regard the context as less one of adding to environmental uncertainty as it is a pressure to maintain engagement with the environment.

IPO and Ability and Willingness to Respond to Pressure

Firms vary in their ability and willingness to respond to perceived external pressures to change and within the IA, this capability is based on the extent to which firms are embedded within relevant (to the issue) social networks versus their desire to exercise agency. I expect weaker IPO is evident in firms that perceive themselves as more strongly embedded in their networks, such as industry associations) sand, as a result, are either more willing to conform to what the network establishes as appropriate IPO or are less willing to extend themselves in an independent search for alternatives. On the other hand, I expect that firms with stronger IPO while still operating within the overall network, exercise a modicum of agency to develop an IPO that is different from others' but not to the extent that it would undermine other important goals such as legitimacy.

IPO and Responses to Pressures

Overall, I argue that the majority of firms adopt an acquiescence strategy in the face of institutional pressures to address information privacy. However, even within this strategy, I believe that there are likely discernible differences between weaker and stronger IPO firms, primarily based on the rationale for the responses employed. Weaker IPO firms acquiesce for either of two reasons (admittedly not mutually exclusive). Either the firms acquiesce for reasons of conformity to a defined legal model or they imitate the privacy behaviors of similar firms with minimalist privacy regimes. The firms' rhetoric will involve appeals to "having to do what the law requires" and "doing the same as other firms in the industry or jurisdiction." However, the logic employed by stronger IPO firms will invoke either the acquiescence or manipulation strategies.

Stronger IPO acquiescent firms will likely imitate the privacy behaviors of firms known to have stronger privacy models (regardless of industry). These firms will use this modeling as a demonstration of agency and employ a bounded language of leadership. Their rhetoric will imply good differences but avoid appearing extreme in order not to undermine their claims to legitimacy. Some firms may use a manipulations strategy and "borrow" the perceived credibility of third party organizations in a bid to suggest that they are exercising agency and not merely following the crowd. They may, for example, join a third party assurance program despite being in a legislated privacy jurisdiction.

In summary, I have explained how the Institutional Approach could be used to explain homogeneity in IPO among firms. I explored the goals, sources of pressures, ability and willingness to respond to the pressure, and the strategic responses employed by firms based on Oliver's (1991) typology. I argued that weaker IPO firms would display different attributes than stronger IPO firms but that the entirety of responses could be explained as consistent within the overall IA paradigm. Firms will use different justifications to explain their IPO but underlying

these reasons is the reality that they are conforming to a basic institutional model and will not deviate greatly from that model because of the risk of undermining their legitimacy, which is at the heart of the institutional approach's explanation for firm behavior.

I will now describe how the resource-based view of the firm will be applied to a consideration of firms that appear to have fundamentally different organizational responses to the pressures for information privacy.

Explaining Differences: The Resource-Based View of the Firm (RBV)

Similar to the Institutional Approach, the Resource-Based View is a "paradigm rather than a theory" (Jarvenpaa and Leidner 1998:344). Both of these paradigms offer broad bases from which to assess organizational operations and compare practices among firms and across industries. However, there are several fundamental differences that distinguish the RBV from the IA. If the Institutional Approach provides a means for considering the activities of the firm from the "outside-in", the Resource-Based View takes an "inside-out" perspective (Srivastava, Fahey and Christensen 2001). If information privacy is conceptualized as an external threat to the organization, the IA offers an explanation for why firms take similar approaches (competitive homogeneity) to adapting to the changed environment while the RBV attempts to explain the differences among firms (competitive heterogeneity). A further difference lies in the organizational goals attached to the different theories. The IA, as I have applied it to my research, argues that firms pursue legitimacy to ensure organizational survival. In contrast, RBV affords a platform for the consideration of how firms can achieve sustained competitive advantage over their competitors through the development and deployment of resources that are bundled into unique organizational routines (Penrose 1959).

In contrast to the arguments laid out in the previous discussion on IA, I suggest that an information privacy orientation in some firms results, not from responding to externally derived "institutional" forces, but as the outcome of deliberate choices made to differentiate the firm in

privacy terms (Chan 2003; Culnan and Bies 2003). In this section, I will define key aspects of the RBV paradigm (resources, processes, capabilities, dynamic capabilities) and discuss how resources and capabilities can contribute to achieving sustainable competitive advantage. I also introduce a framework of corporate resource hierarchy upon which I base my theoretical approach to RBV and information privacy. Lastly, I theorize how RBV can be applied to IPO to serve as a contrasting explanation to the institutional approach.

Resources, Process and Capabilities

Most RBV researchers distinguish among resources, processes and capabilities (Srivastava et al 2001). The RBV takes as a starting point the consideration that organizations are bundles of resources (Penrose 1959) that can be combined and recombined in a variety of ways (Wernerfelt 1984). *Resources*, generally, are "the basic unit of analysis" (Grant 1991:118) and have been defined as "something that can be turned to for support or help; an available supply that can be drawn upon when needed" (Brumagin 1994 after American Heritage Dictionary 1991).

There are several approaches to distinguishing among types of resources. Barney (1991) argued that resources could be *physical* (plant, equipment, location and access to raw materials); *human* (training and experience, judgment and insight); or *organizational* (structure, reporting relationships, coordinating mechanisms). Grant (1991:118) took the approach that resources should be seen as "inputs to the production process" and drew distinctions among tangible, intangible (Itami 1987) and personnel-based resources. *Tangible resources* are easily identified and typify what are listed as financial and physical assets on a firm's balance sheet. *Intangible resources* are much more difficult to identify and include such "things" as reputation, brand image, and product quality. *Personnel-based resources* are comprised of the firm's technical know-how and organizational culture. One way to understand the differences between these two approaches to resource definition lies in the distinctions drawn between resources as inputs to

processes (Grant's approach) and resources as both input and process (Barney's approach). While I prefer the greater precision possibly afforded by Grant's approach and will distinguish from this point between resources and capabilities (the routines that combine resources), I will rely on a third typology for characterizing the resources at issue in considering information privacy orientation.

Miller and Shamsie (1996) argued that the listing of resources as suggested by Grant's and Barney's typologies is limited in its usefulness because it does not point to how resources confer advantage to the firms that have them as assets. In other words, how does having personnel-based resources confer advantage by definition? The answer is simply that they do not confer advantage by their mere presence. Miller and Shamsie (1996) suggested that there are two types of resources of most importance to firms seeking competitive advantage – property-based and knowledge-based resources. *Property-based resources* involve specific product and process resources to which a firm has some exclusive, specific and enforceable claim and to which competitors have no legal access. Examples of these resources include long term contracts for hard to obtain goods or services, rights to important technologies, and exclusive distribution arrangements. Less tangible are k*nowledge-based resources* which are characterized by subtlety and ambiguity rendering them difficult to detect and isolate. Examples of these resources include technical, creative and collaborative skills. This typology was extended by Miller, Eisenstat and Foote (2002) to include *relationship-based resources*. While the exact nature of the resource was undefined, examples were provided and included valued relationships with customers, suppliers and allies.

The marketing literature provides some further guidance about the nature of resources that appear to be most relevant to a discussion of how information privacy orientation may be a source of competitive advantage. Hunt and Morgan (1996) argue that customers and channels are

fundamental resources. Srivastava et al. (1998) define "market-based assets"[3] as assets that result from the organization's externally oriented activities and distinguish two types of market-based assets – intellectual and relational. *Intellectual market-based resources* are the "types of knowledge a firm posses about the environment, such as the emerging and potential state of market conditions and the entities in it, including competitors, customers, channels, suppliers, and social and political interest groups" while *relational market-based resources* are "outcomes of the relationship between the firm and key external stakeholders, including distributors, retailers, end customers, other strategic partners, community groups, and even governmental agencies" (5). While on the surface these two resource types appear to parallel Miller and Shamsie's (1994) and Miller et al.'s (2002) knowledge-based and relationship based resources, I contend that Srivastava et al.'s approach provides a more precise distinction for my purposes by setting the stage to distinguish between firms that value information-based resources (intellectual) and those that value customer relationship based resources (relational), and consequently, have different information privacy orientation. This discussion will be continued in the section on RBV and information privacy.

Owning or having access to resources, however defined, is not sufficient in and of itself to confer competitive advantage, sustained or temporary. Barney's (1991) resource-based framework outlined four *attributes of sustainability* based on the resources' degree of value (valuable or not) and degree of idiosyncrasy (rareness, imitability, substitutability) (Burmagin 1994). These attributes include whether the resource is valuable (able to assist the firm to defend against threats or exploit opportunities); rare (difficult to acquire now and in the future); hard to imitate (unique circumstances, causally ambiguous, complex to understand); and not substitutable (another combination of resources cannot be deployed in the same fashion). Prahalad and Hamel (1990) argue that resource idiosyncrasy (as represented by the attributes of imitation and substitutability) are of less importance than that of organizational accessibility, the ability to

[3] Barney (1991) and Srivastava et al (2001) use the terms assets and resources interchangeably.

apply the resource across business units. Brumagin (1994) suggests the issue is really about the "tradeoff" between resource flexibility (which offers the ability to capitalize on multi-unit resource use) and idiosyncrasy (which limits this flexibility thereby diminishing potential economies). Regardless of whether the analytical framework characterizes the issue as the importance of flexibility or uniqueness, the key to these attributes providing a basis for competitive advantage is for them to be simultaneously present.

Brumagin (1994) theorized a four level hierarchy of corporate resources that provides an arguably more concrete approach to a discussion of resources in achieving sustained competitive advantage(see Table 5-2). The first level comprises resources most associated with the production

Table 5-2: A Hierarchy of Corporate Resources

Resource Level	Definition	Example
4	Resources that support **Strategic Vision** that drives corporate activity including strategic implementation and vision development and sharing	Idiosyncratic strategic vision may be valuable because it is not imitated therefore serving as a barrier to competition. Ongoing corporate commitment to strategic vision reinforces the decision discipline across resource levels.
3	Resources that support **Learning** (Innovation and Change) throughout the organization directed to better utilization of corporate assets	Internally oriented learning – improvement of level 1 or 2 resources (efficiency related) Externally oriented learning – (effectiveness related) improvement in ability to adapt to changing environment Adaptive innovation – use of existing products/processes or acquisition of externally produced innovations Creative innovation – internally generated incremental or breakthrough improvements
2	Resources that support **Administrative Capabilities** to integrate across business units	Managerial skills, management systems, and structurally based coordinating mechanisms that reduce conflict, build trust and develop teamwork across business units
1	Resources that support basic business unit **Production and Maintenance** processes	Porter (1985) Value Chain activities: Inbound logistics, Operations, Outbound logistics, marketing and sales, and Service along with support activities of Firm Infrastructure, Human Resource Management, Technological Development and Procurement.

(Adapted from Brumagin 1994:90)

and maintenance activities of the firm. These are resources that closely resemble Porter's (1985) Value Chain activities. Level 2 resources are mainly concerned with a firm's administrative capabilities to integrate activities across business units. Examples of these resources include managerial skills and management systems. These resources appear consistent with Mata, Fuerst and Barney's (1995) findings of "managerial competence" as a source of IT competitive advantage. Level 3 resources support learning across the organization through the processes to implement innovation and change. These resources assist the firm to increase the efficiency and effectiveness of Level 1 and 2 resources. Learning can be either internally oriented (focused on improving efficiencies of Level 1 and 2 resources) or externally oriented (focused on increasing effectiveness of adaptation to environmental changes). Innovation can be either adaptive (using existing processes and products or acquiring them from external groups) or creative ("breakthrough" improvements). Level 4 resources support the implementation of the firm's strategic vision. These resources include senior level commitment to the vision and decision-making (such as resource allocation) that supports the vision. The point of this hierarchy is to show that the attributes test means that the actual basis for SCA will likely only come if a firm is focused on Level 3 or 4 resources for it is at this level that resources are harder to discern and to understand their fundamental role in supporting sustained competitive advantage, thus rendering imitation by outsiders an extremely difficult task.

Processes are the means by which the firm's resources are converted into their capabilities (Srivastava et al 2001) that groups such as customers find valuable (Barney 2001). These processes involve collections of linked tasks and routines (Davenport 1993) that occur across organizations. Examples of processes include product innovation management, supply chain management and customer relationship management (Srivastava et al 2001). It is the unique selection and combination of resources that firms deploy that create the opportunity to achieve competitive advantage (Barney 1991). These unique routines are often popularly referred to as a

firm's distinctive or core competence and are usually achieved by only a handful of firms (Barney and Griffin 1992).

Capabilities, in contrast, are the "capacity for a *team of resources* to perform some task or activity" my emphasis (Grant 1991:119) or "refer to a firm's capacity to *deploy* valued resources, usually in combination or co-presence" (emphasis in original) (Jarvenpaa and Leidner 1998:343). Capabilities reside within the firm and result from lengthy development times (Barney and Hansen 1994, Collis and Montgomery 1995; Grant 1991). Examples of capabilities include trustworthiness (Barney and Hansen 1994), rapid response to changes in customer tastes and preferences (Srivastava et al 2001), organizational flexibility, and short product lifecycles (Teece, Pisano and Shuen, 1997).

In other words, the fundamental difference between resources and capabilities is that while resources are the basis for developing capabilities, capabilities are the basis for developing competitive advantage (Grant 1991). Barney argued that the issue for firms is not merely the achievement of competitive advantage through the assemblage and deployment of resource bundles. The challenge is to achieve *sustained* competitive advantage through unique combinations and deployment of resources that represent the implementation of a strategy that others cannot easily replicate. *Sustained competitive advantage* is defined as "the advantage that exists after all attempts at strategic imitation have ceased" (Brumagin 1994:81 after Barney 1986). In the language of performance measurement, competitive advantage should translate into increased "rents" or returns to the firm (Coff 1999).

Hamel and Prahalad (1994) extended the dynamic capabilities concept with the addition of a strategic component. This view suggests that firms attempt to deploy their capabilities in order to shape their environments to obtain additional advantage, not to merely respond to them. They argue that strategic foresight, strategic intent and strategic architecture combine to provide this additional advantage. *Strategic foresight* is a capability to discern changes and envisage new responses beyond those over which the organization has direct control, while *strategic*

architecture is a capability to quickly revamp existing capabilities into new routines that better position the firm to capitalize on the environmental changes it is attempting accomplish. *Strategic intent* speaks to the firm's long term vision about its market and competitive positions.

The RBV has been criticized for two perceived deficiencies; first, that environments are assumed to be relatively stable; second, that core competences are assumed to be relatively static and enduring (Jarvenpaa and Leidner 1998). Teece, et al (1997) introduced *dynamic capabilities* as a concept to address these deficiencies and argued that rapid technological change required firms to be able to respond quickly and surely. Dynamic capabilities are defined as "the firm's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments" (516). If the basic resource-based view suggests that firms should align their capabilities to meet environmental conditions, the dynamic capabilities view argues for firms to be able to develop and deploy new capabilities in response to emerging opportunities (Teece and Pisano 1998). Otherwise, firms are susceptible to deteriorating performance as a result of "core rigidities" – inflexible capabilities that cannot be adapted quickly enough to respond to changing conditions (Leonard-Barton 1992).

I believe that the inclusion of a strategic component to RBV and the evolution to dynamic capabilities are particularly important theoretically. First, these additions address the "proactive" aspect of organizational decision-making that is less apparent in the institutional approach. Second, at the same time, the fundamental importance of environmental influences on decision-making are acknowledged. In the next section, I will discuss how I apply the RBV- dynamic capabilities approach to a consideration of information privacy orientation.

Resource-Based View and Information Privacy Orientation

In this section I apply the elements of the Resource Based View as described above to Information Privacy Orientation to demonstrate how this theory will be used in contrast with the previously outlined Institutional Approach. RBV logic suggests that firms will develop their

information privacy programs not simply as a result of external pressure and the need to preserve legitimacy. Instead, certain firms will define their information privacy actions in terms of a deliberate attempt to differentiate themselves from their competitors on the basis of leveraging selective resources into dynamic capabilities. Table 5-3: Resource-Based View and Information Privacy Orientation summarizes my arguments.

IPO and Organizational Goals

Recall that the organizational goal within the Resource-Based View of the firm involves the search for sustained competitive advantage. I argue that this fundamentally involves the search for strategic differentiation and I contend that this differentiation can be achieved through

Table 5-3: Resource-Based View and Information Privacy Orientation

Element	**Resource-Based View Approach**	**Information Privacy Orientation Application**	
		Weaker IPO	***Stronger IPO***
Organizational Goal	Sustainable Competitive Advantage	Strategic differentiation based on superior customer insight	Strategic differentiation based on superior customer trust
Resource	Customer Information as Level 3 resource	Support efficiency focused internal innovation	Support effectiveness focused external innovation
Process	Privacy policies and practices	Information Privacy as an intellectual/knowledge management practice	Information Privacy as a social/relationship management practice
Capability	Information Privacy as a source of information and innovation	Customer Knowledge Capability	Customer Relationship Capability

two different approaches to IPO. In the first instance, firms can strive for differentiation using a customer knowledge capability strategy where the emphasis is placed on the development and deployment of detailed customer information to deliver superior customer insight. For example, these firms would be more likely to focus on obtaining as much detailed information as possible by whatever means and justify their actions based on the need to feed their decision models. In

the second instance, I believe that certain firms will pursue strategic differentiation through a customer relationship capability that emphasizes developing and retaining superior customer trust. These firms would be more likely to gather less rather than more information in order not to alienate their customers. I believe that firms with a weaker Information Privacy Orientation will be more likely to emphasize customer knowledge capability over customer relationship capability than will firms with a stronger IPO.

IPO and Resources

Brumagin's (1994) hierarchy of corporate resources (Table 5-2) demonstrates that not all resources have an equal role to play in the pursuit of sustained competitive advantage. Regardless of the differentiation strategy being pursued by firms, I identify the key resource as "customer information" by definition. The interesting part is identifying the level of resource in play. Whereas within the institutional tradition, I might argue for customer information to be seen as a Level 1 resource (Production and Maintenance - the outcome of transaction processing within the firm's day to day activities), I argue that within the RBV context, customer information represents a Level 3 resource. Recall that Level 3 resources are "Resources that support learning (Innovation and Change) throughout the organization directed to better utilization of corporate assets" (Brumagin 1994:90). I contend that firms gather detailed customer information in order to learn something that they otherwise would not know or could not obtain, and that this learning is applied to achieving some important goals (beyond the mere gathering of data). It is the application to which the resources are directed that is important.

I believe that weaker IPO firms will emphasize the customer information resource as a means to support efficiency focused, internally oriented learning to improve the use of Level 1 and 2 resources. For example, weaker IPO firms will be more concerned to gather as much customer information as possible in order to better target their marketing offerings or deploy their customer systems in order to decrease costs or improve profitability. On the other hand, I argue

that stronger IPO firms will use the customer information resource as a means to learn about better ways to address customer preferences. Brumagin (1994) characterizes this learning as effectiveness focused learning that emphasizes the firm's ability to improve its adaptive capacity in the face of a changing external environment. For example, these firms would be more interested in pursuing privacy regimes that treat the customer information resource as a unique asset important unto itself rather than as merely an input to other firm systems.

IPO and Processes

I suggest that firms will have different information privacy regimes (policies and practices) according to whether they desire to emphasize the intellectual/knowledge aspect of the process or the social/relationship aspect of the process. Firms that emphasize the information aspect of IPO will develop and implement a privacy regime that closely aligns with their information management regime. For example, I expect to find that these firms closely align their information privacy practices with their overall information management practices in order to maximize the efficiencies they can obtain from a disciplined regime. An information rule of thumb would be "if in doubt, collect it and we'll find a way to use it." In contrast, I expect that firms that emphasize the customer privacy aspect of IPO will institute privacy regimes that attempt to maximize the effectiveness of their processes such that only the minimum necessary information is collected in order to preserve their reputation and social ties with customers. In this case, the rule of thumb would be more along the lines of "if in doubt, don't collect." I expect to find that weaker IPO firms pursue information privacy as an information management process while stronger IPO firms would be more likely to pursue a customer relationship process.

IPO and Capabilities

If we accept that customer information is a resource that is managed through a process that renders a capability, then we can distinguish two types of capabilities that firms may pursue in order to achieve sustained competitive advantage. Further, we can locate these capabilities on

the Information Privacy Orientation continuum. I argue that firms that view customer information as an efficiency focused Level 3 internal learning resource and that pursue information privacy as a part of an overall information management regime are firms that are pursuing a customer knowledge capability that is a weaker form of IPO. On the other hand, firms that treat the customer information resource as an effectiveness focused external resource, and implement processes that rank privacy concerns higher in priority than information gathering will be seen to be pursuing a customer relationship capability.

I acknowledge that I have made a distinction between capabilities that do not have to be mutually exclusive. However, I believe that a practical hierarchy exists in which certain firms make decisions based on the information insight to be gained over the privacy concerns and vice versa. It is this distinction that I believe separates stronger IPO firms from the weaker IPO firms within the resource-based category.

In summary, I have explained how the Resource-Based View could be used to explain heterogeneity in IPO among firms. I provided an explanation for the different concepts that make up the RBV paradigm and applied them to a consideration of customer knowledge capability versus customer relationship capability as different avenues for pursuing sustained competitive advantage in firms.

In the last section of this chapter, I synthesize the competing theories I use to explain Information Privacy Orientation in the different firms I examined during the course of my research.

Using Competing Theories to Explain Information Privacy Orientation

Webster and Watson (2002) assert that presenting competing theories to explain organizational phenomena can make an important contribution to IS research. My review of the privacy literature has led me to the conclusion that there is likely not one best explanation for firms' Information Privacy Orientation. Rather, I expect that there are several theoretically sound

explanations for why there is homogeneity and heterogeneity in IPO. Table 5-4 summarizes the competing theories approach I used to examine and explain the differences in firms' Information Privacy Orientation.

Table 5-4: Competing Theories Summary

	Institutional Approach (Acquiescence Strategy)	**Institutional Approach (Manipulation Strategy)**	**Resource-Based View (Customer Information Capability)**	**Resource-Based View (Customer Relationship Capability)**
	Weaker IPO	*Stronger IPO*	*Weaker IPO*	*Stronger IPO*
Organizational Goal argued by theory base	Survival	Survival	Sustained Competitive Advantage	Sustained Competitive Advantage
IPO role in achieving Organizational Goal	Source for Legitimacy	Source for Legitimacy	Support for Differentiation: Intellectual (Knowledge) Resource	Support for Differentiation: Social (Relationship) Resource
Focus of firm activity	Internal	External	Internal	External
Mechanism for achieving Goal	– Reactive – Isomorphism within industry privacy practice	– Reactive – Impression Management to suggest differentiation	– Proactive – Evolution of organizational information management processes	– Proactive – Evolution of organizational privacy management processes

Firms' behaviors should be explainable within either of the Institutional Approach and the Resource-Based View according to the organizational goal – survival (IA) or sustained competitive advantage (IPO). Further, weaker IPO firms within the IA paradigm will display an acquiescent strategy, be internally focused, and will reactively imitate industry privacy practices. Stronger IPO firms within the IA paradigm will be more likely to adopt a manipulation strategy, be externally focused, and to employ impression management techniques to suggest a level of privacy differentiation where none actually exists.

In contrast, the RBV will be used to examine firms that seek to use information privacy as a vehicle for achieving sustained competitive advantage. In the case of weaker IPO firms, I argue that their source for differentiation will be to proactively treat customer information as an input to internally focused information management regimes to achieve superior customer insight. I have labeled this approach "Customer Knowledge Capability." However, I believe stronger IPO firms in the RBV vein will be characterized by differentiation on the basis of an externally focused and proactive treatment of customer information as an important aspect of managing a key social relationship. I have characterized this approach "Customer Relationship Capability."

Chapter Summary

In this chapter I have reviewed the two competing theories that I employed to analyze and explain the differences in IPO I found among the firms I investigated in this research. The Institutional Approach was used to theorize IPO homogeneity while the Resource-Based View was used to theorize IPO heterogeneity across firms.

In Chapter Six, I discuss the research approach and analytical methods I employed in the conduct of this dissertation research.

CHAPTER SIX

RESEARCH METHODOLOGY

My dissertation to this point has emphasized extant theory and the broad literature foundation upon which I based the development of the conceptual model of Information Privacy Orientation. In this chapter, I describe the research methods used and the results obtained in my field research.[1] I begin discussing the ontology, epistemology and research domain that informed my approach. Then I describe the four-phase program of research including the selection and recruitment of research sites, instrument development and validation, and the pilot and main case studies.

Ontology, Epistemology and Research Domain

I believe it is important to locate my approach within the larger paradigms of social scientific research as well as within the disciplinary tradition(s) to which I am attempting to contribute. Creswell (1994; 1998) asserts the necessity of researchers operating reflexively or with self-awareness in order to pursue their inquiries with discipline and rigor. Guba and Lincoln (1994) argue for researchers to specifically address their beliefs with respect to the ontological question (What is my world view? What is the nature of reality?), the epistemological question (What can I know? What is the relationship between what I know and what others know?), and the methodological question (What is the best way for me to discover that which I believe can be known?)

My research was conducted within a postpositivist paradigm (Guba and Lincoln 1994: 109). This paradigm is distinguished by an ontology that argues that there is likely a "real reality" that, while it can only be imperfectly understood, ought to be aimed for as a goal of research. Unlike positivists, who believe in a certain reality that is ultimately knowable and measurable, I

[1] Note that I received approval to proceed with my field research from Queen's University's Research Ethics Board in February 2004.

subscribe to a more nuanced view that such reality as there might be in social science, is difficult to discern and is as likely to be misunderstood as not. Consequently, my epistemological perspective leans to the objective as a "regulatory ideal" (Guba and Lincoln 1994: 110) without denying the need for taking a critical stance in evaluating knowledge claims (my own and others') and recognizing the importance I place on the situatedness of knowledge. In other words, context matters to me and contributes to the selection of qualitative methods as my primary research approach in this dissertation. I conducted case studies of three Canadian financial institutions using a multi-methods approach that leaned heavily on interpretive analytical techniques (Orlikowski and Baroudi 1991) to answer the research questions posed in Chapter One.

I further locate my information privacy orientation research within a tradition grounded in the view that the purpose of MIS research is to bring into focus the "rich phenomena that emerges from the interaction between ... technology [and] the social setting" (Lee 1999:459). I draw on research conducted in information systems and several "reference disciplines" (Keen 1980) including marketing, ethics, strategy and organizational behavior to address information privacy as a social phenomenon that, as a consequence of technological innovations, cuts across organizational functions, industries and societies. I believe that this approach to identifying and understanding information privacy orientation in selected Canadian financial institutions will contribute to the information privacy research stream of several disciplines, particularly MIS and marketing.

Research Methodology Overview

I conducted my research in four phases. Table 6-1 summarizes the research methods and analytical approaches I engaged to accomplish my research goals within each phase.

Table 6-1: Summary of Research Program

Research Phase & Timing	Research Question	Data Collection / Development Approach	Data Analysis Method / Validation Approach
Phase One – Privacy Policy Evaluation Study (Winter 2003-2004)	(R1) IPO definition and IPO continuum	• Capture websites for 10 Canadian Financial Institutions • Download privacy policies	• Interpretive – comprehensiveness, readability, attitude to privacy • Seek evidence for IPO definition • Seek evidence for IPO continuum placement
Phase Two – Instrument Development and Validation (Spring 2004)	(R1) IPO definition and continuum (R2) IPO construction in firms (R3) Institutional Theory (R4) Resource-based Theory	IPO Interview Guides • Interview questions mapped to research questions IPO Survey • IPO survey items developed according to IPO concepts (see C. 4) • IPO typology development	IPO Interview Guides • School of Business academics and external privacy experts IPO Survey • Four rounds of card sorts • School of Business academics and external participants
Phase Three – Field Research and Within-Case analysis (Summer and Autumn 2004)	(R1) IPO definition and continuum (R2) IPO construction in firms (R3) Institutional Theory (R4) Resource-based Theory	Pilot Study & Main Case Studies • Interviews – face to face and telephone • Surveys – paper and web-based • Documents - copies retained and items read on site	Pilot Study & Main Case Studies • Interviews - Interpretive, pattern-matching review of transcripts • Surveys – descriptive statistics (SPSS) • Documents - Interpretive, pattern-matching • Triangulation for within-case analysis to establish placement on IPO continuum
Phase Four – Cross-Case Analysis (Autumn 2004)	(R3) Institutional Theory (R4) Resource-based Theory	(No new data to be collected.)	• Interpretive, pattern matching • Triangulation to: - Seek evidence for Institutional Theory - Seek evidence for Resource-based Theory - Establish relative placements on IPO continuum

Recall that I defined Information Privacy Orientation as:

> *the principles, values, decision rules, policies, and desired objectives that organizations adopt to guide them in the collection and use of their customers' personal information (Greenaway, Cunningham & Chan 2002).*

Also, readers are reminded of the research questions identified in Chapter One, which are specifically addressed by the multiple case studies[2]:

1. (R1) Do firms have an Information Privacy Orientation?
2. (R2) How is Information Privacy Orientation constructed in firms?
3. (R3) To what extent does the Institutional Approach help us to explain homogeneity in information privacy orientation across firms in the same industry?
4. (R4) To what extent does the Resource-Based View help us to explain heterogeneity in information privacy orientation across firms in the same industry?

I conducted my "intensive research" (Weick 1984 as quoted in Markus and Lee 1999:35) in four phases during the period of December 2003 to September 2004. Phase One (Privacy Policy Evaluation Study) was conducted in the winter of 2003-2004. Phase Two (Instrument Development and Validation) was conducted in the spring of 2004. Phase Three (Field Research) was conducted from June to September 2004. Phase Four (cross-case analysis to apply the competing theories) was conducted in the autumn of 2004. In the next section I describe the Privacy Policy Evaluation Study which constituted Phase One.

Phase One: Privacy Policy Evaluation Study

In this section I describe the Phase One study's purpose, sample, data collection and data analysis approaches. The study's findings are discussed in Chapter Seven. Appendix J provides the firm by firm results.

Study Purpose

The purpose of the Phase One study was to address research question R1 – Do firms have an IPO? A secondary question involved whether there was discernible variance among the IPOs

[2] Research Questions R5 and R6 are outside the scope of this immediate discussion as the primary interest of this research concerns the focal variable – Information Privacy Orientation.

for different financial institutions. There were five goals for the study to support the research question:

1. Document the customer information privacy polices and practices that were publicly announced on the websites of selected Canadian financial institutions in the winter of 2003-2004.
2. Using the information obtained, apply the IPO Definition to each site to determine the extent to which data can be collected to support the definition and distinguish among different organizations.
3. Using the information obtained, assess the placement of each organization on the IPO Continuum.
4. Determine the variance in IPO across the study sample.
5. Establish a list of potential sites for case study research to be conducted in Phase Three.

Sample

The Phase One Study followed a "criterion" sampling logic (Paré 2004). I evaluated the information privacy policies of ten Canadian financial institutions including nationally chartered banks and provincially regulated credit unions. I selected the Canadian financial institutions sector for four reasons. First, as an exploratory study, it was important to control for industry effects (McGahan and Porter 1998) in order not to confound the analysis. Second, previous research has established that personal financial information is one of the most sensitive areas of concern for personal information privacy (Dinev and Hart 2003; Sheehan and Hoy 2000). This suggested that the study would approach the privacy topic from a "conservative" perspective. Third, I chose Canadian firms in order to control for the legal environment and national culture. Last, I have some experience with and contacts in this sector which increased the likelihood that I would be able to recruit research sites.

Data Collection

The data for this study consisted of the privacy policies posted to the websites of ten Canadian financial institutions. I included the privacy information connected to the "privacy" link from the homepage as well as any additional information that was linked to the privacy section of

the website. For example, some firms link the privacy and security sections of their websites; others link their privacy information to external groups such as a regulator.

I recorded the information about the privacy policies posted to the websites of the ten Canadian financial institutions using the Privacy Policy Evaluation Form (Appendix J-1).

Data Analysis

The findings for each of the ten sites evaluated in this study are contained in Appendix J-1.1. I evaluated the data as follows. First, I reviewed the privacy policies for each organization against three criteria: *comprehensiveness* (how well and in-depth is the policy explained); *readability* (how easy is it understand the policy and its implications); and *attitude to privacy* (what messages are being conveyed by the policy). This analysis combined interpretation with statistics (such as readability scores). Second, I operationalized the different aspects of the IPO definition. Then I coded the privacy information in order to discern the extent to which the different aspects of the IPO Definition could be identified. Third, I re-coded the privacy policies using the IPO Continuum layers and categories (based on the definitions given in Chapter Four). I mapped all evidence onto individual IPO Continuum charts. Fourth, I summarized these findings onto a Master IPO Continuum chart to ascertain the variance across these financial institutions. Based on these findings, I prepared a "wish list" of potential research sites.

Summary – In Phase One of this dissertation research, I studied the privacy policies posted to the websites of ten Canadian financial institutions. Based upon my interpretive analysis of the policies, I concluded that each firm had an identifiable IPO (based on the IPO definition) as well as an identifiable position on the IPO Continuum. I used this information to identify the potential sites for the main case studies.

In the next section, I describe how I developed and validated the Interview Guides and IPO Survey Instrument used in this dissertation research.

Phase Two: Instrument Development and Validation

In this section, I provide an overview of how I developed and validated two categories of instruments to use in my field research - a series of Interview Guides and the IPO Survey, which comprises three sections of questions dealing with different aspects of the IPO Continuum.

Interview Guides

Purpose: The interview process was structured to address research questions R1 through R4. As is typical with most case studies and, given the exploratory nature of my research, I employed semi-structured interviewing as the primary data collection method (Yin 2003). Semi-structured interviews are useful for a researcher who "knows most of the questions to ask but cannot predict the answers" (Paré 2004:247). This process was more likely to yield fundamental insights into the decision-making context in which the case study companies developed their privacy policies (Fink 1995). Therefore, I needed to develop and validate guides to use at the research sites. The guides would serve three purposes. First, they would help me to keep track of the conversations over the course of the interview, as well as provide a template for taking notes. Second, they would provide a means for comparison of responses within the case. Third, they would provide a means for assessment across the cases.

Development and Validation: The Information Privacy Orientation Interview Guides (IPOG) were developed from a set of core questions to address contextual aspects of IPO and the different research questions. I distributed them across the range of types of organizational positions that I was hoping would be available to be interviewed at each site. I proceeded to validate these guides in two stages. First, I mapped the draft interview questions and follow-ups/probes against the overarching research questions and anticipated interviewee (i.e., Chief Privacy Officer, Legal Counsel, Marketing VP, etc.). Second, I pre-tested the IPOGs and IPO Survey simultaneously through people with a wide variety of privacy expertise (such as privacy

consultant or privacy manager) and functional experience (such as marketing or IT). The feedback I received from the pre-test was grouped into two categories – content and construction – and instigated several changes to the instruments. Details on the validation process and the specific changes suggested and actions taken are addressed in Appendix H. The revised guides used in the field pilot test appear as Appendix H. The pilot study results are reported in Chapter Eight.

Survey Instrument

Purpose: The second data collection technique I used in this research was a survey (Information Privacy Orientation Survey – "IPOS"). The survey addressed research questions R1 and R2. I selected a survey as a second data collection method for two reasons. First, interviewing can be very subjective for both the interviewees and the researcher. A survey is relatively objective, in comparison, and thus serves as both a counterpoint to and a source for reinforcement of findings from the interviews. Second, a survey provides for very specific comparisons to be made both within and across cases. In both instances, the survey supported my triangulation analytical strategy.

The IPOS was drafted to reflect the IPO as a multi-tiered continuum based on the marketing ethics continuum (Smith 1995). The individual items addressed four distinctive categories (weaker to stronger IPO) within each of the four sub-constructs that made up the tiers of the continuum (Customer Relationship Stance, Information Management Strategy, Privacy Philosophy, Privacy Behaviours). The IPO survey was designed to be in three parts:

1. IPO Continuum - The purpose of this section was to collect data specific to the layers and categories of the IPO Continuum.
2. IPO typology - The purpose of this section was to collect data to assess whether a single typology could be devised to capture the nuances of IPO in short paragraphs.
3. Demographic data about respondents - This data would help me to assess if responses to the previous sections had discernible patterns based gender, age, education, position, etc.

The development and validation of the three separate sections is discussed below.

Development: The development of the survey reflected its three separate parts. The first section addressed specific characteristics of IPO. I developed 16 statements per IPO sub-construct based on the IPO Continuum model explained in Chapter Four. Responses were categorized using a seven-point Likert-type scale (DeVellis 1991). The second section, IPO Typology, summarized the vertical categories of the IPO Continuum. I developed these "ideal type" categories following the Miles and Snow Strategic Types (1978), a well known typology in the strategic management literature. The third section, demographics, was developed using standard models used in company based research. The covering letter was written in accordance with Queen's University's General Research Ethics Board's requirements (tailored to a business audience). The layout for the survey was designed according to the guidelines for surveys established in Salant and Dillman (1994) and was intended be offered as a traditional "paper and pencil" exercise. In the end, however, I was able to offer the survey in both paper and web-based formats.

Validation: The IPO survey instrument was reviewed for face validity by two faculty members and two graduate students. Each reviewer provided feedback on the structure and wording of the instrument and suggested alternatives. Improvements to the draft instrument were made based on the comments received. On the whole, the draft instrument was considered to have acceptable face validity and the decision was made to proceed to formal validation through a card sort process (Moore and Benbasat 1991). The first version of the IPO survey instrument appears in Appendix H-9.

The Continuum items of the survey were further reviewed through a series of four card sort exercises using professors, graduate students, and business professionals. For details and a discussion of the results of the card sorts, see Appendix H-10. After having reviewed the transcripts for the debriefings for all four rounds of card sorts, and in consultation with my supervisor, it was decided that further card sort rounds were unlikely to yield additional insights. We decided that pre-testing of the revised instrument with knowledgeable experts would be more productive. The pre-test process is described below.

Pre-Testing the IPO Survey Instrument: IPO Continuum

The pre-test of the IPO Survey Instrument took place simultaneously with the pre-testing of the IPO Interview Guides (as discussed above). I had two objectives for this phase of the IPOS validation process – content and construction. First, I wanted to ascertain whether the instrument was comprehensible, addressed issues of interest to business people, could be completed without too much cognitive difficulty, and similar content issues. Second, I wanted to assess the flow of the items, layout, clarity of instructions, and similar construction issues. These follow Salant and Dillman (1994) requirements. I will address the content and construction results of the pre-test in turn.

IPO Survey Instrument – Content: In all cases, the participants expressed confidence that the topic of Information Privacy would be of interest to business people, in general, and financial institutions personnel in particular. In addition, they indicated that the items in the survey raised important questions. Generally, the comments were positive about the wording of the items and that the level of language was appropriate. There were some specific suggestions for improvement in content. Appendix H-12 summarizes the suggestions and the action taken (if any).

IPO Survey Instrument – Construction: There was general agreement that the layout was adequate and that the participants would be able to make clear choices when responding to the items. Some minor typographical errors were pointed out. There were two main instrument construction issues raised by the expert reviewers – the rating scale and order effects.

A participant raised the issue of whether the 7-point Likert type scale was a useful approach for business people completing the survey. It was suggested that a more meaningful alternative would be to use words like "Sounds like my company" or "Doesn't sound like my company." I asked the experts in subsequent interviews if they agreed with this observation. Most thought the alternative wording was worth considering. I attempted to reword the rating scale and

circulated it for comment by several MIS faculty with survey expertise. This alternate approach was rejected. My supervisor and I decided to continue to use the 7-point Likert type scale.

A second construction issue concerned the potential for order effects to influence respondents. For example, the items in the IPO Survey instrument that they reviewed faithfully followed the continuum categories sequencing. This meant that each section began with the "weakest", "negative" or "worst case" items and proceeded to the "stronger", "more positive" and "best case" items. Several of the expert reviewers volunteered that they thought that leading each section with negative statements might discourage completion or lead respondents to not read carefully and hence not answer "correctly". Because order effects can significantly bias responses (Bradburn 1983: 303) I altered the order of the survey items. However, I was also concerned not to create a cognitive burden (Bradburn 1983: 304) by completely randomizing all 64 items. I discussed this issue with three committee members and we were all of the opinion that managers respond better to groupings of similar items rather than a totally randomized and therefore cognitively difficult approach. I decided to maintain the integrity of each sub-construct and to only partially randomize the items. Given that there are four items for each of four categories per construct, I reordered the items intobblocks of four similar items. As a result, I created four different versions of the IPO Survey, and these four versions were pilot tested.

Pre-Testing the IPO Survey Instrument: IPO Typology

The IPO typology consists of four short descriptive paragraphs that provide a summary of all the different conceptualized characteristics of IPO. The typology was pre-tested using three knowledgeable experts – the Privacy Compliance Manager and Director, Public Affairs indicated in the previous table as well as a Faculty Member familiar with the research. All three read through the paragraphs. Their comments were very similar and rested on three points. First, they liked the idea of a typology and agreed that it would be interesting to see if there was a relationship between the typology and the answers offered in the IPO Survey section dealing with

the individual constructs. Second, while the language was seen to be appropriate, there was some concern expressed that the typology might look intimidating as presented. "It's a lot to read," was a typical comment. However, there were no suggestions for improvement. Third, there were concerns expressed that the typology added significantly to the amount of time required to complete the survey and that this could be a problem. However, they thought it was worth keeping the typology, at least through the pilot stage, to see what resulted. I decided to retain the typology as is; testing it would confirm whether it could contribute to our understanding of information privacy in firms.

Pre-Testing the IPO Survey Instrument: Demographic Data

The final page of the IPOS asks for demographic data. This data includes gender, age, level of attained formal education, years with the company, type of position, location of position, whether training had been received on privacy laws and the company's privacy policies, and whether implementing privacy policies formed part of the performance expectations for their position. The data was collected only for statistical control purposes. The final selection of items and layout was based on consultations with three other PhD candidates using survey methodologies in their dissertation research. The expert reviewers did not have any comments for improvement.

The first version of IPOS is contained in Appendix H-9 and the revised version used in the Pilot Test is in Appendix H-14 as well.

IPO Survey On-Line Version

It is appropriate at this point to indicate that a web-based version of the IPO Survey was developed in response to requests from participating research sites. The firms noted that their staff would be more likely to complete a web-based version of a survey rather than a paper-and-pencil version. The literature on the differences between responses to paper and pencil versus on-line surveys suggested that issues with conducting research using both versions could be

mitigated (Webster and Compeau 1996). On the advice of a Committee member, I arranged with a Unix programmer/developer (with extensive experience developing academic surveys) to develop an on-line version. This version closely paralleled the paper-and-pencil version in several important ways including having multiple items presented per screen, allowing users to back track, allowing changes to previously completed items, and allowing respondents to complete the survey at their own pace (Webster and Compeau 1996: 575-576).

I provided the programmer with a soft-copy for each of the four survey versions (including the cover letter and final page) and these were converted into an online format. Appendix H-15 provides the screen shots of the on-line version. The on-line survey was tested by six individuals – three graduate students at the Business School who are familiar with the research (two of whom had assisted with previous validation exercises and one of whom connected from an off-campus location) and three business people (all of whom connected remotely to the test site from non-Ontario locations). All provided helpful comments ranging from catching typographical errors to layout issues. I exchanged emails with the developer until I was satisfied that the paper-based and web-based versions were essentially similar. The opening screen and closing screens (which mimicked the cover letter and closing page) were customized for each site. The developer set the program to assign different versions of the survey to ensure a reasonable distribution across the four versions. A unique domain name and a password were assigned for the individual firms. In the end, only one research site used the on-line version. Further information is provided in Chapter Eleven (Case D) and the related Appendix N.

Section Summary: In this section, I reviewed the processes of developing and validating the IPO Interview Guides and IPO Survey instrument. The Guide was developed based on my understanding of the contexts in which organizations determine the relationship among three words – customer, information and privacy. The different guides were revised based on two validation rounds – one internal to the School of Business and one using eight outside subject matter experts. The IPO survey instrument, despite being of secondary consideration in this

research, was likewise subjected to a thorough construction and validation process through card sorting and pre-test scrutiny.

In the next section, I provide an overview of the field research I undertook as Phase Three of my research program.

Phase Three: Field Research

In this section, I introduce the field research conducted in Phase Three, including the Pilot Study (case A) and multiple case study (Cases B,C,D). I describe my site recruitment methods and briefly discuss the on-site research activities. I also explain the techniques I used for interviews, documents and survey analysis.

Purpose

The purpose of the multiple case study research was to "go behind" the previously documented information privacy policies and practices announced on the websites in order to investigate in detail the decisions made by the selected financial institutions. These case studies assisted me to address all six research questions but through different mechanisms, as explained below. The case studies were carried out in the summer of 2004.

Yin (1980, 1994) defines a case study as a research strategy that offers deep insight into "contemporary phenomenon in its real-life context." A further benefit of the case study method is that it provides for the inclusion of the firm's personnel's perspective on the phenomenon through interactions with the researcher (Leedy 1997). In IS research specifically, case studies are seen to be "well suited to capturing the knowledge of practitioners" especially as research questions move "from technological to managerial and organizational questions" (Benbasat, Goldstein and Mead 1987:370). Furthermore, Paré (2004:259) argues that "qualitative research ... remains the best approach available for studying complex phenomena like ... emerging IT management issues."

Recruiting the Research Sites

I undertook two recruitment stages. The first stage was to secure a financial institution to serve as the site for pilot testing. I secured, through personal contacts, a financial institution not included in the main study. The second stage involved recruiting four financial institutions that represented different IPOs based on the Phase One study. I will discuss each stage in turn.

Pilot Study Site: I decided that it would be preferable to attempt to recruit an FI not included in the Phase One study (in order not to diminish my ability to gain access to a "priority" firm). As the purpose of the study was to test the different approaches and instruments, it was less important that I had previously studied the firm.

A regional financial institution in Canada with retail banking as one of its lines of business was recruited for the pilot test. I was "sponsored" by a senior marketing executive but negotiated entry with the Project Manager for Compliance Initiatives ("Project Manager") who is located in the Sales Operations division. This individual reports to the bank's Chief Privacy Officer. We agreed on the wording of a Confidentiality and Non-Disclosure agreement and arranged for a three-day site visit. The Project Manager and I exchanged a series of telephone calls and emails in which we discussed the range of potential interview subjects available and agreed upon an approach. The Project Manager contacted the interview subjects and arranged the meeting schedule. The company and its staff were very welcoming and provided meeting facilities. The pilot site visit was conducted June 1-3, 2004 at the company's head office complex. The Project Manager attended the majority of the interviews (this had been a condition of agreement to participate). I do not think that this person's presence unduly affected the openness of participants.

Main Case Study Research Sites: I had initially identified four desirable research sites based on the findings from the Phase One study (3,4,5,7). On the advice of my supervisor, I invited all companies included in the Phase One Study to participate (in order to ensure that I was

able to recruit four sites). I also contacted two other financial institutions (one bank and one credit union) not included in the Phase One study but for whom I had contact information for senior executives. I reasoned that I could always undertake an initial placement study fairly quickly if I needed to use either of these "convenience" sites.

All twelve firms were couriered an initial information package that included a covering letter, a summary of the research objectives, and two Queen's School of Business publications that I thought might be of interest. Appendix I includes the generic information package. Wherever possible, I contacted either someone with whom I had a current or previous professional relationship or an individual recommended to me by, for example, a trade or professional association. In certain cases, these more "personal" contacts were able to identify, and in some circumstances serve as, advocates for their firms' participation. I followed up with telephone calls and email messages at regular intervals.

My initial recruitment efforts secured three research sites (4,7,10). While this set did not constitute my ideal collection of cases, each site appeared to offer a different approach (based on the mapping conducted in the Phase One Study). I considered that there was adequate apparent variance among the three firms to warrant proceeding with them. I scheduled the research visits with these firms and continued my efforts to secure a fourth site over the course of the summer. However, I was unsuccessful. My supervisor and I decided to proceed with concluding the dissertation with the three research sites as we agreed that considerable insight was available from them. The main reasons given for declining to participate (if any were offered) were, first, the amount of time and effort required to secure participation of senior executives, and, second, the perception (by the contact person) of a likely lack of interest in the topic by senior managers. It may be that the rigor (i.e., multiple methods approach) I brought to this study served as an impediment to participation.

Once agreement to participate was achieved, I provided the firms' contacts with information about the site visit as well as the text for a Confidentiality and Non-Disclosure

Agreement[3] (Appendix I-5). I had a series of telephone and email exchanges with the sites to settle logistics and negotiate issues such as who would be recruited for interviews, the development of a survey participant list, and access to documents. In all cases, the firms provided meeting facilities as well as work space, recruited the interview participants, and provided mailing labels (for distribution of paper based surveys) or sent out a targeted email communication (for encouraging participation in the web-based survey). Table 6-2 summarizes the site visit schedules.

Table 6-2: Site Visit Schedules

Case	Dates for Site Visit	Dates for Survey
A (pilot)	June1-3, 2004	July 15 – 30, 2004
B	July 12-15, 2004	July 15 – July 30, 2004
C	July 18-22, 2004	
D	Aug. 16-20, 2004	Aug.27 – Sept. 15, 2004

Data Collection

Table 6-3 summarizes the data collection methods by research question and the information sources. I used three primary modes of data collection. First, I conducted semi-structured interviews with senior managers and other staff in the respective firms. Second, I distributed the IPO survey to the interview participants (and others subsequently identified). Third, I collected and analyzed privacy related documents (i.e., training manuals, policy manuals). I chose this multiple methods approach to increase the construct validity (Yin, 1994) and to reduce the effects of researcher bias in interpreting findings (Leedy 1997). In addition, the particular methods used in this study supported the "triangulation strategy" to deepen understanding of the information privacy phenomenon under study (Jick, 1979; Yin, 1994). These data collection methods are elaborated in the section below.

[3] The text of the Agreement was based on the wording I had negotiated with the Pilot Site.

Table 6-3: Summary of Data Collection Methods

Data Collection Method	Research Question Addressed	Information Sources
Semi-structured personal interviews	Primary • (R1) existence of IPO • (R2) construction of IPO Secondary • (R5) context of IPO • (R6) outcomes of IPO	• Key senior managers (i.e., Chief Privacy Officer, Chief Information Officer, Senior Marketing Executive, Senior Legal Officer, Senior Administrative Officer, etc.) • Others as identified during course of the study
Information Privacy Orientation survey	Primary • (R2) construction of IPO Secondary • (R5) context of IPO	• Key senior managers (as above) • Additional participants as determined during course of the study
Documents	Primary • (R1) existence of IPO • (R2) construction of IPO Secondary • (R5) context of IPO • (R6) outcomes of IPO	• As identified in interviews, through website, etc.

Research Site Activities: The pilot and case sites were geographically dispersed across the country and visits varied in length from three to five days. I travelled to each site on a Sunday and met with the Project contact early Monday morning. At that initial meeting, we reviewed the interview schedule and I gained some background information about each participant (such as position in the firm and its privacy relevance). This information helped me to try to match the different interview guides to the interviewees. The seniority level of participants varied from site to site. This was due to two factors. One, while I had attempted to gain access to senior manager and executive levels, this was not always what the Privacy Contact recommended or was able to deliver. In the end, I think it was more important to cooperate with the firms than to try to take a hard line about the interview processes. Second, I was conducting the research at the height of the summer. At one level, firms were a bit more willing to spend time on a non-essential activity. However, it also meant that staff levels were reduced. I am grateful that, despite summer holiday schedules and the attendant inconveniences, the participating firms were generous in offering

what staff they could to assist my research. I am convinced that the people I dealt with provided a broad perspective and offered useful information, in every case.

In general, I conducted interviews, collected documents and posed questions to project contacts throughout the days at the site location. In the evenings, I skimmed and sorted documents and entered them into the database. I did "quick and dirty" transcriptions from my handwritten notes for the interviews I was unable to audiotape. I also tried to maintain a diary of activities. The Appendices for the separate cases contain information from the separate case study databases including information on who was interviewed, what documents were selected and the approach taken to distributing the IPO survey as well as survey statistics.

Interviews: Table 6-4 summarizes the interview activity by case site. I conducted formal interviews with staff at Head Office locations, and, in two cases, also with regional and branch personnel, usually at their work locations. While the majority of interviews were conducted face-to-face, a few were of necessity conducted by telephone. In addition, some interviews were conducted with two or three participants. This approach, while not ideal, made it possible for me

Table 6-4: Summary of Interviews Conducted

Research Site	# of Interviews	# of Staff interviewed
B	16	20
C	14	14
D	20	20
Total	50	54

to interview people I might not otherwise have met. I believe that I was able to manage the dynamics successfully. Most interviews were audio-taped. (I experienced some technical problems but had extensive handwritten notes as a back up.) All interviewees signed consent forms (attached to the Confidentiality and Non-Disclosure Agreement as Schedule A).

In as many interviews as possible, I used one of the IPO Interview Guides. However, there were instances where the guide was not useful and I pursued lines of inquiry that were more suited to the participants' interests and expertise. For example, the Interview Guide for Marketing

(which emphasized customer issues) was not too useful with staff working with marketing databases. Their concerns were related to marketing techniques (such as data mining) and the limitations that the consent provisions of the privacy legislation had for their operations. As well, it was apparent to me that working with staff in the headquarters of a chartered bank was very different from working with the head office staff of a regional financial institution. The bank staff were even further removed from "customers" than their regional financial institution counterparts. This rendered some exercises (such as the "reality TV" game) less useful. Given the exploratory nature of this research program, I was not too surprised or concerned that the Interview Guides were not uniformly useful. I believe that the interview techniques I employed helped overcome any challenges and that valuable data was collected despite these difficulties.

I also had several additional conversations with the Project Contacts for context, checks on "reality" and on my "instincts", and for additional information. Details of the interview subjects and questionnaire guides are contained in the specific case appendices.

Documents: Table 6-5 summarizes the documents collected or reviewed by case site. My access to documents varied from site to site. One firm provided relatively unfettered access to a wide range of documents and agreed that I could take photocopies of any that I chose. Another site was more controlled but very cooperative in providing documents that I requested (either by name or subject) and, in most cases, permitted me to take photocopies. Another site was quite restrictive. Publicly accessible information was provided (most of which I had already collected). However, over the course of the week, the firm agreed to allow me to read an extensive array of documents and I took handwritten notes on a few essential items.

Table 6-5: Summary of Documents Collected

Research Site	# of Documents Collected	
	Documents	Pages
B	76	642 (approx)
C	67	427 (approx)
D	8	50 (approx)
	151	1,119

Overall, I collected or reviewed more than 160 privacy related documents across the sites. The contents ranged from organization charts to the Privacy Project Charters, as well as training materials, policies and procedures circulars, and internal assessment and audit reports.

For each site, I sorted and catalogued the documents into six categories - general organizational, privacy implementation process (internal), privacy policy and procedure (internal), privacy external (financial institution industry), privacy external (government), and privacy external (other). Details of the documents used in each of the case analyses are contained in the specific case appendices.

Surveys: Table 6-6 summarizes the IPO survey activity at each case site. I was able to distribute the IPO survey without difficulty at two of the three main case sites. One site distributed 54 "paper and pencil" survey kits (divided among the four versions) that I had prepared in advance of the site visit. (I would have preferred to offer the site an online survey but was unable to complete the necessary testing by the time of this visit). Another site solicited participation in the web-based version of the survey from 50 identified personnel. The third site experienced timing difficulties (their firm had a series of staff surveys already planned), and despite negotiations, I was unable to secure agreement for timely distribution of the survey. Each site was offered a completion incentive of a $100 donation to a charitable organization supported by the company.

Table 6-6: Summary of IPO Survey Activities by Main Case Site

Research Site	Survey Type	#of Surveys distributed	Total Completed Surveys	
			#	%
B	Paper	54	33	61
D	Web	50	17	34
		104	50	48

In summary, I conducted on-site research for the main multiple case study at three different financial institutions. In total, I interviewed 54 staff, collected over 1,000 pages of

privacy and related documents, and distributed 104 surveys, of which 48% were returned completed. I will now describe the techniques I used to analyze the data.

Data Analysis

I employed an *interpretational approach* to analyze the data (Leedy 1998) by emphasizing themes and patterns that helped to explain the phenomenon of information privacy orientation in each case. However, the different data collection modes required distinct analytical approaches as summarized in Table 6-7.

Table 6-7: Summary of Analytical Techniques by Data Collection Method

Data Collection Method	Analytical Technique
Semi-structured personal interviews	• Intentional analysis • Confirmation and clarification of transcripts by respondents • Manual high level coding of transcripts • Coding schema – Policy Assessment, IPO Definition, IPO Continuum
Survey	• Descriptive statistics
Documents and artifacts	• Intentional analysis • Manual high level coding of transcripts • Coding schema – IPO definition, IPO Continuum
Case study database	• Comparisons and pattern matching across cases

Interviews: The interview data was analyzed according to the interpretivist approach defined as "intentional analysis" (Lacity and Janson 1994). Intentional analysis is characterized as a means to discern the subject's intentions and is particularly useful when analyzing interview transcripts. Second, it assumes that the researcher is sufficiently familiar with the era in which the research is taking place so that language and cultural issues are minimized. Lacity and Janson (1994:151) describe a process that depends on discerning both facts and intentions by sifting the data for themes from which to abstract the "essences of the text." This mode of analysis was used by Lacity and Hirscheim (1993) to analyze interviews concerning IS outsourcing decisions.

The successfully audio-taped interviews were transcribed by an assistant. I transcribed my handwritten notes for the interviews that had not been taped. (I would have preferred to have the individual transcripts verified by the subjects. However, firms were not willing to devote this additional time. Their primary interest lay in receiving a management report [a condition of agreeing to participate] and to minimize the demands on their time. While this is an unfortunate circumstance, I stand by my research based on the number of interviews (transcripts), documents and surveys I was able to secure.) Then the transcripts were reviewed manually to identify top level themes, key words and patterns. The first task was to describe the privacy program stage for each site. Then I assessed the privacy program (comprehensiveness, readability and accessibility). The next step involved establishing patterns against the IPO Definition (principles, values, objectives, policies, decision rules). Then the material was reviewed a final time for data to populate the IPO Continuum (customer relationship stance, customer information management strategy, customer information privacy philosophy, customer information privacy behaviors). I validated my interpretations by having another researcher (e.g., my supervisor or a fellow PhD candidate) code a sample of the transcripts.

Survey: The IPO Surveys were analyzed primarily to examine within-firm variation. The survey analysis was conducted using SPSS to generate descriptive statistics. Given that the IPO Survey is of secondary interest in this research, I refrained from performing inferential statistical analysis (such as structural equation modeling) at this time. However, I anticipate this as part of a future research agenda. In addition, I also took into consideration feedback from the case sites about the survey.

Documents: Finally, the various documents I collected were reviewed in three rounds. First, I reviewed them to ascertain whether they primarily contributed to addressing the first two (R1, R2) or last two (R5, R6) research questions. (If the latter questions, the documents were not analyzed in detail but skimmed only to identify top level contextual information. These data will be set aside for future detailed analysis. The remaining documents were reviewed and coded

according to the high level schema developed for the analysis of the interviews – IPO Definition and IPO Continuum.

Case Study Database: Qualitative analysis is rarely linear. It represents an interactive and cyclical process with the researcher moving between different data and attempting to discern broader trends (Leedy 1997). This is a taxing and messy process that requires discipline and attention to detail. To aid me in keeping track of the enormous amount of data generated by this research, I implemented a database for each firm to ensure that all data, coding and interpretations were properly tracked. This helped me to maintain "a chain of evidence" and increased the reliability of this multiple case study (Yin 1994:98). Evidence for the case study database for each research site (Cases A, B, C, D) appears in separate Appendices (K, L, M, N).

Section Summary: In this section I have introduced the field research constituting Phase Three of this dissertation. I described the research sites selection and entry. I detailed the data collection methods – interviews, survey, and documents. Lastly, I provided a brief overview of techniques I used to analyze the different types and data. Throughout this section, I demonstrated how these approaches addressed the different research questions I posed as the raison d'être for the research.

Phase Four: Cross-Case Analysis

The primary purpose of Phase Four – Cross-Case Analysis was to specifically address research questions R3 (IPO homogeneity) and R4 (IPO heterogeneity). Again, this was largely an exercise in interpretation. I adopted an objective stance with which to present the findings but, to the greatest extent possible, I used direct quotes from the interviews and documents to supplement and give life to my interpretations.

The method used in Phase Four extended the triangulation process by using the three within-case analyses as the data for the final, cross-case analysis. I prepared three charts for assessing the cross-case data. The first chart addressed the IPO definition and IPO Continuum

data for each main case site. I used this chart to map information and assess variation across the cases. The second chart operationalized the key aspects of Information Privacy and the Institutional Approach – organizational goals, sources of pressure, ability to respond, and response strategies – as outlined in Chapter Five. The third chart likewise operationalized the key aspects of Privacy and the Resource-Based View. Based upon this analysis, I drew my conclusions about the relative contribution of these two theories to our understanding of Information Privacy Orientation as an organizational phenomenon. Chapter Twelve presents the detailed analysis and discussion of the cross-case findings.

Chapter Summary

In this chapter, I described the research methods and analytical approaches I used in this dissertation research. First, I discussed the ontology, epistemology and research domain of this research. Second, I provided an overview of the four phases of the Research Program. I described the purpose, sample, data collection and analytical strategies for the Phase One Privacy Policy Evaluation study. Then I described the Phase Two activities which involved the development and validation of two research instruments – the Interview Guide(s) and the IPO Survey. Then I described the field research conducted in Phase Three including the Pilot Test and three Case Studies. I described my site recruitment methods and entry activities, and provided an overview of the on-site research activities. I also briefly described the techniques I used for interview, document and survey analysis. Lastly, I described the approach taken in Phase Four, the "cross-case" analysis of IPO.

The next chapters of this dissertation report the findings of the empirical studies conducted in this research program. Chapter Seven reports the findings of Privacy Policy Evaluation Study. Chapter Eight explains the findings from the Pilot Site (Case A) while Chapters Nine, Ten and Eleven address the detailed within-case findings for Cases B, C and D respectively. Please note that the order of the case presentation follows the order in which the

research was undertaken. The identification of the cases is unrelated to the identification of sites from the Phase One Study. The next chapter provides a detailed recounting of the Privacy Policy Evaluation Study conducted in Phase One.

CHAPTER SEVEN

PHASE ONE: PRIVACY POLICY EVALUATION STUDY

In this chapter I describe in the purpose, sample and findings of the Privacy Policy Evaluation Study which constituted the first Phase of the research program.

Study Purpose

The purpose of the Phase One study was to address research question R1 – Do firms have an IPO? A secondary question involved whether there was discernible variance among the IPOs for different financial institutions. There were five goals for the study to support the research question:

1. Document the customer information privacy polices and practices that were publicly announced on the websites of selected Canadian financial institutions in the winter of 2003-2004.
2. Using the information obtained, apply the IPO definition to each site to determine the extent to which data can be collected to support the definition and distinguish among different organizations.
3. Using the information obtained, assess the placement of each organization on the IPO continuum.
4. Determine the variance in IPO across the study sample.
5. Establish a list of potential sites for case study research to be conducted in Phase Three.

Sample

I evaluated the information privacy policies of ten Canadian financial institutions including nationally chartered banks and provincially regulated credit unions. I selected the Canadian financial institutions sector for four reasons. First, as an exploratory study, it was important to control for industry effects (McGahan and Porter 1998) in order not to confound the analysis. Second, I selected financial institutions because previous research has established that personal financial information is one of the most sensitive areas of concern for personal information privacy (Dinev and Hart 2003; Sheehan and Hoy 2000). This suggested that the study would approach the privacy topic from a "conservative" perspective. Third, I decided to conduct my research in Canadian firms in order to control for the legal environment and national

culture. Last, I have some experience with and contacts in this sector which increased the likelihood that I would be able to recruit research sites.

Table 7-1 lists the organizations that were included in this phase of the research. These organizations were selected from a sample of the deposit-taking institutions in Canada including domestically chartered banks and credit unions. I obtained a list of the top 20 Canadian domestic banks from the Canadian Bankers Association and the top 20 credit unions from Credit Union Central of Ontario (Appendices E and F provide information about the banks and credit unions from which the sample for the website evaluation study was selected).

Table 7-1: Selected Canadian Financial Institutions (Alphabetical Order) and Their URLs

Banks	URL	Credit Unions	URL
Bank of Montreal Toronto, ON	www.bmo.com	Capital City Savings Credit Union Edmonton, AB	www.capitalcitysavings.ca
Bank of Nova Scotia Toronto, ON	www.scotiabank.com	Coast Capital Savings Credit Union Surrey, BC	www.coastcapitalsavings.com
Canadian Imperial Bank of Commerce Toronto, ON	www.cibc.com	Community Savings Credit Union Red Deer, AB	www.communitysavings.ca
National Bank of Canada Montreal, PQ	www.nbc.ca	Hepcoe Credit Union Toronto, ON	www.hepcoe.com
Royal Bank of Canada Toronto, ON	www.rbc.com	Niagara Credit Union St. Catharines, ON	www.niagaracu.com
Toronto-Dominion Bank Toronto, ON	www.tdcanadatrust.com	Vancouver City Savings and Credit Union Vancouver, BC	www.vancity.com

The selection criteria for inclusion in the Phase One study required that each institution:

1. Have a website, thus excluding organizations from whom I could not easily gather information.
2. Exercise direct privacy oversight, thus excluding banks operating through brokerage networks (i.e., Bank West of High River, Alberta).
3. Have a primary interest in retail banking, thus excluding banks without deposit-taking operations. (i.e., Canadian Tire Bank of Canada, Ontario).
4. Operate both traditional (branch) and electronic (web-based) delivery networks (i.e., are not "virtual banks" such as Manulife Bank, Ontario).

5. Not be owned by a credit union (i.e., CS Alterna Bank owned by CS Coop, Ontario).
6. Have multiple branches (thereby excluding Steinbach Credit Union, Manitoba).
7. Belong to a recognized financial institution trade association such as CBA or CUCC (thereby eliminating CS Coop, Ontario).
8. Is reported separately (thereby eliminating Amicus and Presidents' Choice Banks both of which are operated by CIBC and not reported separately).[1]

Note that I deliberately excluded foreign controlled banks operating in Canada in order to focus on privacy in a Canadian context and avoid jurisdictional confusions.

At the same time, I did not think that focusing solely on chartered banks provided an accurate portrayal of the potential variability in information privacy orientation likely to exist across the financial institutions sector. As a result, I included an equal number of the country's largest credit unions in this phase of my research.[2] Including credit unions helped to expand the likely variance to be found across the policies to be surveyed because while they are competitors, credit unions and banks exist for different reasons and tend to compete in different ways. Appendix G shows some of the main differences between chartered banks and credit unions by regulation, trade association, market coverage, service offerings, size, capitalization, customers, governance and privacy regime.

Data Collection

There were two steps to data collection. The first step in data collection involved capturing and storing the website for each financial institution I was reviewing within the same time period. I attempted to eliminate a time-bias by capturing the websites within a one month time period – most sites were captured during the December 2003 – January 2004 period. I used Blue Squirrel's "Grab-A-Site™" software for this purpose. Grab-A-Site™ has been used in previous web site studies (i.e. Culnan 1999a) because it captures the entire website so that its

[1] In order to provide an equal number of sites and geographic diversity, I removed from the sample the smallest of the three BC- and Alberta- based credit unions.
[2] I have also excluded the Québec-based Caisses Populaires from this survey in order to reduce the complexity of conducting initial research in two languages.

contents can be analyzed offline. This makes it possible to analyze the websites consistently. Two of the 12 sites could not be captured by the software and were dropped from the study[3].

Second, each of the remaining ten sites was reviewed and information about the firm's privacy policies recorded using the Privacy Policy Evaluation Study Form (Appendix J-1)[4]. This instrument was developed by examining the data collection forms used in previous evaluation studies and adapting them for this project. I sought feedback on this instrument from three Queen's School of Business faculty and graduate students as well as two personnel from a financial institution not included in the study. I also pilot tested the instrument using the privacy policies posted to the websites for two financial institutions (Canadian Western Bank and St. Willibrord Credit Union) not included in the sample.

Data Analysis

Once the 10 sites had been captured and their information privacy policies documented, I evaluated the data in three ways – an overall assessment (comprehensiveness, readability and accessibility); an assessment using the IPO Definition (what is the evidence for principles, values, policies, objectives, and decision rules); and an assessment against the IPO Continuum (what evidence is there for any of the categories within the four layers).

First, the privacy policy for each organization was reviewed against two criteria. The first was *comprehensiveness* which addresses how well and in-depth the policy is explained. This assessment was made by reading through and documenting the extent to which the policies addressed the PIPEDA principles and/or fair information elements, if a summary was provided, and if responsibility for the policy was identified. The second element was *readability* meaning how easy is it to understand the policy and its implications. This assessment computed readability

[3] I contacted Grab-A-Site's help-desk to ask for an explanation of why I could not "grab" certain sites. Their response was that the technology "wasn't perfect" and sometimes simply did not work. Their experience was that certain websites had "blockers' that prevented capture.

[4] In the interests of preserving the anonymity of the research sites that were eventually selected, I have chosen not to indicate the financial institutions that were dropped in this last culling exercise. This means that the 10 sites that were eventually reviewed for the Phase One study are not specifically identified.

scores and examined policies for examples and consent forms. Readability scores have been used in different privacy research (Cadogan 2001) because the ability of consumers to comprehend privacy notices can lead to increased confidence in dealing with the firm posting the notice (Milne and Culnan 2002). I used the Word Count feature (in the Spelling & Grammar menu for MS Word) to analyze the reading ease scores for the privacy policies (all sites) and important additional information if provided, such as separate FAQs (Firms 4 and 9). The readability analysis indicates the level of reading capability that customers would need in order to comprehend the privacy policies. The Flesch Reading Ease Score is based on a scale of 100. The higher the score the easier it is to understand a text.[5] The Flesch-Kincaid Grade Level analysis evaluates documents according to the reading ability to be expected by those with various grade school attainment.[6] Last, I assessed the *accessibility* by examining how users could find the policy and if there were links to external sources of privacy information. Table 7-2 summarizes these assessment criteria.

In the second step of the study, I applied the IPO Definition to each of the ten organizations using the IPO Definition Analysis Form. In order to accomplish this evaluation, I operationalized each aspect of the definition. Table 7-3 explains the operationalization of the different elements of the IPO definition and provides examples relevant to this research.

---

[5] The information about the Flesch Reading Ease Score is taken from the Microsoft Office Word help file : "Rates text on a 100-point scale; the higher the score, the easier it is to understand the document. For most standard documents, aim for a score of approximately 60 to 70."

[6] The information about the Flesch-Kincaid Grade Level Score is taken from the Microsoft Office Word help file : "Rates text on a U.S. school grade level. For example, a score of 8.0 means that an eighth grader can understand the document. For most documents, aim for a score of approximately 7.0 to 8.0."

Table 7-2: Initial Assessment Criteria

Criterion	Key Questions/Concerns
Policy Comprehensiveness	• Are all PIPEDA/fair information elements addressed? • Is there a summary of the policy that emphasizes key features? • Is responsibility clearly identified?
Policy Readability	• What is the readability score for the privacy policy document(s)? • Is the policy written in accessible language (or in "legalese")? • Are key terms explained? • Are examples provided? Are the examples thorough and understandable? • Are consent forms provided?
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points? • Are there links to other privacy information (external)? • Is there a webseal or other "seal of approval"?

There are four aspects of this exercise that require explanation. First, I distinguished between external and internal principles. I considered this necessary in order to capture whether the organizations justified their privacy actions based on external principles (such as those laid out in PIPEDA) and/or on internally derived principles. Second, I categorized the objectives according to a modified version of Earp et al's (2002) typology. In addition to their five perspectives - legal, technical, business, social and contractual – I have added an ethical category. Third, I assumed that it would be unlikely that I would be able to identify "decision rules" when limited to reviewing only the firms' privacy policies. The decisions rules of interest to me involve organizational choices (for example, information management policies resulting from the use of CRM technology) that affect or are affected by privacy considerations. Last, I assessed whether there was a preponderance of evidence to make the case that IPO could be identified.

In the third step, I reassessed each privacy policy against the IPO continuum. I sought evidence to support the different categories within the continuum's four layers - customer relationship stance, customer information management strategy, customer information privacy philosophy and customer information privacy behavior. Then I mapped all evidence (i.e., multiple categories within the layers) of these initial categorizations onto the IPO continuum to generate initial placements for each of the 10 firms.

Table 7-3 IPO Definition Components

IPO Component	Definition	Example
Principle	a primary assumption forming the basis of a chain of reasoning	Openness (an organization shall make readily available to individual specific information about its policies and practices relating to the management of personal information *(PIPEDA Principle 9)*
Value	the generally accepted or personally held judgment of what is valuable and important in life	Integrity (behavior that is honest, fair and trustworthy) or Innovation (behaviors to anticipate customer needs)
Policy	any course of action adopted as advantageous or expedient	The privacy policy that defines the objectives, strategy, structure, and system that an organization implements
Objective	[a goal] sought or aimed at. There are six objectives: 1. Legal - opportunities, requirements or constraints imposed by privacy law 2. Technical – security measures undertaken to protect privacy 3. Contractual – binding agreements between an organization and its suppliers 4. Business - enterprise objectives supported by privacy 5. Social – the interaction between organizations and customers based on or caused by the organization's information and privacy actions 6. Ethical – - opportunities, requirements or constraints imposed by standards of ethical conduct *(1-5 from Earp et al 2002)*	1. Legal - we will comply with the law; the law prevents us from selling your information. 2. Technical – we use 128 bit encryption to protect your information. 3. Contractual – we require our suppliers to have the same privacy standards as we do 4. Business - we respect the trust you place in us when you give us your personal information 5. Social - sharing your information helps us to determine your financial needs so we can offer you other products and services that may meet your needs 6. Ethical – we believe that protecting your privacy is an ethical obligation.
Rule	Any of various codes of practices or sets of regulations	Grandfathering – only new customers will be specifically advised of the privacy policy consent provisions by Customer Service personnel. Existing customers will be sent a pamphlet.

- All definitions are drawn from *The New Shorter Oxford English Dictionary* (1993).

My aim throughout this Phase One study was to find the greatest variance in information privacy behaviors. This strategy is similar to a "maximum variety sampling" strategy in which the researcher seeks a deliberately heterogenous sample in order to observe similarities and differences across the sample (Morse 1994:229.)

Detailed Findings

The detailed findings for each organization included in the study are provided in Appendix J.

Overview

Comprehensiveness – This refers to how well and in-depth the privacy policy is explained. Table 7-4 summarizes the comprehensiveness of policies across the sample. The comprehensiveness of the policies varied considerably across the sample. Most firms did not refer to the federal statute or provide other information to underpin or legitimize their privacy policies. This lack of information could leave readers with two misimpressions. First, the policy could leave the erroneous impression that the firms had implemented privacy policies strictly for altruistic purposes ("treat you with fairness and respect") (Firm 3) or, second, that the policy was merely an extension of traditional "bankers' confidentiality." ([since our founding], we have been committed to keep all information about you and your banking relationships with us confidential") (Firm 10).

All websites contained some privacy information ranging from a cursory treatment of privacy as part of a legal disclaimer (Firm 7) to a lengthy, multipart statement following the PIPEDA principles (Firm 9) to an extensive web-based approach and attachments (Firm 5) that explicitly and in great depth addressed fair information and PIPEDA.

Readability – This refers to how easy is it understand the privacy policy and its implications. None of the privacy statements in this sample of ten firms was "easy to read" using the assessments provided by the Flesch-Reading Ease and Flesch-Kincaid Grade Level Scales. Table 7-5 summarizes the readability data for the privacy policies.

All 10 firms have privacy information that would be considered quite difficult for many customers to read as all score well below the 60-70 range (target for Flesch-Reading Ease). As

Table 7-4: Summary of Privacy Policy Comprehensiveness

Firm	Company Privacy Information	PIPEDA/Fair Information Practices	Summary of key points provided	Responsibility Identified	Consent Form provided	Total Pages
1	• Privacy Policy	• No specific reference • PIPEDA principles covered minimally	• Yes	• No mention of a designated Privacy Officer; refers only to Ombudsman for complaints	• No	7
2	• Our Commitment – introduction to policy • Ten Principles • What Information we collect • How your information is used • Security of your personal information • Accessing and Amending information • Opting Out • Your online privacy • FAQ privacy link	• PIPEDA not specified • Reference to CSA model code • PIPEDA principles covered thoroughly	• Yes • Also FAQ	• Generic reference within Accountability Principle • Email link to Privacy Officer	• No	8
3	• Confidentiality Policy • ABC's of Security	• PIPEDA not specified • PIPEDA principles covered minimally	• No	• No mention of a designated Privacy Officer; refers only to Branch Manager for complaints	• No	4
4	• General Information about Privacy and Security • Privacy Code • Privacy Statement • Privacy FAQs • Security	• PIPAEDA (sic) specified • CSA Model Code referenced • PIPEDA principles covered thoroughly	• Yes • Also FAQ	• Several references to Privacy Officer but not identified by name; contact information provided • Privacy Representative at each branch for questions, concerns	• YES – opt out form	21

5	• Our Commitment • What Information is collected • How your information is used • Safeguarding information • Cookies • Questions, concerns & complaints	• PIPEDA specified • CSA Model Code referenced • PIPEDA principles covered thoroughly	• Yes	• Generic reference within Accountability Principle • Contact information provided for Customer Relations Centre	• No • 1-800 number provided	27
6	• Commitment to Privacy • (contains 12 links to paragraphs within the document)	• PIPEDA not specified • PIPEDA principles covered minimally	• Yes	• No mention of a designated Privacy Officer • Contact information provided for Customer Relations Centre, Ombudsman	• No • 1-800 number provided	11
7	• Website terms of use, Privacy and Copyright information	• PIPEDA not specified • PIPEDA principles not covered	• No	• No mention of a designated Privacy Officer	• No	7
8	• Privacy Code	• PIPEDA specified • (provincial) credit union privacy code • Consistent with CSA standards	• Yes	• Generic reference within Accountability Principle • Several references to Privacy Officer but not identified by name; available through email link	• No	15
9	• Privacy Policy • FAQs • Privacy Pledge	• PIPEDA not specified • PIPEDA principles covered thoroughly	• Yes • Also FAQ	• Generic reference within Accountability Principle • Several references to Privacy Officer but not identified by name; available through email link	• No • Contact Centre number provided	18
10	• Privacy Policy • What is Personal Information • Security Information	• PIPEDA not specified • PIPEDA principles covered thoroughly	• Yes	• Several references to Privacy Officer but not identified by name; contact info provided	• No	13

Table 7-5: Summary of Privacy Policy Readability

Firm	Flesch Reading Ease				Flesch-Kincaid Grade Level	Key terms explained	Examples provided
	Score	Hard*	Harder**	Hardest ***			
1	46.0	✓			12	• No	• Very few
2	38.3 (policy) 54.0 (FAQ)	 ✓	✓		12 9.4	• No	• Very few
3	40.2	✓			12	• No	• Very few
4	19.2 (policy) 35.6 (FAQ)		 ✓	✓	12	• Legal definitions	• Many
5	15.8			✓	12	• Technical terms	• Many
6	43.6	✓			12	• No	• Many
7	28			✓	12	• No	• Very few
8	37.8		✓		12	• Legal definitions	• Some
9	16.4 (policy) 34.9 (FAQ)		 ✓	✓	12	• Legal definitions	• Many
10	34.3		✓		12	• Technical terms	• Some

Note: Unless otherwise indicated, the Flesch Reading Ease Score is for privacy policy information.

* Indicates scores > 40

** Indicates Scores >30

*** Indicates Scores < 30

well, all are rated at a Grade 12 level (Flesch-Kincaid Grade Level). Because of the apparent clustering of scores, I analyzed the scores on the basis of level of difficulty with scores greater than 40 considered hard, scores between 30 and 39 rated as harder and scores less than 30 rated as hardest. Three Firms had "hard" to read privacy information, three had policies rated "harder" to read, and four were placed in the "hardest" category.

These findings are interesting because they could suggest that firms are deliberately making their policies inaccessible for their customers, or are relying on the presence of a privacy link to act as a symbol of good intention (Milne and Culnan 2002). Furthermore, some research has demonstrated that consumers prefer shorter and less legalistic privacy notices (Turow 2003). An alternative interpretation, suggested by (Milne and Culnan (undated):19) is that privacy notices that are provided in order to fulfill a compliance function may be written "to be exhaustive and not necessarily to be accessible to consumers and informative." This appears a reasonable working assumption, especially when considering that the financial institutions sector is a heavily regulated industry, and that there has not been a great deal of information available to firms about how to both comply and effectively communicate.

Another important observation about the communications aspects of the privacy policies concerns terminology. There is a plethora of different terms used by the firms to characterize their information. Terms include privacy "statements", "pledges", "commitments", "principles", and "policies." In addition, firms used privacy and confidentiality interchangeably. (This point is taken up in later discussions of the field research findings). The lack of terminological consistency may contribute to confusion if consumers attempt to compare privacy activities among firms. The lack of "well-defined standards for the content of privacy notices" (Milne and Culnan 2002) may represent a greater barrier to consumer understanding than the actual wording itself.

Accessibility– This refers to how easily customers can locate the policy and if there are links to external sources of information about privacy. Table 7-6 summarizes the accessibility of privacy policies across the sample.

Almost uniformly, the privacy policy was generally easy to locate and could be accessed from homepages as well as other parts of the websites. Some sites linked their privacy and security statements but that was not a uniform practice. In one case, the firm's privacy link was called the "confidentiality link." (Firm 3) Interestingly, none of the sites offered a privacy web seal. Previous research suggests that privacy web seals can serve as a symbol to proceed without having to review the details of privacy policies (Milne and Culnan 2002). It is curious that two things that could communicate a reassuring message to customers – an explanation of legal rights ("the government backs our policy") or the display of a webseal ("this means we're okay to bank with online") are lacking in almost all cases. This is something to be explored in the case studies.

Summary – I assessed the privacy policies on the bases of their comprehensiveness, readability and accessibility. Table 7-7 summarizes the scores and subsequent rank I assigned to the ten firms. This first exercise demonstrates that there is variation to be found among these firms.

Applying the IPO Definition

I was able to apply the IPO definition to all the firms in this Phase One study. Table 7-8 contains a summary of these findings.

Principles: It was not too difficult to discern the existence of external or internal principles guiding privacy approaches. Six firms did not communicate an external set of principles while only half presented an internal set of principles. Those firms with external principles relied primarily on the CSA Model Code (four firms) and/or PIPEDA (three firms). Of the five firms stating internal principles, four based them on PIPEDA or PIPA (with limited

Table 7-6: Summary of Privacy Policy Accessibility

Firm	Ease of locating policy	Links to external information	Privacy Seal
1	• Home page and subsequent pages • Next to security and legal links	• No	• No
2	• Home page and subsequent pages • Next to locations and contact links	• Canadian Standards Association • Privacy Commissioner of Ontario • Privacy Commissioner of Canada	• No
3	• Home page and subsequent pages • Next to legal and security links	• External organizations (Banking Ombudsman, OSFI) identified but not linked, contact info provided	• No
4	• Two links from home page • Links from subsequent pages	• External organization (unspecified Privacy Commissioner) identified but not linked	• No
5	• Two links from home page • Links from subsequent pages	• Privacy Commissioner of Canada • Electronic Commerce Branch of Industry Canada	• No
6	• Two links from home page • Links from subsequent pages	• External organization (Privacy Commissioner of Canada) identified but not linked, contact info provided • Ombudsman for Banking Services and Investments	• No
7	• Home page and subsequent pages	• No	• No
8	• Home page and subsequent pages	• External organization (provincial Privacy Commissioner) identified but not linked	• No
9	• Home page and subsequent pages	• Canadian Marketing Association • Other external organizations (Credit Union Central of Canada, to a regulator, or to an independent mediator or arbitrator), no contact info provided	• No
10	• Home page and subsequent pages	• External organization (Privacy Commissioner of Canada) identified but not linked, contact info provided • Ombudsman for Banking Services and Investments	• No

Table 7-7 Summary of Comprehensiveness, Readability and Accessibility Scores

Firm	Comprehensiveness	Readability	Accessibility	Total	Rank
1	2.5	2	1	5.5	8
2	4.5	1.5	2.5	8.5	5
3	1.5	2	2.5	6.0	7
4	7	3	2	12	1
5	5.5	3	2.5	11	2
6	3	3	2.5	8.5	5
7	0	2	0	2	9
8	5.5	3	1.5	10	3
9	4.5	3	1.5	9	4
10	3	3	2	8	6

Table 7-8: Phase One Study - Summary Chart for IPO Definition

Evidence	Principles: External	Principles: Internal	Values	Policies	Objectives[7]						Decision Rules
Firm					L	T	C	B	S	E	
1	No	No	• Service Excellence • Confidentiality	Yes		✓		✓			No
2	• CUCC Model Privacy Code • CSA Model Code	• Ten principles • Based on external principles	• Inherent rights to privacy • Appropriate conduct	Yes	*	✓	✓	✓			No
3	No	No	• Rights	Yes	✓	✓	✓				No
4	• CSA Model Code • PIPEDA	• Ten principles • Based on external principles	• Legal compliance • Ethical obligations	Yes	✓	✓	✓	✓	✓	✓	No
5	• CSA Model Code • PIPEDA	• Ten principles • Based on external principles • Meeting or exceeding standards	• Fundamental business practice • Safeguarding Confidentiality • Protecting personal and financial information	Yes	✓	✓	✓	✓	✓	✓	No

[7] Legend for Objectives: L = Legal, T = Technical, C=Contractual, B=Business, S=Social, E=Ethical
*Note that the * in an "Objectives" column indicates that while a goal may not have been stated, it is implied by, for example, adherence to specified privacy principles.*

6	No	• Five principles	• Fundamental business practice • Best customer service • Fair and respectful treatment	Yes		✓	✓		✓		No
7	No	No	• Customer information privacy as an obligation	None discernible	✓	✓					No
8	• CSA standards • Alberta Credit Unions Model Code • PIPEDA • PIPA	No	• Respecting rights • Maintaining confidentiality	Yes	✓	✓	✓				No
9	No	• Ten principles	• Respect for privacy • Inherent responsibility to be open and accessible • Consistency with mission and beliefs	Yes	✓	✓	✓			✓	No
10	No	No	• Confidential and secure banking services and privacy are critical	Yes		✓	✓	✓	✓		No

wording changes) while one firm had a five principle approach.

Values: I had a more difficult time to identify values. While I was able to identify some privacy related "values" type statement for each of the ten firms, I believe that it might have been more appropriate to also check for firm's enterprise-wide statements of values. Given that I restricted my examinations to the privacy sections of the websites, I cannot comment on the relationship between larger corporate values and privacy (e.g., is privacy considered a fundamental corporate value?). Seven firms offered some version of "respect for privacy rights" as a value. In addition, three addressed privacy and/or confidentiality as some form of "critical" or "a fundamental business practice. "Customer service" was identified as a value for three firms. Two firms identified privacy as a matter of "appropriate conduct" or as part of its "inherent responsibility to be open and accessible." One firm identified privacy as an ethical obligation. I expect that conducting a more thorough search of the individual websites might render better information about values. However, the purpose of this study was to attempt to gather evidence to support my contention of the existence of IPO as I define it. I believe that there is sufficient data to support my contention that firms have values that inform their approaches to privacy.

Policies: With one exception (Firm 7), all firms had discernible privacy policies. Different firms provided greater or lesser detailed information about procedures, structures, systems, etc. However, there was enough information to generally declare that there firms exhibited patterns of intention or a "chosen course of [privacy] action" that could be discerned. Some of the specifics of these policies are discussed in the section reviewing the application of the IPO Continuum.

Objectives: There were objectives discernible for all ten firms' privacy policies. All the firms had at least a modest technical objective while eight had discernible contractual and seven had some form of legal objective. It was not surprising that the technical objective was evident given the explicit PIPEDA and PIPA requirements for "safeguards." Less expected was the finding that not all firms had a discernible contractual objective given the liability that privacy

regulation places on the firms when dealing with third party use of customer information. Perhaps more understandable is the fact that three firms lacked a specific "legal" objective. There seems to be two potential explanations for this. First, the firms may not feel the necessity to state what for them might be obvious, to wit, that there is a privacy law. Second, these firms may want to communicate a message that suggests that they are privacy sensitive without the necessity to be required to be by the government. It will be interesting to examine these kinds of issues in the field research.

Decision Rules: The one part of the IPO definition that I could not readily discern for any firm in this study was the firms' "decision rules." This circumstance was not unexpected, as I indicated previously. The decision rules portion of the definition refers to internal rules that are unlikely to be publicly posted or would not necessarily appear in the privacy policy itself. This situation underscores the limitations of website privacy policy studies (Milne and Culnan 2002).

Summary – I sought evidence of the different elements of the IPO definition through a careful reading and coding of the ten firms' privacy policies. Table 7-9 summarizes the scores and ranks I assigned to these firms. This exercise confirmed that there are discernible differences among the firms.

Applying the IPO Continuum

The next part of the Phase One Study involved reviewing the privacy information for evidence of the firms' customer relationship stance, customer information management strategy, customer information privacy philosophy and customer information privacy behaviors. I read through all the firms' policies and extracted examples to support the different categories within the IPO continuum. Based on this evidence, I mapped the firms within the categories of the layers of IPO continuum chart. Figure 7-1 illustrates these results.

Table 7-9: Phase One Study - Summary of IPO Definition Scores

Firm	Princ.-Ext.	Princ. – Int.	Values	Policies	Objectives	Dec. Rules	**Total**	**Rank**
1	0	0	1	1	1	0	3	7
2	1	1	1	1	1.5	0	5.5	3
3	0	0	.5	1	1.5	0	3	7
4	1.5	1	1	1	3	0	7.5	2
5	1.5	1.5	1.5	1	3	0	8.5	1
6	0	.5	1.5	1	1.5	0	4.5	5
7	0	0	.5	0	1	0	1.5	8
8	2	0	1	1	1.5	0	5.5	3
9	0	.5	1.5	1	2	0	5	4
10	0	0	.5	1	2	0	3.5	6

Note that this figure suggests that firms occupy multiple positions on the IPO Continuum. For example, Firm 6 appears in both the "buyer self-position" and "shared responsibility" positions on the customer relationship stance layer. This is because I simply recorded evidence to support classification, even if there were multiple entries. I did not, and indeed could not, evaluate which of these positions was more justified.

Customer Relationship Stance – All ten firms demonstrated some evidence of viewing privacy as a matter of mutual responsibility (firms gathered information to provide a service – customers shared their information to obtain the service; firms provided security to safeguard information – customers should take reasonable steps to safeguard themselves). Two firms also suggested that customers had to take special steps to protect themselves (Firms 6, 7). There was evidence that two firms felt some obligation to enhance their customers well-being through their privacy approaches (Firms 4,5).

Customer Information Management Strategy – Finding evidence from the websites to populate this layer of the IPO continuum was difficult. This is not too surprising given that I was not expecting find that many firms explicitly and publicly linked their privacy activities with their information management strategies. However, I was able to discern that all firms appear to approach privacy as part of a risk management effort. This was not unexpected given that

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
	⑦	①②③④⑤⑥⑧⑨⑩	②③④⑤⑧	⑤
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
	⑦	①②③④⑤⑥⑦⑧⑨⑩	①②③④⑤⑥⑧	⑤
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		①②③④⑤⑥⑦⑧⑨⑩	①④⑤⑥⑧⑨⑩	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
		⑥⑦	①②③④⑤⑥⑦⑧⑨⑩	④⑤
	Weaker ⟷			***Stronger***

Key:

Banks	Credit Unions
①③⑤⑥⑩	②④⑦⑧⑨

Figure 7-1: Phase One Study - Summary Placement of Ten Financial Institutions on IPO Continuum

financial institutions have well developed risk management regimes. Seven firms appeared to use customer information to attempt to add value to their products and services. However, the

threshold to be included was low ("bring other products and services to your attention"). Four firms appeared to truly use the information they collected to change, tailor and otherwise customize their products and services ("research, develop and present products and services that may interest you"). There was no evidence of any firm using customer information to "create new realities."

Customer Information Privacy Philosophy – Inherently conservative and compliant industries like financial institutions are unlikely to declare on a publicly accessible website that they dislike certain regulations. However, they do leave evidence of their approach to customer information privacy as a result of legislated requirements, or at least most do. One firm did not appear to have a very great awareness of privacy (Firm 7). At the other end of the continuum, was one firm that appeared to be differentiating itself. Firm 5 appeared to have used the development of privacy legislation to its advantage by actively participating in the development of codes and regulations. All firms expressed a "constrained view" of privacy in two ways. First, they expressed that they did not sell customer's personal information. There is nothing in the law to prevent this but firms are required to disclose if they intend to do so. Therefore, firms are choosing to be constrained. Second, the law constrains customers' choices. These firms indicated that while customers were able to refuse to provide certain information or not to consent to the sharing of information, the firms were likewise free to deny them certain products and services. The most frequently used example was credit granting, understandable for banks and credit unions. Similarly, seven of the firms showed some evidence of treating privacy as an exchange in which customers gave their personal information to receive benefits. Again, I used a low threshold for this category (e.g. "assess your suitability and eligibility for products and services"). Overall, I think that there is evidence for this category but I believe that a review of other corporate information may provide greater insight.

Customer Information Privacy Behavior – There were two "extreme" positions from this sample of Canadian financial institutions. One firm's lack of information suggested that it was

not compliant with privacy law (Firm 7). At the other end of the continuum, was a firm that engaged in privacy behaviors that exceeded what was evident in other firms (Firm 5). Most firms provided information to support a minimally compliant position while five also subscribed to professional or trade association codes. I must acknowledge that the minimally compliant position represents a high standard of privacy conduct given the principles laid out in Canadian privacy legislation. However, it must also be acknowledged that the legislation represents a floor and that firms are able to choose their privacy behaviors. The most important consideration is to communicate firm activity. The fact that there is a cluster of firms "in the middle" is less a surprise than are the two outliers.

In summary, I was able to find evidence to support the existence of all four layers of the IPO continuum and most of the categories therein. Table 7-10 summarizes the scores and ranks for this third exercise.

Table 7-10: Phase One Study - Summary of IPO Continuum Scores

Firm	Non-Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy	**Total**	**Rank**
1	0	3	4.5	0	7.5	5
2	0	3	4.5	0	7.5	5
3	0	3	4.5	0	7.5	5
4	0	3	6	2	11	2
5	0	3	6	6	15	1
6	0	4	4.5	0	8.5	4
7	1	1.5	1.5	0	4	7
8	0	3	6	0	9	3
9	0	3	3	0	6	6
10	0	3	3	0	6	6

Initial Selection of Research Sites

The selection of the potential research sites was done on the basis of the accumulated evidence of the strength of Information Privacy Orientation. Table 7-11 summarizes the strength of rankings across the three exercises completed for this evaluation.

Table 7-11: Final Ranking of Potential Research Sites

Firm	Evaluation 1 Rank	IPO Definition Rank	IPO Continuum Rank	Total	Final Ranking
1	8	7	5	20	8
2	5	3	5	13	4
3	7	7	5	19	7
4	1	2	2	5	2
5	2	1	1	4	1
6	5	5	4	14	5
7	9	8	7	24	9
8	3	3	3	9	3
9	4	4	6	14	5
10	6	6	6	18	6

Overall, I placed the ten firms in relative position to each other on a single continuum representing weaker (score >20), middle strength (20< score >10) and stronger IPO (score <10). The results of this exercise are summarized in Figure 7-2. The circled numbers at the top indicate the firm. The numbers below the double-headed line represent the scores in which a lower score indicates a stronger IPO.

Based on conclusions above, I prepared a "wish list" for my research. I wanted to have representatives of stronger IPO and weaker IPO from both banks and credit unions for a total of four case studies. My research site preferences were organized as indicated in Table 7-12. The recruitment of the research sites is addressed later in this chapter.

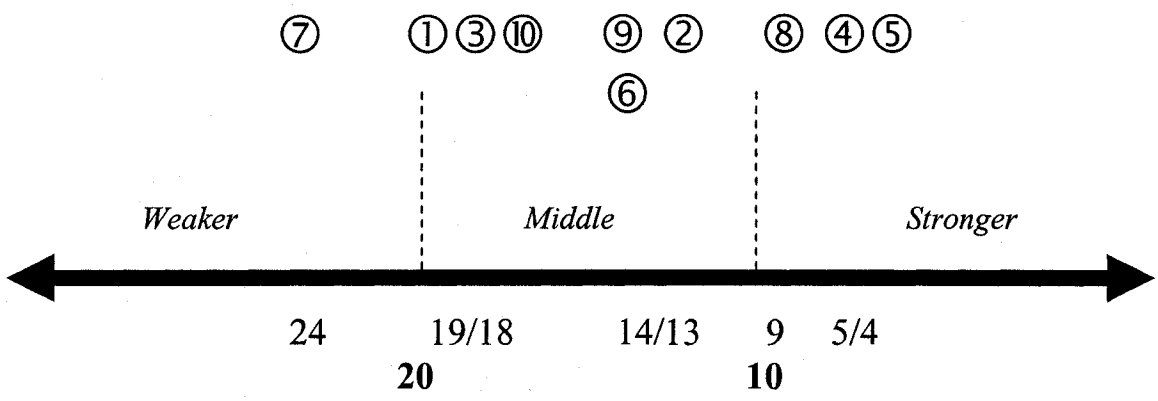


Figure 7-2: Phase One Study: Summary of Firms' Relative Positioning on IPO Continuum

Table 7-12: Research Site Preferences

	Firm number	Categorization
1	⑤	Bank – Stronger IPO
2	①	Bank –Weaker IPO
3	④	Credit Union – Stronger IPO
4	⑦	Credit Union – Weaker IPO

Limitations

Of course, I must express the limitations inherent to this three pronged evaluation exercise. First, this sample is highly selective. I might have obtained different results from a differently constructed sample. However, I believe that this sample serves the limited purposes for which this study was designed. Second, academic researchers are not the target audience for privacy policies posted on firms' websites. Therefore, my ability to meet my research requirements solely through an examination of posted policies appears to place an unfair burden upon those organizations. As well, in the absence of dialogue with these financial institutions, I can only surmise their intentions. As a result, I may be incorrect in my interpretation and more sensitive to language and presentation than a typical customer. However, given that these organizations all profess, to greater or lesser extents, to care about their customers' privacy concerns, a focused examination is legitimate to the extent that it can reveal what the

organizations' consider to be important to disclose about their treatment of customer information privacy (Milne and Culnan 2002). As well, the very strictness of the test lends support to my claim that organizations have discernible and various information privacy orientations. Fourth, the numerical treatment of the data (assigning scores and ranks) is not definitive and, admittedly, flies in the face of an interpretive study. However, it does provide a sense of where these firms lie in relation to each other based on the preponderance of evidence. To the extent that this helps to differentiate among the firms for the purpose of selecting research sites, then the practice is defensible.

Chapter Summary

In this chapter, I reviewed the research methods and findings for the Privacy Policy Evaluation Study that I conducted as Phase One of the research program. I explained the purpose, sample, data collection and analytical strategies used in the review of privacy policies in ten selected Canadian financial institutions. I described how I assessed the comprehensiveness, readability and accessibility of each firm's privacy policy. Then I discussed the findings of the application of the IPO definition to the posted policies and evaluated the relative position of the different Financial Institutions on the IPO Continuum. I computed a score and ranked the firms in each of these steps. As a last step I provided an overall ranking for each firm and plotted this onto a continuum. From this plot, I identified the four organizations that I believe would provide the greatest variance in IPO and hence the greatest scope for investigation. In the next chapter, I describe Phase Two, the development and validation of the interview guides and survey instrument I used in my field research.

CHAPTER EIGHT

PILOT STUDY (CASE A)

In this chapter, I describe the process and results of the pilot study. Briefly, I conducted a three day research site visit at Case A's head office in June 2004. I interviewed 20 executives, managers and staff about how the company had gone about organizing and implementing their customer information privacy program. I collected one privacy specific document (Privacy Notice). I received 16 completed "paper and pencil" IPO Surveys from this case site.

This chapter is in three sections. First, I provide an introduction to the research site by discussing their "stage" of privacy program development. Second I describe the success of the pilot against the study's five goals. In the chapter's final section, I apply the IPO Definition and the IPO Continuum to the pilot research site's privacy circumstances. Note that Appendix K contains a collection of information from Case A's case study database, including interview and document lists, and IPO survey statistics.

Privacy Program Status: "Managing the Immediate Exposure"

The requirement for Case A to meet the requirements of any privacy legislation had come as an unpleasant surprise. A manager with the firm noted that the company was engaged in "playing catch up" with their privacy compliance. They were in the "design phase" of their "Privacy project." The company's situation was described by one senior manager as,

> I think if it weren't for the legislation we wouldn't have it [a privacy program]. We have some focus on it today, it's not a great amount of focus, we'd probably have even less focus on it [without the legislated requirement].

When asked why the bank hadn't taken a proactive stance (given that their competitors were already PIPEDA compliant) another senior manager cited uncertainty as the reason for non-action:

> The cost of not doing so [not implementing a privacy program] hasn't been quantified. The only thing, it [any new initiative] requires a financial business plan, so if you can't quantify your exposure, we're going to work on those initiatives that do [have a financial

> business plan]. Or that can be identified, exactly what the benefit is, or cost of not doing it. So when you don't know exactly what the legislation is going to be, and you don't know what the cost of it's going to be, and when you have better things to work on, that's what you're going to work on.

First Responses

The company's first response to the imposition of privacy legislation was to engage an outside consultant to complete a privacy audit to review the areas of vulnerability. The manager assigned the responsibility for developing and implementing the company's privacy compliance regime described their approach as one of "managing immediate exposure" while at the same time "minimizing customer expectations."

To manage immediate exposure, the company *inter alia* developed a Privacy Notice; appointed a Chief Privacy Officer and managers to deal with customer and employee inquiries and complaints; undertook basic awareness sessions with branches (when requested); and developed a consent policy and procedure. The branch staff level awareness focused mostly on aspects of physical security (e.g., not leaving customer files lying out in open, shredding sensitive material), the basic mechanisms of customer consent, and the inquiries/complaints response process. In order to avoid raising customer expectations about privacy that could not be met immediately, the company did not undertake a comprehensive customer awareness campaign or provide any additional privacy or security information (beyond the basic privacy notice) on their website. However, as expressed by one senior manager, more work is required:

> I'm not sure if we have a full understanding throughout organization what PIPA is, and what it requires. So, I mean, you can read the legislation, but I think it's beyond that, it's understanding the intent and the spirit of it itself. So even if something's not specifically covered in there, the intent is that we won't do that. So I don't know that we've had enough communication or training or understanding around that. And if I haven't had it, I'm pretty darn sure people up the line haven't had it.

Present Activity

At present, the firm is engaged with "short term" concerns. These include:

1. Preparing the Business Case to secure financial and organizational resources for developing and implementing the larger privacy regime.
2. Building awareness across the company of the need for privacy to be built into work processes and undertaking targeted training.
3. Identifying privacy issues in different functional areas, assessing impacts and assigning priorities for action.
4. Identifying all locations of customer information and ensuring appropriate privacy measures are in place.
5. Reviewing contracts for "representations and warranties" of sufficient privacy protections.
6. Ensuring that current IT projects are privacy compliant. For example, ensuring screen-by-screen reviews of the new banking system.

Later on, the bank will have to address "longer term" issues, including:

1. Ensuring that all new contracts include adequate and appropriate privacy language.
2. Verifying that the "representations and warranties" in current contracts are, in fact, being upheld by the signatories.
3. Reviewing the bank's many forms, identifying the ones needing updated privacy language and developing replacements.
4. Developing and implementing document retention and destruction policies.
5. Building privacy into systems implementation activities.
6. Deciding the extent to which the bank chooses to engage in other privacy initiatives.

Looking Ahead

For the immediate and foreseeable future, the firm's primary privacy goal could be characterized as "to become compliant as quickly as possible and as economically as possible, with smallest amount of disruption to the status quo" given that "banking is a bottom line business." Others expressed the short term goals in tactical terms of being seen to be compliant, avoiding disputes with the provincial Privacy Commission, and keeping privacy "a non-issue" with customers. However, over the longer term some suggested "strategic" privacy issues for the firm will be dominated by the need to manage a "cultural shift" in how customer information is dealt with, particularly as an information management challenge. The strategic challenges to be managed are exemplified by the following questions that became apparent across several interviews:

1. To what extent does a firm's privacy regime support the "trusting" relationship that financial institutions claim is a necessity to success? How can this concern to maintain "trust" be squared with the "bottom line?"

2. How should firms manage customer information as an "absolutely critical" organizational resource without which "we couldn't do anything" while, at the same time, using the information to customer advantage, all within the limitations imposed by legislation?

3. How should financial institutions balance relatively intrusive risk management regimes with respect for customer information privacy? Intrusions were justified as the need "in large part ... to help identify when fraud is happening on your [credit] card." The ability to run predictive behavioural models necessitates gathering large amounts of information. For example:

> So we gather that information about you, we gather information on all of your assets and liabilities, what your payments are on those assets and liabilities, we gather trend data on how much you use your line of credit, the types of transactions you have, the number of debits and credits you have on your account. Whether or not you've ever had an NSF cheque, the amount of the cheque, whether or not we've put holds on your account. We gather information through the credit bureaus on all of your dealings with other financial institutions, and we do quarterly updates on that so that we can tell whether, even if you applied for a loan 3 years ago, how current you are with everybody else. And on your cards, your credit cards, we take a look at your, and use information about the way you transact, and where you normally shop, the types of places where you buy.
>
> Do you also look at amounts?
>
> Yes.

When combined with the marketing group's desire to move beyond "guessing" and "inferring" life stage to being able to deliver specific products and services targeted for individual customers, the problem becomes apparent. The dilemma was characterized as

> we have part of the organization going, "we've got to manage those [risks]", and "God, I wish we didn't have customers" [the source of the risks], and the other side of the organization's going, "come on, bring in everybody, I don't care!" [Laughter]

In summary, the Pilot Study was conducted at a site in the very early stages of developing and implementing its privacy program. The bank was focussing its efforts on managing short term tactical issues to minimize its exposure while beginning to show concern for longer term strategic issues. These issues involve such larger themes as the role of privacy programs in maintaining customer trust in financial institutions, generally, and theirs, in particular. Having provided information about the research site and setting for the Pilot Study, I will now address

what was achieved during this study by examining my progress against the five goals for the pilot study.

Pilot Study

I had five specific goals for this pilot study. First, I wanted to test the efficacy of the different versions of the Information Privacy Orientation questionnaire with employees working in a financial institutions setting and who had a modicum of "subject matter expertise" about the privacy regime within their company. Second, I wanted to validate the Information Privacy Orientation survey instrument. Third, I wanted to assemble a list of the types of documents that I could expect to find consistently in financial institutions, regardless of type, location or size. Fourth, I was interested to spend time in a retail banking environment to assess where my own learning needed to proceed. Fifth, I wanted to define Case A's IPO and assess their position on the IPO continuum by "triangulating" whatever data I was able to gather. I will discuss how successful I was in achieving each of these goals and the lessons I learned in turn.

Goal One: Testing Interview Questionnaires' Efficacy

I achieved my goal to assess the efficacy of the Interview Guides. As discussed in the previous chapter, I had prepared five Interview Guides covering different aspects of company operations including IT, Marketing, Legal, General, and Privacy (I and II). With guidance from the Project Manager, I matched the interview guide to the individual so that the questions would be relevant to their information privacy experiences and organizational roles. Appendix K-2 identifies the interview subjects for the pilot study, the interview guide administered, and the interview type (in person or telephone, and whether or not the interview was audio taped). I was able to assess the efficacy of each type of interview guide in at least two interviews. However, I used the General guide more and the Privacy guides less than I had anticipated (largely as a result of the privacy inexperience of certain interviewees).

Efficacy of Interview Guides

The questionnaires worked fairly well in eliciting useful information. When asked, participants indicated that they understood the questions (even if they could not provide an answer), the language was appropriate to their circumstances (and they did not appear to hesitate to question or correct when I used unfamiliar terms or academic jargon), the subject matter appeared interesting to them, and they generally understood why they were being asked the questions. I think they appreciated being asked their opinions, and several inquired whether the firm would be receiving a copy of my dissertation. The process of using the different Interview Guides also helped me to observe whether I was getting the information I needed, the extent to which the separate Guides were necessary, and what additions may be necessary. To the extent that many respondents were not deeply familiar with the firm's privacy program (because it is under development), the General questionnaire guide sufficed. However, I assumed that research at sites with greater privacy experience would require more specialized treatment.

Improvements in Process

One early improvement made during the pilot study was to more explicitly explain two important aspects of the interview process at the beginning of the interview. First, I had to emphasize that I am not a lawyer and that my research seeks to understand broad themes of organizational approaches to privacy and not the legal ins and outs of the firm's privacy policy. Second, I articulated my specific interest in examining customer, information, privacy – three words that make up a single term. I tried hard throughout the different interviews to follow a routine that more explicitly transitioned from one section to the next. Both these small changes appeared to help reduce the frustration expressed in certain earlier interviews – namely, that they were being asked questions about customers or information when they thought they were being interviewed about privacy. For details and further discussion on the specific questions that were revised, see Appendix H-7.

Regional and Branch Versions

Another issue concerned the need to have specific Regional and/or Branch versions of the questionnaire, depending on the structure of the privacy program at each case site. Highly centralized organizations will likely only require the General version, while decentralized ones may require a more specific approach. I discuss the structural issue below.

Recognizing Organizational Idiosyncrasy

I believe that a critical aspect of my learning at the pilot site was regaining my appreciation for organizational idiosyncrasy. Clearly, it is important to be careful and consistent in conducting the interviews, to the greatest extent possible. However, my research protocol involved "semi-structured" interviewing. This approach does not require that interviews be exactly replicated. Rather, the questionnaires serve as conversational guides. It was my role as the interviewer to steer the interview, recognize and capitalize on the conversational dynamic to reveal information, and guide the sense-making between me and the interview subject. My experience at the different case sites showed that, while the guides are useful, the conversations were driven by a variety of factors largely unique to the research sites and, often, the least of which was my set of questions.

Goal Two: Validating the IPO Survey Instrument

The pilot study site agreed to distribute 40 survey kits to knowledgeable staff (including those who were interviewed). The survey kits were prepared as described in Appendix H-13.

I had initially negotiated with the pilot organization to have the surveys distributed during the week of the field visit (June 1, 2004). However, this was delayed because of some operational issues that required the Project Manager's attention. The surveys were eventually distributed in July for completion during the period July 15 – 30, 2004. However, almost half of the returned surveys arrived after July 30. Appendix K-3 summarizes the distribution of the completed

surveys. I received 16 completed surveys, representing a 40 percent response rate. Appendix K-4 summarizes the respondent characteristics. There were no significant differences among respondents by version, date or personal characteristics.

The surveys were analyzed in SPSS for frequencies and basic descriptive statistics (i.e., means, standard deviations, reliability) only as there was not a sufficient response to warrant further analysis as a separate case. Appendix K-6 reports these statistics. The information gleaned from the surveys was used as part of the triangulation strategy. The interpretation of the results is discussed in the section on applying the IPO Continuum to the pilot site.

Goal Three: Identifying Key Privacy Documents

I had hoped during the pilot study process to identify "typical" internal privacy related documents. This proved to be the most problematic issue given the pilot site's early privacy development stage. Very few internal documents were available, and I was not able to acquire several that do exist (requests were denied by the Legal department). Based on conversations with the Project Manager about "typical" compliance project documents, information gleaned during the questionnaire validation exercise, and my own research for privacy documents through corporate websites, I assembled a list of documents (see Appendix K-5).

These types of documents set my expectations for what I would attempt to review (and hopefully acquire) in the three main case research sites.

Goal Four: Expanding My Learning

This pilot study expanded my learning in two ways. First, I gained experience in carrying out systematic research using a variety of approaches. Second, I expanded my knowledge of information privacy as an organizational activity.

Lessons About Conducting Research

I identify and discuss four specific lessons including selecting interview subjects, the importance of using a knowledgeable insider, interviewing practice, and the need to stay organized (and to the extent possible, in control of the process).

Selecting Interview Subjects: A particularly important "research" lesson concerned the selection of interview subjects. I found that including a cross-section of personnel both vertically (addressing different functions) and horizontally (addressing different roles within the hierarchy) is necessary to gain real insight. Senior executives provided good "policy" perspectives on customer information privacy. They could talk about such issues as the tradeoffs made at the management committee table. For example, I asked a senior manager why the company had not proactively embraced PIPEDA but rather waited until PIPA became an uncomfortable and immediate inevitability. The response indicated that:

> ... it's [complying with PIPEDA] crossed our mind, it's just when are you going to do that? There's other, and as you go through your interview process there's a lot of other activities and initiatives happening right now in order to try to get a competitive advantage and maintain a competitive advantage to the other banks. There's so much going on, I don't think it's not a desire to do it, it's just too many other things happening at the same time.

Another senior person offered that:

> We had a consultant do a privacy audit just before Christmas. She gave us lots of recommendations and ideas. This was positive because it forced a good senior executives discussion about what we will and will not do.

Mid-level head office personnel, such as the marketing manager or the business systems implementation team leader, offered different insights. For example, a discussion of the challenges facing the organization as it implements its privacy program revealed the existence and possible source of a kind of arrogance around the gathering and use of customer information:

> [Manager]: I think we really need to, we've gone along for years with the kind of arrogance that we just know everything, you know, that Big Brother thing, that we can get that information, and we've got it...I'm saying long-time, like five-year or greater employees just think we're entitled to that information. They think it's an entitlement to have that information, and so we need to do a re-education.

> [Researcher]: What's the source of this arrogance ... and entitlement? I mean where did that come from?
>
> [Manager]: Three hundred years of banking. ... I think it's cultural. And that's across financial institutions, I believe. ... I still think that, I think there's still core bankers within there that have that, you know, "I might need that information." "What if you go bad and I need to track you down?" " What if?" And so, because we're such a risk averse business, like a lot of it is collected just because of, you know, the "what if". Even though you're, you know, less than 1 percent of our customers go that way. It doesn't matter: what if?

In a different vein, Operations personnel, such as the Help Desk staff, reflected the head office "policy imperative" as well as the branch level "practical implementation" perspectives in their understanding of the firm's privacy regime. For example, when asked about the circumstances when a branch would call the Help Desk with a privacy related question, the interviewee suggested that rather than having a specific concern,

> ... it's more that a customer has found out about this privacy and come in and confronted us and we're, our staff is not really sure, themselves, what they can do and what they can't do. So I think it's just confidence that they call us, just to reassure them.

Regional and branch staff likewise revealed differences in two ways. First, they talked almost exclusively in terms of the "physical security" aspects of information privacy. For example, when asked for an opinion on what constituted success in privacy terms, a regional manager responded:

> I'd characterize success, for example, if I was going into a branch, and I can see that there's nothing on the front counter that customers would have privy to that are actually, you know, customer files, anything to do with a customer is behind lock and key, and out of view where it could be looked at.

The information content aspects of information privacy were distinctly absent from the reality of non-headquarters personnel. Second, a separation of roles was articulated in which head office decreed and the branches executed, relatively unquestioningly. For example, a branch manager described the privacy program as "more of a corporate issue" and that the "branch manages what they've been told." There were no (and no perceived need for) privacy goals in the branch. It was merely a question of following the corporate policy and "practicing privacy", particularly emphasizing confidentiality and physical security.

These examples illustrate the benefit of interviewing a variety of personnel in the case studies. This is not only an important lesson from the pilot study but proved helpful in the negotiations with the case sites. I believe that my willingness not to require that the interviews be conducted exclusively among members of the top management team assisted in securing co-operation. I think it also suggested to the potential research sites that I understood the complexity of information privacy regimes in their kinds of firms and that some of the best insights would be gained from those not at the top of the hierarchy. However, as will be seen, this was not the case for all sites.

Importance of Knowledgeable Insider: Two important aspects of the insider role are identifying and gaining access to interview subjects, and clarifying the organization and its personnel. The Project Manager suggested adding "operational support personnel" (policy and helpdesk) who are knowledgeable about the specifics of organizational policies and who provide advice to branch personnel. To the extent that the case research sites are similarly organized, I requested the inclusion of these kinds of personnel in my site visits. In addition, while I had some understanding of the organization as a result of previous discussions with my "sponsor," it was the insights of the experienced Project Manager that helped illuminate aspects of the operation with which I was unfamiliar. For example, the knowledgeable insider provided insights about the history behind certain participants' comments, the way "compliance" issues typically are dealt with by the organization, and the different computer-based information systems (that related to customer information) in use in the branches and at head office.

Interviewing Practice: The third research lesson concerns my own work as the interviewer. The pilot site afforded me the opportunity to practice and refine my interview style. Over the course of the three days, I improved in my ability to be patient and not rush to fill awkward silences. I improved in my ability to listen actively, rephrase questions, provide feedback for verification, and connect disparate thoughts. As well, I was able to gauge timing more accurately. Two interviews ran longer than the scheduled hour, and were extended by

mutual agreement. In both cases, the quality of the information exchange merited this deviation for both parties. However, in every other case I was careful to begin and end on time as much as possible. I also learned to adapt to "group" interviewing on the fly. In a couple of instances, the Project Manager had arranged for more than one person to attend the interview. I quickly adjusted to the need to specifically address individuals, ask for verification between them, and keep control so that one individual could not monopolize the interview. In retrospect, I think that the "collective" approach is appropriate for certain types of employees, as it allows them to share experiences. I thus received a more comprehensive picture of the firm. As a result of this experience, I offered the case research sites the option to arrange "group" interviews if necessary, which I believe helped obtain cooperation.

Staying Organized: A final research lesson involved taking time at the beginning and end of each day to get organized and collect my thoughts. The pilot study mimicked what I expected to experience at the case study sites – long days of fairly high intensity involving exposure to many different people and much "data." The pilot study showed me the value of establishing routines in order not to be come overwhelmed by the experience. Each morning, I reviewed the interview schedule, ensured that I had sufficient consent forms, the correct number and type of questionnaires (along with extras in case of last minute changes), and extra batteries and tapes for the recorder. After each interview, I labelled the consent form, tape and questionnaire (on which I took notes) and placed them in separate folders. I added the identification number to the interview schedule. I also took a moment to write out any questions I wanted to follow up with the Project Manager. At the end of each day, I double-checked the consent forms, tapes and questionnaires against the interview schedule and made any notes for my own action. I also met with the Project Manager for a short debriefing session and to ask any questions that had emerged over the day.

The delays with the administration of the IPO survey also taught me the value of identifying survey participants prior to my arrival. The three main case study sites agreed to identify the 50 survey recipients in advance and to prepare a set of mailing labels for me to affix

to the survey envelopes on my first day at the research site. However, my best intentions were not always realized, as will be explained in subsequent chapters.

Lessons About Privacy as Organizational Activity

My second area of learning concerned gathering insight into customer information privacy as an organizational activity. There are four lessons of particular interest to my dissertation research: the importance of structural choices, locating privacy as a functional responsibility, stages of privacy, and the complexity of implementing privacy programs.

Importance of Structural Choices: A benefit of conducting the pilot in a "new" privacy organization was that the issues of importance were still being identified and debated. One issue concerns the structure of the privacy regime. While my study of the websites of financial institutions had suggested that there were structural differences among firms, I had not understood the potential significance of this structural decision. Through conversations with the Project Manager and my own reflections, I began to think of structure as an important indicator of something about an organization's information privacy orientation, though I was not immediately certain exactly what. I have since notionally begun to distinguish two broad structural types based on the degree of centralization of privacy program structure – what I refer to as the "islands of competence" structure and a more diffused approach. Structural issues will be monitored at the main case research sites.

Locating Privacy as a Functional Responsibility: Another important lesson is suggested by the choice of where the responsibility for privacy resides. I had originally considered this decision likely to be the result of political bargaining in the top management team (TMT). The TMT may, indeed, make the decision but the "meaning" behind the location decision may be more subtle and idiosyncratic than I had understood. For example, at the pilot site, the decision to locate the lead for the implementation was made because there was an existing group that led compliance based operational projects. The choice was made among Marketing (because privacy

involves communicating with customers, a central marketing function), Operations (because privacy involves all aspects of the operations of a financial institution), HR (because they already had a "privacy" person on staff), or Legal (because they also have a compliance mandate).

While IT could arguably be a candidate, this was not the case at the pilot site. The company has a comprehensive outsourcing agreement with a major global IT services provider which has reduced the capability of the IT group to assume a broader privacy role. The outsourcer was seen to be a "best practices" company on whom IT staff could rely for guidance on issues such as information privacy. IT staff were more concerned with ensuring that the pilot site implemented appropriate data and systems security standards than assuming corporate privacy leadership:

> primarily all of our IT services are provisioned by [outsourcer], so I have a partner in crime from the [outsourcer] camp who is my window into the back end. Coupled with that, as part of renewing our contract with [outsourcer] last year, I developed a security services schedule that stipulates exactly what we expect [outsourcer] to do for us in that arena.
>
> Researcher: So what kind of things [are] included?
>
> It's a fairly thick document, but it essentially – it determines or it governs how servers and resources are set up in our environment. Who has the authority to do what, how our perimeter security is set up, how our routers are configured, how our fire walls are configured. So every aspect, every technical aspect as well as logical access is determined by [outsourcer], or is governed by us for [outsourcer] to deliver.

The specific reasons for responsibility location decisions are likely a combination of factors, and I intend to explore this area at the case research sites. As was expressed to me in more than one interview (as typified by this quote),

> Look at where they put the job [meaning locating implementation within Operations]. I'm not saying it's a bad decision or the wrong one. It just says that the company doesn't see privacy as a broad issue but as a narrow issue.

Stages of Privacy: Most interviewees at the pilot site agreed that the company was in an "early" or "developmental" or "formative" stage of customer information privacy implementation. This was given as a main reason for the emphasis on control ("Legal tells us this is still a grey area so we have to be cautious") and cost minimization ("People are conscious of

how much you can end up spending. You're concerned with whether you're investing enough or too much" and "right now all we hear is that privacy is a drain on resources"). Interestingly, nobody expressed concerns over underinvestment in privacy. The pilot site's approach appears to stand in contrast to RBC's approach (which I discussed in Chapter Four). I have begun to think that perhaps organizations move through different stages of customer information privacy. The pilot site experience suggests that in initially organizing for privacy (particularly if the organization is hurrying to meet compliance), the emphasis is placed on symbolic acts such as placing a Privacy Notice on a website as a way to buy time and limit organizational exposure (hence the centralization of control) until the company has been able to carry out other critical tasks. This would suggest that "new privacy companies" may default to a compliance based, legitimacy seeking Information Privacy Orientation. As the Project Manager relayed to me, "We've got to be careful not to raise our customers' expectations. We're not in a position to do more than what we are currently doing. I'm still putting together the business case."

My thinking about a stages approach was still notional but I believed it warranted attention at the main research sites. As a result, I decided to ask specifically for information about how the privacy programs were initiated and what major changes have taken place over time. How this "stages approach" relates to the competing theories I am employing will be considered during the analytical phase of this dissertation research.

Complexity of Privacy Implementation: The pilot study helped refine and reinforce my understanding of the complexity of developing and implementing customer information privacy in information based organizations. I have been immersed in thinking about information privacy in organizations for three years, but I think I was beginning to take a fairly sterile perspective on operational impacts of how companies actually deal with customer information privacy. While I was at the pilot site, the Project Manager was preparing the Business Case for Privacy in order to receive the resources to carry out the policy implementation / compliance process. I was not privy to the contents of the Business Case but we had several discussions about certain issues to be

addressed. For example, the company has "thousands" of forms to be updated and reviewed by Legal staff. Outsourcing and third party supplier contracts required review in order to identify and resolve privacy issues. Information systems needed to be examined for privacy impacts, and programming changes identified and prioritized. Customer communications need to be developed and branch staff required training. All of these exemplify the complexities of implementing customer information privacy.

However, some of the interviewees suggested that there are bigger and tougher cultural and competitive issues to tackle as part of the implementation exercise. For example, several participants indicated that there was no uniform understanding across the company of the potential impact of privacy compliance on operations other than a certainty that it might be difficult and messy. Further, there was a "spectrum" of opinions on the merits of customer information privacy that ranged from "customers don't care about privacy" and "compliance is a necessary evil" to "compliance is an ethical imperative" and privacy as a way for the company to "demonstrate integrity." One participant expressed concern for the development of "trust issues within the organization." He suggested that violations of customer information privacy occurred routinely because employees would "keep a copy [of information] in order to keep the other departments honest." These opinions reflected the challenge of establishing what I call a coherent "cultural" understanding of customer information privacy in the firm.

A second large organizational challenge is forging a consensus on whether and how customer information privacy represents a competitive challenge or opportunity. Some interviewees did not see information privacy as a competitive issue at all but primarily as a "cost of doing business." They argued, "What's the upside of doing more than other FIs?" and "Where's the revenue opportunity?" They emphasized "privacy compliance" is mostly an issue of "managing customers' perceptions" in order to render this "a non-issue." In contrast, some participants identified maintaining or increasing customer trust as an important "upside" of customer information privacy. However, most interviewees were more concerned with the

perceived "downsides" of customer information privacy. These included managing around the constraints on collecting and using customer information to developing better offers; concerns for avoiding bad publicity because of a privacy failure; having to weather the negative effects of poor privacy behaviour by other financial institutions; and managing the impact of change on operations. A small minority of participants suggested that customer information privacy could be a "service differentiator" that supported "demonstrating respect for customers" better than their competitors. These distinct and different positions illustrate the complexity of introducing a change with firm wide ramifications. The pilot visit helped to make these complexities far more real and much less theoretical than I had previously experienced them.

Goal Five: Assessing Case A's IPO

My final goal for the pilot study was to assess Case A's information privacy policy, and its position against the IPO definition and on the IPO Continuum. To accomplish this, I undertook a mini "triangulation" exercise. I could not do a complete exercise as I did not have access to any written material beyond the privacy notice. However, I considered that the data collected in the interviews and through the surveys would be sufficient to attempt to apply the definition and tentatively place the firm on the IPO continuum.

Assessing the Information Privacy Policy

Consistent with my practice in Chapter Seven, I assessed Case A's privacy information on the basis of comprehensiveness, readability and accessibility. Table 8–1 summarizes the findings. Note that this firm had developed a Privacy Notice but not a full Privacy Policy. I assessed the Privacy Notice. The overall score generated for the Privacy Notice is 4, placing this firm's privacy approach near the bottom of the rankings identified in Chapter Seven.

Table 8–1: Case A - Privacy Notice Basic Assessment

Criterion	Key Questions/Concerns	Case A Results
Policy Comprehensiveness SCORE = 2	• Are all PIPEDA/fair information elements addressed?	• Refers to PIPA and claims compliance with that Act • Addresses key aspects of PIPA
	• Is there a summary of the policy that emphasizes key features?	• NO
	• Is responsibility clearly identified?	• Customers are directed to discuss questions with Customer Contact Centre. • Contact information provided for Privacy Manager.
Policy Readability SCORE = 1	• What is the readability score for the privacy policy document(s)? • Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 27.4 ("hardest" category) • Flesch-Kincaid Grade Level = 12 • Written in Plain English legalese
	• Are key terms explained?	• NO – other than very basic (and unhelpful) definition of "personal information"
	• Are examples provided? Are the examples thorough and understandable?	• NO
	• Are consent forms provided?	• NO
Policy Accessibility SCORE = 1	• How easy is it to find the policy? Are there multiple access points?	• Accessible from home page and subsequent pages; lower right corner next to Terms of Use, Legal Info, Contact Us & Site Map • Part of Legal Disclaimer site
	• Are there links to other privacy information (external)?	• NO
	• Is there a webseal or other "seal of approval"?	• NO

Comprehensiveness - The Privacy Notice refers to the provincial legislation (PIPA) and addresses the key aspects of the statute, specifically accountability; consent; collection; use; disclosure; access and correction; and care (accuracy, protection and retention). There is no policy "summary" (likely as a result of the absence of a comprehensive policy at this point). The Privacy Manager position is identified as the contact for complaints and enquiries, and contact

information is provided. This firm would be ranked low in comparison with the companies assessed in the Phase One study.

Readability - This firm's Privacy Notice is one of the more difficult to comprehend. The Reading Scores place it in the "hardest" category (Flesch Reading Ease <30). The Notice largely uses active voice and is written in what I call "Plain English Legalese." There is no glossary. Personal information is defined in an unhelpful manner ("Personal information is defined in the Personal Information Protection Act, and means information about you, as an identifiable individual.

However, personal information does not include business contact information about you, such as your business address, title, email or fax number.") No examples are provided and there is no consent form. This firm would be ranked low in comparison with the companies assessed in the Phase One study.

Accessibility - The Privacy Notice was easy to locate and could be accessed from homepages as well as other parts of the websites. There are no external or internal links to additional privacy information. There is no privacy webseal. This firm would be ranked low in comparison with the companies assessed in the Phase One study.

Section Summary - Overall, this firm provides a minimum of information to customers about information privacy. It appears to be minimally compliant with the provincial privacy statute. The score generated for this assessment exercise is 4 which, when compared to the firms in Study One, represents one of the lowest assessment scores. This is not too surprising given the early stage of development of this bank's privacy program.

Applying the IPO Definition

I also applied the IPO definition to this firm's privacy approach. However, whereas the Phase One Evaluation Study was restricted to a consideration of the respective firms' privacy policies, the Pilot Case was conducted using the Policy Notice as well as the data collected from the personal interviews and documents that were available on the bank's website. Table 8-2 summarizes the findings for the application of the IPO Definition.

Principles (External)

The bank is striving to implement the basic privacy principles articulated in the provincial statute (and those that are specifically identified in the schedule attached to PIPEDA). However, reference to the existence of these principles was restricted to those individuals one would expect to be aware of them, such as legal staff and those with specific privacy responsibilities. For example, when asked about what should be the goal for the bank's privacy program, a legal staff person responded,

> I'm actually just going to go back to the basic compliance with the act in terms of the 10 guiding principles. I think those are so firmly established, both federally and provincially, and through to the European Union, they're 10 very simple goals that, when you have them, you've got the whole thing down. So you're looking at the accountability, the retention, and – I can't remember – obviously they're so important. [Laughter] I got 2 out of 10, that's great. So, for that – that to me is like the ultimate checklist. If I can answer yes to those 10 questions.

Principles (Internal)

There were no specific internal principles articulated. This is not surprising given that the Business Case (wherein you would expect to find these principles) had not yet been prepared. However, I would expect that the external principles referred to above would figure prominently in any discussion. One interviewee mentioned that the bank's "philosophy of the privacy mandate" was best characterized as "primarily security of customer information, and only using

that information for which expression has been explicitly provided." This statement encompasses the fair information principles of safeguards, restricted use, and consent to use.

Table 8-2: Case A - IPO Definition

IPO Definition Component			Findings
Principles (external)			• There is reference to PIPA as the legal statute to which the firm must comply. • There was a reference to the "10 principles" and PIPEDA as a standard.
Principles (internal)			• There were no specific internal principles identified. However, the reference to the external "10 principles" appeared to serve as a guide to those who were aware of their existence. • Brief mention of security, consent and restricted use.
Values			• There is an ethical code that addresses confidentiality. • There is a customer service philosophy termed WUHAR - Welcomed, Understood, Helped, Appreciated and Respected. • There is a corporate value of being seen to be credible and having integrity in comparison with competitors. • There is a desire to be seen to be transparent and accountable.
Policies			• There is a rudimentary privacy structure in place. • Key initial privacy actions have taken place (i.e., appointment of CPO, appointment of customer and employee privacy managers, release of Privacy Notice, customer consent capability, information security in place). • Business Case to obtain resources is being prepared.
Objectives			• The objectives for the privacy policy have not been specifically articulated (await the Business Case). Certain objectives articulated by individuals in interviews.
	X	Legal	• Overriding concern for the bank is becoming compliant with privacy legislation.
	X	Technical	• Concern to implement ISO 17799 Information Security Standard but uncertain the degree to which this goal is understood or shared across the bank.
	X	Contractual	• Understand the need to ensure all third party agreements meet the bank's notice as soon as practicable.
	X	Business	• Some desire to create a "privacy culture" while others express goal for privacy to be a "non-issue" that does not consume too many resources.
	X	Social	• Some emphasis on privacy as a means to support development of broader, deeper and longer term customer relationships.
	X	Ethical	• Some expression of privacy policy as a vehicle to indicate bank's "honesty" and "integrity."
Decision rules			• Still being developed • Emphasis likely to be on minimizing implementation costs.

Values

I identified four individual or groups of values within the pilot site – confidentiality, WUHAR (customer service values), and credibility and integrity. I will address each in turn.

Several staff mentioned the importance of "confidentiality" as an overriding value in any financial institution. This value is expressly referred to in the Directors' Code of Conduct and Ethics (September 2003). Interestingly, confidentiality is not expressly defined. The relevant duty "to maintain confidentiality of any information gained" is illustrated in terms of customer expectations, specifically that

> [our] customers believe and expect that their financial business and personal information is protected at all times and that it is only viewed by those individuals who have a business reason to do so and is only used in a manner limited to information about customers' business operations, financial position, inventory and future plans, as well as personal information about an individual.

Secondly, a customer service philosophy called WUHAR (Welcomed, Understood, Helped, Appreciated and Respected) was referred to in several instances by a variety of staff as "implicitly support[ing] the idea of privacy." The importance of this service philosophy as a guide to privacy behaviors was particularly apparent in conversations with staff that articulated providing customer information privacy as demonstrating respect for customers. When asked to consider how privacy and the customer service philosophy meshed, it was suggested that

> For the company, it should mean that we say "privacy, this is good" not "privacy is an obstacle." It's in the best interests of the customers and employees, too. It's about having respect for customers and meeting their needs even if they want to opt out. It's in the best interests of customers, like the Fair Trading Act. So it's in our interests, too.

A last group of values included the ideas of operating with "integrity" and "credibility." It was important to the staff at the bank to overcome some "negative history" through establishing visible practices that strongly signaled that the bank was not seen to be any less credible or operating with any less integrity than their competitors. As was expressed by a senior manager,

> ...Because it would go to your credibility – you can't do privacy, how can you do anything else, you know? How can I rely on any information you give me if your systems

> are deficient? ... It's not like we have a monopoly. There's lots of people out there [competitors] who do what we do. Lots of alternatives.
>
> And,
>
> ...We're trying to build long relationships. Broad relationships ... [and so because] you have a broader relationship or a longer relationship, you have more responsibility [because]you have more information about them.

A few staff also expressed that integrity was an important value and that implementing a privacy program was an important aspect of being seen to be operating with integrity. This was especially the case when discussing the impact that the privacy program might have on staff, especially if the company was seen to be saying one thing and doing another:

> if you *say* you're providing confidentiality to customer information and you're not, that's going to have an impact on the morale of our staff, because we are then saying something and doing something totally different. So that has also an impact on [firm] and on our bottom line. So management can say one thing and do another, there's nothing to stop me from saying one thing and doing another, equally dishonest.

Policies

The bank has undertaken a series of "quick hits" in order to begin the process of developing and implementing a privacy regime. Key initial privacy actions have been undertaken (as described in the previous section on "Privacy Project Status"). The next step was to be the preparation of a Business Case to obtain necessary resources for undertaking the enterprise wide effort of embedding privacy into the bank's operations.

Objectives

I was able to gather evidence in support of all six objectives. While I identified that the overriding objective is to achieve compliance, I discerned that there were important secondary objectives as well.

Legal – The primary response to a question about the goals for the bank's privacy initiatives was "compliance." Privacy is, at this point, overwhelmingly a legal issue. The bank's 2004 Annual Report declared that "we are working to become compliant" [with the provincial

privacy legislation]. Furthermore, it was stated that the design of the privacy program would "entail actions that are supportable from a regulatory point of view."

Technical – There was some discussion of information security as an important privacy program objective. The bank appears to be pursuing implementation of the ISO 17799[1] Information Security Standard. In addition, automated systems for fraud detection were already in place (safeguards, and identified use of collected information) as were encryption, file transfer protocols, access controls and other important basic security measures. A challenge on the technical front will be to upgrade systems so "that the IT systems mirror the paper systems" with respect to the bank's privacy policies.

Contractual – Contractual objectives are and will continue to be important to the bank's privacy program. The bank's Privacy Notice advises customers that third parties must "comply with the Personal Information Protection Act or other similar legislation." However, it was indicated in the interviews that the bank was relying on "representations and warranties" to fulfill this aspect of their privacy notice. As noted,

> we've only been dealing with it [third party privacy assurance] really on an ad hoc basis, like every, when we're entering into a new contract we haven't been going back and reviewing our existing ones yet, which we have to do. And we don't share personal information with all the contractors, obviously. Most of the time, actually, what we've been relying on are their contractual representations and warranties, so we haven't been reviewing their privacy policies. Instead, what we've been asking is for a warranty so that in case it gets breached, we can hang them on that.

Over the longer term, the staff considered that reviews of third party agreements for privacy compliance may lead the bank to focus on fewer suppliers.

Business – There appeared to be two sets of potentially conflicting business goals. In one case, several staff (generally privacy knowledgeable) expressed a desire for the bank to cultivate a "privacy culture." While the specifics of that culture were not identified, several individuals

[1] ISO 17799 is a detailed information security standard that identifies 10 areas for organizational action: 1. Business continuity planning; 2. System access control; 3. System development and maintenance; 4. Physical and environmental security; 5. Compliance; 6. Personnel security; 7. Security organisation; 8. Computer and operations management; 9. Asset classification and control; and 10. Security policy. (http://www.iso17799software.com/what.htm) accessed 29/09/2004.

offered that the bank needed to engage in "change management initiatives" to support a privacy culture. This business goal seemed to have a sense of restriction attached to it – that the bank should preclude itself from certain behaviors (such as collecting every piece of information it could "just because" and for the reasons of "what if") and should invest in its privacy initiatives such as extensive staff training and strong customer awareness campaigns.

This seems to be a different goal from that articulated by a few (equally apparently knowledgeable staff) that privacy was really a "non-issue" and should be kept that way, and that privacy undermined the bank's ability to fulfill more important business goals, such as increased cross-selling and greater share of wallet. "It's not a corporate top issue. Try to manage costs and execute to minimize efforts." There was some expression that the business goal should essentially be one of balance – "We've got to deal with the legal/compliance side, living up to the letter and spirit of the legislation and getting on with running the business."

Social – There was evidence of a social goal for the privacy program. The goal intertwined the desire to create long lasting (and profitable) customer relationships with building customer trust. Some staff articulated a view that with the proper privacy measures in place, the development of the desired "broad", "deep" and "long term" customer relationships might be achieved. They used the term "know your customer" (which is a watchword for money laundering and fraud prevention practices) and applied it to a more positive approach in which knowing customers (through the collection of detailed personal information) could be used to assist the customers to purchase products and services that would better meet their needs (expressed as "financial goals"). The development of the longer term relationship would be taken as evidence that the bank was perceived as trustworthy by its customers.

Ethical – I found some limited evidence to support the ethical goal for privacy. The Directors' Code of Conduct and Ethics (which indicates that it is essentially similar to the managers' and employees' codes) includes Confidentiality as a major consideration. This Code states that "trust and integrity are the cornerstones" of the bank's business. I interpreted this

statement to mean that ethical behaviour, such as maintaining confidentiality, was one mechanism by which the bank would be perceived as being trustworthy. Only one interviewee argued for privacy as an ethical consideration. The context was that it would be unethical for the firm to publicly say that their privacy policy was a certain way and then proceed to operate differently. The ethical impact would be on employees. Specifically,

> ... if you work for a company that you don't believe is honest, it has an impact on all the employees ....So , if you're saying one thing and doing another, then *I* can say one thing and do another. I'm just, you know, *borrowing* this customer information ... if you're doing something illegal, I can do something illegal ... You create a culture of dishonesty, that we're *really* not here for the customers."

However, I suspect that many of the participants would have claimed that complying with privacy legislation was an important form of ethical behaviour if I had asked them specifically.

Decision Rules

No decision rules have been developed.

In summary, I was able to apply the IPO definition to the Pilot Case site. I found limited evidence of external and internal principles. I was able to discern several values that appear to guide corporate decision-making generally. While the Pilot Case site has yet to develop a comprehensive privacy policy, they have made several key policy decisions and are preparing a Business Case. All six privacy goals are in evidence to greater or lesser extents. The bank's overriding concern is to be seen to comply with the law. Based on the interviews, I would conjecture that the Business Case will be written to minimize implementation costs and minimize disruption to the operational status quo while achieving satisfactory compliance (according to the legal staff's interpretation of compliance) in order to minimize "reputational risk." Any decision rules will follow as a result of the Business Case development process. Applying the IPO Definition using all available data demonstrated the necessity of examining more than privacy statements if we are to learn the "why's" of organizational privacy actions. I will now describe this bank's placement on the IPO Continuum.

Case A's Position on the IPO Continuum

I triangulated data from the IPO Survey, the personal interviews, and the few documents I could obtain to establish Case A's placement on the IPO Continuum.

Survey Results

I used the results from Case A's IPO survey to establish a preliminary placement on the IPO Continuum. Appendix K-6 provides the statistical details. Table 8.3 shows the findings organized as an IPO score. To do this, I calculated a mean of the means for each component of the four constructs – customer relationship stance, information management strategy, privacy philosophy, and privacy behaviors. Then I weighted the items according to the level of effort required to achieve the different positions on the continuum. This generated a score for each layer

Table 8-3: Case A - IPO Survey Findings

IPO Component	Weighting	Mean of Means	Score for Component	Score for Layer	Interpretation
CRSA	-1	2.72	-2.72	5.35 = **5**	"Positive" relationship with respect to obligations owed to customers. **"Shared Responsibility"**
CRSB	-0.75	4.01	-3		
CRSC	0.75	6.12	4.59		
CRSD	1.25	5.18	6.48		
IMSA	-1	3.61	-3.61	1.71 = **2**	"Negative" use of customer information. **"Risk Management"**
IMSB	-0.75	5.3	-3.98		
IMSC	0.75	5.07	3.75		
IMSD	1.25	4.44	5.55		
PHILA	-1	1.69	-1.69	1.87 = **2**	"Negative" privacy philosophy **"Privacy as Constraint"**
PHILB	-0.75	4.19	-3.14		
PHILC	0.75	3.09	2.32		
PHILD	1.25	3.50	4.38		
BHVA	-1	2.47	-2.47	2.65 = **3**	"Negative" privacy behaviors **"Minimally Compliant"**
BHVB	-0.75	4.29	-3.22		
BHVC	0.75	5.25	3.95		
BHVD	1.25	3.52	4.4		

which I used to assign a placement. Figure 8-1 shows how I plotted the firm's position on the IPO Continuum based on the survey findings.

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		Case A		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
		Case A		
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case A		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case A	
IPO Score		↑		
	1	**2- 3** **4**	**5- 6**	**7**
	Weaker ←			→ ***Stronger***

Figure 8-1: Case A's Initial Placement on the IPO Continuum (Based on IPO Survey Results)

Note that I developed a weighting scale for assessing the relative contributions of the different components (i.e., CRSA, CRSB, etc.) that make up a layer (i.e., Customer Relationship Stance). The weightings are:

- -1 for items numbered 1 – 4 in any layer. (extreme left position)
- -.75 for items numbered 5 – 8. (mid-left position)
- .75 for items numbered 9 – 13. (mid-right position)
- 1.25 for items numbered 14 – 16. (extreme right position)

I developed these weights for the following reasons. First, I wanted to be able to generate an IPO score that would help differentiate among firms. Second, I wanted the score to reflect the level of effort that I am discovering that it takes a firm to implement a privacy program. Third, I wanted

the score to reflect that the level of effort does not appear to be symmetrical. Therefore, positions on the left of the continuum (weakest = -1, weaker = -.75) would not be as valuable as those on the right (stronger = .75, strongest = 1.25). That is, I believe that the effort to minimally comply with PIPEDA is less than that required to adopt a more developed approach (such as a Professional or Trade Group Code). However, becoming an "Enhanced Privacy" firm would take even more effort. I substantiate these uneven weights based upon my familiarity with privacy initiatives in firms and the different levels of effort required to achieve compliance let alone enhanced privacy. To my knowledge, there is no research documenting how firms go about the task of implementing their privacy initiatives. However, the following quote by from Cavoukian and Hamilton's (2002:124) practical primer on approaches to privacy in organizations indicates that this is not an easy effort:

> Before posting a Web site privacy statement for all the world to see or communicating a privacy policy to offline customers, it is essential that a company conduct a comprehensive review of its information management practices, documenting all information flows and making sure that processes and procedures are in place to achieve privacy objectives and mitigate risks. But the work doesn't stop there. Once a privacy policy has been crafted, a genuine effort must be made to instill a culture of privacy within your organization, through a top-down approach that includes education and training.

The scope of this challenge was underscored at a conference sponsored by the Canadian Marketing Association. Representatives of Bell Canada commented on the difficulty of managing customer information privacy across more than 100 billing systems that cover approximately 25 million "customer connections"[2]. Clearly, the practical experience of large organizations in implementing privacy programs suggests that movement across the IPO Continuum takes significant and sustained organizational commitment. This reality is reflected by the differentiated weightings I used to develop the positioning on the IPO continuum.

[2] Personal communication with Charles Giordiano, Bell Canada, September 2003.

In the next section, I discuss the findings by sub-construct and supplement the IPO Survey results with interview data to arrive at a final positioning for Case A on the IPO Continuum.

Customer Relationship Stance (CRS)

Recall that CRS is defined as *the organization's predominant characterization of its relationship to its customers based on the definition of its obligations to its customers.* Case A scored 5 on the CRS layer of the survey, indicating a "shared responsibility" position.

There was no evidence to suggest that the respondents considered their bank to operate with a buyer exploitation customer relationship stance. Respondents were neutral about the buyer self protection position. This may reflect the contractual nature of many banking relationships, and therefore, the legal requirement for customers to inform themselves. There was some limited evidence to suggest a consumer well-being position. However, there was less support for the two statements (CRS14, CRS15) that would require the firm to "give up" something in order to benefit their customers.

The strongest evidence was for the Shared Responsibility position. Respondents agreed with statements that indicated that firms and customers "exist for mutual benefit" (CRS 10) and that they should work together "to maximize customer benefits and firm profits" (CRS 9). In addition, there was agreement for the need for the two parties to "understand their respective responsibilities within the commercial relationship" (CRS 11). Consistent with this stance of mutual responsibility, respondents agreed that customers "deserved explanations of our business practices if they requested such explanations" (CRS12). Interview data supported this position on the IPO continuum.

Consistently across interviews, respondents expressed views of the importance of "customer focus" across the range of corporate activities, primarily in terms of the customer service initiative WUHAR (Welcomed, Understood, Helped, Appreciated and Respected)

circumscribed within the understanding that the business issues required participation by customers. For example, one participant remarked that customers can choose the information they share with the bank, such that "If you want to open an account with us, then you've got to give us certain information. If you don't want to, you can go to another bank but they'll just ask for the same information as we do."

In summary, there is survey and interview data to support Case A's position on the Customer Relationship Stance layer as "Shared Responsibility."

Customer Information Management Strategy (IMS)

Recall that IMS is defined as: *The organization's predominant strategy with respect to its objectives for gathering and using information.* Case A scored 2 on the IMS layer, indicating a "Manage to minimize risk" position.

All four positions were addressed to different degrees in the survey. Two positions (IMSA: manage to reduce information costs and IMSD: manage with information to create new reality) received the lowest scores. Two positions (IMSB: Manage to minimize risks and IMSC: manage with information to add value) were more evident. This apparent inconsistency across the IMS layer of the continuum is not too surprising given that the bank is in the early stages of developing its privacy program and has not yet defined how their information strategy should interact with their privacy approach (if at all).

At the same time, the certainty around the risk minimization and value-add positions is consistent with a bank's operations. Banks, by definition, are concerned to manage risk. Personal information is collected to manage credit risk and mitigate against fraud. These are stated purposes for collection and use of personal information (Policy Notice). As well, banks as financial services firms collect and manipulate personal information to tailor their market offerings. Again, this is a stated purpose in the bank's privacy notice, lending support to the IPO position. Data from the interviews further reflect this emphasis.

When asked in interviews why the bank collected personal information, responses consistently and, at a minimum, addressed risk issues and marketing opportunities. The following quotes neatly summarize these two information imperatives. The first quote is from a person involved with managing the bank's credit risks:

Researcher: What are the business's primary objectives for gathering and using customer information?

Participant: Well, managing fraud. Secondly, for identifying bankruptcy, when you have an interest in a loan or a card with us. Third, for being able to manage our own portfolio. And fourth, for being able to offer you new products and services.

This response indicates that risk management is a priority for the bank. Later on in the conversation, the participant also raised the issue of managing for information security. This was offered in the context of a discussion about the bank's objectives for its privacy program. The "security of ... our customer information .... making sure that it doesn't leave the organization" was offered as a primary objective.

Information security as a risk management tool was also raised by other participants. Several participants cited information security activities including the ISO Information Security Standard, firewalls, data encryption, access controls, as well as physical security activities.

However, the marketing importance of customer information was also prominent in the interviews, as illustrated in this quote from a marketer:

Researcher: What are your business' primary objectives for gathering and using customer information?

Participant: There are two objectives. First, we have to appropriately handle the business the customers have chosen to do with us. For example, if they have a RSP with us, we need to be able to contact them about maturity and options for dealing with that. Any kind of loan means we have to contact them over the course of the contract. We need this information to maintain service. Second, we need to be able to introduce products and services of interest to them. If they have a mortgage with us, do they know they can borrow against the equity in their house? So, we need that kind of information to communicate our offers.

The use of personal information to provide value-add service to the bank's customers was a consistent response among participants. Several interviewees commented that the bank's

customer service mandate (WUHAR) necessitated information collection. Customers can only be understood and helped if information is provided and acted upon (with respect). As well, a branch manager asserted that in order to achieve the marketing objectives of providing customers with the "full meal deal" (a comprehensive suite of financial services tailored to the individual), the bank had to gather very detailed information.

In summary, while the initial placement according to the survey data is "risk minimization", interview data suggests that the "add value" position is equally important to the firm. As a result, the revised positioning places CASE A as straddling the negative and positive sides of Information Management Strategy.

Customer Information Privacy Philosophy (PHIL)

Recall that PHIL is defined as *the organization's predominant philosophy about the role and impact that customer information privacy norms and laws have on the firm's ability to carry out its business.* Case A scored 2 on the PHIL layer of the survey indicating a "privacy as constraint" position.

The survey respondents did not agree with statements that suggested that their firm was not aware of or concerned for privacy. Neither did they agree with statements that viewed the imposition of privacy law as an exchange, an occasion to be used to obtain further information from customers. (This seems inconsistent with a position that views relationships with customers as one of mutual obligation as was indicated in responses to the Customer Relationship Stance.)

Interestingly, there was weak evidence that the bank viewed privacy as a constraint and an opportunity. For example, respondents somewhat agreed that "customers cared more about efficient service than privacy protections" (PHIL7) but somewhat disagreed that the "privacy law made it difficult for customers to get the best deal" (PHIL5). At the same time, respondents weakly disagreed with statements supporting the position of privacy as an opportunity for the firm. Data from the interviews support this apparent ambivalence about the impact of privacy

legislation but undermine any notion that this situation presents an opportunity. Interview data clarify this position to demonstrate that the bank is not interested in being a privacy leader. At the same time, it is concerned not to be compared negatively with its competitors on privacy issues.

With a few exceptions, participants were consistent in viewing privacy as a constraint on the firm's activities. For example, a marketer expressed frustration with the legislation, commenting that, "You know, most people really appreciate being told about these additional products and services. It's hard to understand the big deal about providing this information. It's what customers want. And more of them want this information than not." Furthermore, the constraints potentially affect how customers are segmented (and by extension how well serviced they may be): "We can infer from the products that they have, kind of, I guess, life stages, right? We can infer that, but a lot of the information we don't directly ask the customer because you're not *supposed* to ask the customer about that." From an operational perspective, the legal requirements were seen to be impediments mainly because they forced the workers to make changes to how they performed certain tasks and any change was seen to be unwelcome. Three participants remarked on the need for a "change management" effort to be engaged in order that the view of privacy could be altered from simply "it's mandated" and "it's a drain on resources" to "it's a priority" and "let's [use privacy as an opportunity] to be innovative and different." However, these views were a minority opinion. Overall, there was little support for any position other than privacy was "a pain" that had to be endured . In summary, survey and interview data place Case A in the "privacy as constraint" position.

Customer Information Privacy Behaviours (BHV)

Recall that BHV is defined as *the organization's publicly visible and internal information privacy activities*. Case A scored 3 representing the "minimally compliant" layer of the IPO Continuum.

There was clear and consistent disagreement with the extreme positions on this layer of the continuum. Respondents did not support statements indicating a lack of privacy activity, neither did they support statements that indicated an enhanced privacy position. Respondents were mixed in their views of whether the bank was minimally compliant (weak evidence) or was doing more than the legally mandated minimum but less than what would be seen to be privacy leadership (somewhat stronger evidence). Interview data reinforced the sense that the bank has yet to clarify its desired position (beyond basic compliance). This will likely be addressed in the Privacy Business Case currently being prepared.

In repeated interviews, respondents indicated that they could not see the benefit of doing anything more than what the law required. As was articulated by one of the legal staff, "I do see it more as like a price of entry. I'm not sure that *being more private* would help you ... once it becomes part of the culture and part of people's training, it's just a given, and it's not such a big issue. And that's where you want to get to." Many participants expressed the desire to not stand out from other financial institutions. The rationale given was either customer based or reputation based. The following quotes illustrate these positions.

Researcher: How important is it for your company to be seen to be behaving the same/different as other financial institutions with respect to dealing with customer information privacy?

Participant 1: [behave the same] We have to make sure our customers' perceptions are that they feel we are delivering their minimum requirements. Beyond that, I'm not sure it does matter to customers.

[behave differently] We wouldn't want to be perceived as looking worse. We want this to be a non-issue.

[assume privacy leadership] What's the upside of doing more than other FI's? I'm not completely convinced that there is one, but maybe there is.

Participant 2: [behave the same] It's important for [firm] to be, you know, where the rest of the industry is. And I think people would like their information to be confidential, but I think, but I think more important to them is the fact that you've approved the loan. Later, it might be more important that you're holding it [information] confidential, and nobody wants on lists, either. Nobody wants to have their name sold. So long as you're not selling then name, and you're giving them the loan, and you're coming in the pack the way every other financial institution deals with it, I think that that's what's important.

[behave differently] I think there could be negative press ... and then some loss of reputation. So if somebody gave you the loan, you'd go there, if nobody else gave you the loan, you'd still come here. We just would not be the first choice.

[assume privacy leadership] You may attract some customers, some people looking for a loan. And I think you *would* attract those people who have been burnt before, who have gotten onto a mailing list when they didn't want to, or [are concerned for] who's farming my name out there.

There appeared to be a broad consensus that privacy was best honoured quietly. It would be most important for the bank not to be seen to be different from other financial institutions and that any supposed benefit from privacy leadership had yet to be demonstrated to their satisfaction.

This view of privacy may partly be attributable to the perception that there was not a great deal of information available for "start up" privacy initiatives. This would help to explain the perception that there was only one set of available privacy behaviours (minimal compliance and nothing else). As well, participants did not identify any competitor as standing out as a privacy leader, therefore, there was no possibility for emulation even if there was interest in so doing. Finally, the perception that the bank's executive was very concerned to minimize the cost and disruption of implementing the privacy program may have lead participants to respond in a manner that downplayed the ability and desirability of exercising privacy leadership.

In summary, taking together the IPO Survey responses and the interview data, there was more evidence to support Case A in a "minimally compliant" position than any other position on the BHV layer of the continuum.

Section Summary

Case A is repositioned on the IPO Continuum as a firm that is working on becoming compliant and firmly ensconcing itself as a compliant but not leading privacy firm. It casts its Customer Relationship Stance as a matter of "shared responsibility." It conceives its Information Management Strategy as a combination of "minimize risk" and "add-value" positions. It views privacy legislation as an imposed "constraint" that must be endured. Finally, it aspires to be

"minimally compliant" on the Privacy Behaviours layer. Figure 8-2 shows the redrawn IPO Continuum for Case A.

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		Case A		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
		Case A		
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case A		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case A	
	Weaker ◄——————————► ***Stronger***			

Figure 8-2: Case A's Final Placement on the IPO Continuum (Based on Triangulated Results)

Theoretical Assessment

In this section, I review Case A's information privacy orientation first using the Institutional Approach and then the Resource-Based View.

Institutional Approach

Case A's information privacy orientation can best be explained using the lens of the Institutional Approach. I briefly apply the attributes of the institutional paradigm (more fully described in Chapter Five) to demonstrate how this theory helps to explain Case A's approach to their privacy program.

Organizational goal: Case A's orientation to information privacy is overwhelmingly a question of complying with legal requirements. The bank does not appear interested in making changes to their operations other than those that are absolutely required (managerial legitimacy) to bring them into compliance with the PIPA legislation in their province (pragmatic legitimacy). The search for legitimacy is largely expressed as a desire to not be perceived by external audiences as being "offside" in comparison with their competitors. As indicated in previous sections, the concern is to "minimize exposure" and implement the initial activities required to bring the bank into basic compliance. In sum, Case A's organization goal can be described as seeking pragmatic and managerial legitimacy through their privacy program.

Source of Pressure: Case A is implementing their privacy program strictly as a response to the PIPEDA/PIPA requirements (cause). Furthermore, the bank claims that there was no internal organizational demand or customer demand for this action (constituency). The bank is presently determining what the principles and norms will be for their privacy policy. Currently, they rely on a basic interpretation of the 10 principles in PIPEDA to underpin their privacy actions (content). The privacy program has been "legally coerced" in that the bank would not have adopted a formal, enterprise-wide program if there had not been the law and accompanying

sanctions to force this action (control). However, the bank also recognizes that it is part of the larger financial institutions industry. As such, Case A needs to be able to operate within the industry (interoperability standards) as well as withstand scrutiny from peer organizations (context.) Note that Case A is a member (partial) of the same national trade association as Case D.

Ability and Willingness to Respond to Pressure: Case A is attempting to respond to the pressure to implement a privacy program by, on one hand meeting their legal obligations while, on the other, minimizing resource consequences. At the time of this case, the Project Manager was researching organizational privacy models and preparing a business case. However, it must be noted that this bank sees itself as occupying a particular market niche. As such, they appear to be less embedded in a social network than is the case for the other banks I studied. As a result, the Chief Privacy Officer and the Privacy Project Manager are advocating a narrow compliance approach to the program. However, until the actual business case is prepared, there is insufficient evidence to identify the extent to which the bank chooses to emulate other financial institutions' privacy programs.

Response to Pressure: As indicated above, there is insufficient data to assess Case A's actual response to pressure given that their program was in the design stage at the time of this research.

In summary, Case A's information privacy orientation can be analyzed using the Institutional Approach. The bank appears to be pursuing an acquiescence strategy.

Resource-Based View

Recall that I theorized in Chapter Four that the Resource-Based View would offer a lens through which to consider IPO heterogeneity. That is, I offered two resource-based interpretations for firms that appeared to be interested in pursuing privacy as a source of sustainable competitive advantage either through a knowledge or relationship based capability.

It is premature to consider the Resource-Based View with respect to Case A's information privacy orientation. The bank is not currently interested in pursuing privacy as a source of competitive advantage either through their information or privacy practices. The focus of their activities at present and for the foreseeable future is to implement a basic and compliant privacy program. Once that has been accomplished, I would expect that the bank will expend minimum resources to maintain the program and devote their energies to more central organizational concerns.

In sum, the RBV currently offers limited insight into Case A's information privacy orientation.

Chapter Summary

In this chapter, I reviewed the process of conducting the Case A: Pilot Study and discussed the results. I described the research site and setting, outlined the goals for the pilot study, and discussed the successes and learning from the pilot study. Using a triangulation approach (based on interview, survey and documentary data), I applied the IPO Definition and defined the layers of the IPO Continuum. Then I mapped Case A onto the IPO Continuum. Finally, I considered Case A's information privacy orientation through the competing theoretical lenses and suggested that their present position is best explained using the institutional approach. Through these efforts, I achieved the five goals I had set for the Pilot Study, demonstrated the validity of the research instruments in a field setting, and showed how the institutional approach could be applied to explaining IPO.

CHAPTER NINE

CASE B

In this Chapter, I describe the results of the first field case study, Case B. This research site was one of the desired sites that I identified in the Privacy Policy Evaluation Study. Briefly, I conducted a four day research site visit at Case B's head office in July 2004. I interviewed 14 executives, managers and senior staff about how the company had gone about organizing and implementing their customer information privacy program. I also collected 65 documents related to privacy and distribute 54 IPO surveys (of which 33 were completed and returned for a 61% response rate).

This study was undertaken to answer the first two research questions:

R(1) Do firms have an Information Privacy Orientation?

R(2) Is Information Privacy Orientation constructed as I have theorized?

This chapter provides evidence to support an affirmative response to these questions. To demonstrate this support, I assess Case B's information privacy orientation based on the triangulation of the interview, survey and documentary data I collected. First, I assess the firm's privacy policy for comprehensiveness, readability and accessibility. Second, I review the firm's privacy program against the IPO Definition including principles (external and internal), values, policies (governance, resources, evaluations), objectives and decision rules. Third, I position the firm on the IPO continuum. I report the initial positioning based on the results of the IPO Survey. Then I reconsider the positioning layer by layer (customer relationship stance, information management strategy, privacy philosophy, and privacy behaviours) by triangulating the survey, interview and documentary evidence. I provide a final positioning on the continuum for Case B. Note that Appendix L contains a collection of information from Case B's case study database, including interview and document lists, and IPO survey statistics. To set the stage for

understanding the IPO analysis, I provide a brief background to the development and implementation of Case B's privacy program.

Case B Privacy Program Status: "The Privacy Project is Completed"

Case B undertook the development and implementation of their privacy compliance program in May 2001 well in advance of the January 2004 deadline. The bank decided to move up its compliance schedule for four reasons. First, it expected that the provincial legislature would pass its own privacy legislation in order to assert provincial regulatory authority and, therefore, the firm would have to comply at some time with some privacy statute. The thinking appears to be "we might as well get it over with." Second, several service delivery partners (such as insurers) were already required to be PIPEDA compliant as they were engaged in "inter-provincial" businesses (personal information crossed provincial borders in the course of doing business). These suppliers were beginning to ask the financial institution for "representations and warranties" that personally identifiable information was being handled in accordance with the law. Third, the national trade association, of which this firm is a perceived leader, was encouraging its members to "voluntarily" implement privacy compliance regimes before being required, in order to:

> a) Not lose ground to competitors who were already compliant ("achieve competitive parity");
> b) To signal to the federal government that these firms took the privacy issue seriously and would be compliant by the deadline ("address reality"); and
> c) To demonstrate their concern for their customers' information privacy ("meet consumer expectations").

Privacy Program Context

However, there was a fourth explanation that many participants in this study thought was the real reason for Case B's early privacy efforts. The bank was able to "efficiently" address privacy by "piggybacking" it onto another compliance initiative. The Proceeds of Crime (Money Laundering) regulations had been promulgated in February 2001 (with compliance required by

September 2001). A Project Charter[1], drafted by the Senior Manger, Compliance & Audit, argued for the simultaneous tackling of the two compliance projects because of the "commonalities between the requirements of the two pieces" pertaining to the collection of personal information. (Interestingly, the documentation suggests the issue of commonality had more to do with the assignment of responsibility for compliance than for information management practices).

I asked several participants in the interviews two questions concerning the priority and, hence, the timing of the privacy initiative at Case B. First, would the privacy program have been initiated in advance of the deadline if the Money Laundering regulations had not also been required? Second, what would have happened to the privacy program if the firm had been in the process of another, unrelated major initiative, (such as a merger with another financial institution) or a significant information system change (such as changing the banking platform)? I received mixed responses to both questions. The Privacy Officer seemed convinced that the Privacy Program would have proceeded at that time and under any and all circumstances because the Board thought it was important to do (as did the national trade association) and it was "mandatory" (meaning a legislative requirement). However, several others (in Head Office and in the Branches) indicated that they thought that the Money Laundering project was the real priority. It was because the Compliance & Audit staff was able to combine the two initiatives that the privacy project was undertaken prior to the deadline. Furthermore, it was asserted that the privacy initiative would have been forced to the backburner by a significant merger (which requires the commitment of many resources during both the negotiation/due diligence and the actual merger stages). As a head office staff person indicated, "We would have done it [implemented PIPEDA] but not until the last minute."

Why is understanding the timing of the privacy implementation initiative important? Why do we need to know about the dual compliance project? The answer to these questions is that they reveal how privacy is handled at Case B – Customer information privacy is an exercise

[1] Project Title: Money Laundering and Privacy Legislation.

in compliance, nothing less but certainly nothing more. More interestingly, perhaps, is the juxtaposition between the Money Laundering initiative and PIPEDA. Technically, these initiatives may share "some commonalities" and, thus, it appears to be efficient to pursue them in tandem. However, the statutes exist for very different reasons and mixing the two processes may obscure these differences. The Money Laundering Regulations "set[s] out the reporting, record keeping and client identification requirements" that financial institutions (and others) are required to implement to assist the federal government to track the movements of large sums of money. These regulations require organizations to intrude on their clients' privacy as a means to protect society. In contrast, the PIPEDA exists to protect individuals and provide them with a measure of control over their personal information. By tackling the two pieces as a single project, Case B may have signaled, however unintentionally, that PIPEDA was not really a priority. Interview data suggests that some participants in training sessions, for example, had difficulty recalling what was covered in the privacy training but recalled the "extensive" training they received on the Money Laundering regulations.

The Privacy Project Charter was presented to the firm's Board of Directors and approved with very little discussion. This was "not because of indifference" according to the Privacy Officer but because early adoption of the privacy program was considered to be "the good and proper thing to do." Approval was given for the project to be undertaken as a two pronged compliance initiative. The first priority was to develop and implement the requirements of the Money Laundering Regulations that while the second priority was to develop and implement the response to PIPEDA. The total project was undertaken over the course of a year with the PIPEDA implementation piece occupying the period of October 2001 to July 2002. The Senior Manager, Audit & Compliance (who was appointed the bank's Privacy Officer) was placed in charge of the project.

Implementing the Privacy Project

As a result of the two-pronged approach, Case B undertook the development and implementation of its privacy compliance program using what I term a "minimization strategy." The Project Charter illustrates that the firm was interested in complying with the statute but not at any cost nor to the greatest possible extent. Specifically, the Charter authorized a limited project scope:

Scope IS	Scope IS NOT
To change/add policies/procedures to ensure compliance with legislation	To make changes in policies/procedures that may be identified during the project but are not essential to compliance with the legislation
To identify and implement system changes necessary to support procedures for compliance	To make system changes other than those needed for compliance e.g. do not build a *system* to enable us to identify suspicious transactions

I interpret this scope statement to mean that while the implementation team was to maintain awareness of the broader privacy picture in the firm, no specific action was to be undertaken unless it could be specifically identified as directly contributing to compliance. While no specific cost-benefit analysis was performed (because it was not deemed to be possible to calculate), the Project Charter acknowledged that while "Establishment/ maintenance of the requirements is in any event mandatory. Efficient, cost effective practices will be built into the measures adopted so that they are "comfortably adequate but not exaggerated." In other words, Case B's privacy team was to take the "no frills" approach to privacy compliance because PIPEDA compliance was really "more an issue of understanding the rules and applying them to our business."

This approach dictated that Case B find the most expeditious means to achieving PIPEDA compliance. To do this, the Privacy Officer recommended (and received approval) to adopt the regime recommended by its national trade association. Adoption of the regime had two important implications for Case B. First, it meant that the bank achieved its "efficiency" goal in PIPEDA implementation. By adopting the national model code, they received a complete package

of privacy guidelines (including board resolutions, communications plans, training session outlines and detailed policies and procedures) as well as an implementation guide. This meant that the privacy team did not have to engage in independent research to craft a PIPEDA response that would minimize the bank's risk of being non-compliant[2]. Second, they achieved a compliance level that was consistent within their industry. This addressed their goal to have a level of compliance that was "comfortably adequate but not exaggerated."

In July 2003, the Privacy Officer declared that the "Privacy Project was completed." All the boxes were ticked on the implementation checklist. The Privacy Officer writing in the project closeout report ("Post Implementation Review") indicated that the project was complete and had achieved its goals. When I asked what was next for the privacy program at Case B, the reply was to "keep on top of things" but there were no plans to engage in any activities beyond a "maintenance" level (my term). For example, there were no plans to have an external audit/verification process or to engage in raising the profile of privacy with customers (unless something untoward happened). The Privacy Officer mused that perhaps they would attend to some "reinforcing" activities with staff. (Beyond the annual ritual involving reading and signing the Code of Conduct Policy (which addresses privacy and confidentiality issues), there was no ongoing effort to maintain staff awareness of privacy.) However, there were no plans beyond maintaining vigilance and reporting quarterly to the Board's Audit Committee.[3]

In summary, Case B represents a financial institution that has taken a straight forward "compliance" approach to the task of implementing their privacy program. They have concluded

---

[2] The one exception was the draft brochure to explain the privacy policy geared for customers. Case B did not use the draft. Instead, they adapted language used by a competitor and, with assistance from their external legal counsel, produced a brochure that they felt better conveyed their privacy message.

[3] At the time of my research visit, Case B announced that they were in merger talks with another regional financial institution. The firm that is the potential acquisition had been included in my original evaluation of privacy policies (Phase One Study – see Chapter Seven). Interestingly, the target firm had scored higher than Case B in the evaluation. I asked the Privacy Officer about how the privacy programs would be assessed and amalgamated. The response was that this would be part of the discussions and that there had been conversations between the privacy staff of the two banks prior to any announcement of the merger proposal. The Privacy Officer wsa looking forward to the challenge of bringing together the two privacy programs.

the "privacy project" and thus, completed having the organizational spot light turned onto privacy initiatives.

In the next section, I assess Case B's privacy policy.

Assessing Case B's Privacy Policy

Consistent with my practice in all cases, I assessed Case B's privacy information on the basis of comprehensiveness, readability and accessibility. Table 9–1 summarizes the findings. I assessed the information contained in the brochure "Our Commitment to Protecting Your Personal Information" that is also available on the online banking site (but only in the password protected area).

The overall score generated for the Privacy Notice is 7.5, which would place this firm's privacy approach in 5th place within the rankings of the ten firms examined in Chapter Seven.

Comprehensiveness – Case B scored 4.5 for comprehensiveness. The Privacy Notice refers to and provides basic information about each of the ten principles (called a summary) of the Model Code adopted by the firm, accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance. Key aspects of the policy are easily identifiable through headings and subheadings. The Privacy Officer position is identified as the contact for complaints and enquiries ("Questions? Ask Our Privacy Officer"), and contact information is provided. As well, a brief description of the Privacy Officer's duties is provided:

> ... Privacy Officer is your point of contact if you wish to raise any matters regarding the use of your personal information. The Privacy Officer is responsible for monitoring information collection and data security and ensures that other [firm] staff receive appropriate training on privacy issues and their responsibilities under the Code. The Privacy Officer also handles all privacy inquiries and personal information access requests under the Code.

Table 9-1: Case B - Privacy Notice Basic Assessment

Criterion	Key Questions/Concerns	Case B Results
Policy Comprehensiveness SCORE = 4.5	• Are all PIPEDA/fair information elements addressed?	• Refer to Model Code and claims compliance with it. • Addresses key aspects of PIPEDA
	• Is there a summary of the policy that emphasizes key features?	• No.
	• Is responsibility clearly identified?	• Privacy Officer is referred to. • Customers are directed to discuss questions with Customer Contact Centre or to seek information through online banking website. • Contact information is provided for customer contact centre.
Policy Readability SCORE = 1.5	• What is the readability score for the privacy policy document(s)? • Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 35.4 ("harder" category) • Flesch-Kincaid Grade Level = 12 • Written in Plain English legalese
	• Are key terms explained?	• NO – other than very basic definition of "personal information"
	• Are examples provided? Are the examples thorough and understandable?	• NO examples.
	• Are consent forms provided?	• Yes – in privacy brochure. • Not able to access from online banking – exists within password protected space only.
Policy Accessibility SCORE = 1.5	• How easy is it to find the policy? Are there multiple access points?	• Privacy link from home page to Legal Disclaimer site is confusing (as this does not provide the policy). • Need to access on-line banking to obtain information (through password protected section). • Only information available is on-line banking related security information. • Brochures are obtainable from branches and by calling the Customer Contact Centre.
	• Are there links to other privacy information (external)?	• NO.
	• Is there a webseal or other "seal of approval"?	• NO.

Readability – Case B scored 1.5 for readability. This firm's Privacy Notice is one of the more difficult to comprehend. The Reading Scores place it in the "harder" category (Flesch Reading Ease >30). The Notice is largely uses active voice and is written in what I call "Plain English Legalese." Personal information is defined in the Privacy Brochure as –

> "We hold personal information ... to help us meet and maintain the highest standards of financial service. This information can include your name, address, age, income, use of accounts and credit history, as well as the relationship of others linked to you in account services." (My emphasis)

The highlighted section of the definition is confusing but otherwise this is useful information for customers.

There is no glossary and no examples are provided. A consent form is available in the brochure. There is no generally accessible (i.e., not password protected) consent form available through the firm's website.

Accessibility – Case B scored 1.5 for accessibility. The firm's privacy brochure can be obtained from a branch or by contacting the Customer Contact Centre. However, it is more difficult to locate and obtain from the firm's website. Specific privacy information and consent preferences can only be obtained by customers that have signed on for on –line banking services. The privacy policy is not obtainable from the homepage (there is a link that connects to legal disclaimer information). The only generally available information is about security in online banking. The only instance in which privacy is mentioned is in the final paragraph of the Security FAQs:

> **Security**
> [FIRM] Internet Banking offers you the best security available in a commercial environment using the SSL3 method of encryption (Secure Socket Layer). This together with the using a 128 bit enabled browser means your *privacy* and confidentiality are ensured. (My emphasis)

There are no external or internal links to additional privacy information. There is no privacy webseal.

Summary - Overall, this firm provides good basic privacy policy information to existing customers about information privacy. However, prospective customers might experience difficulty in finding privacy information. The policy appears to be basically compliant with PIPEDA. The score generated for this assessment exercise is 7.5 which, when compared to the firms in Study One, represents a middle position (5th rank) among the range of assessment scores that were generated in the initial evaluation of privacy policies (see Chapter Seven).

Applying the IPO Definition to Case B

I applied the IPO definition by coding the interviews and the privacy documents I was able to obtain. The coding was reviewed and approved by my supervisor. In both instances, I looked for information, quotes and examples of the different aspects of the IPO definition – principles (external and internal, values, policies, objectives and decision rules). Table 9-2 summarizes Case B with respect to the application of the IPO Definition.

Principles

External: There is reference to PIPEDA as the legal statute to which the firm must comply. External Principles were articulated in several documents (such as the national trade association's Model Code) as well as by certain more knowledgeable interviewees. The documents expressly identify the CSA Model Code and PIPEDA as the basis for privacy action by the firm.

Internal: The previously identified External principles form the core of the firm's Privacy Principles and are referenced in documents including the Project Charter, the Code of Conduct Policy, the Privacy Notice (including Customer pamphlet), the staff section of the intranet, and the actual Privacy Policy. Privacy and Confidentiality Standards" form part of the Code of Conduct and include specific reference to the 10 privacy principles.

Table 9-2: Case B - IPO Definition

IPO Definition Component	Findings: Case B
Principles (external)	• Model Code provided by national trade association refers to CSA Model Code, PIPEDA and the 10 interrelated privacy principles.

Principles (internal)	• Privacy and confidentiality standards form part of Code of Conduct Policy. Privacy Standards are the 10 privacy principles that are in CSA Model Code/PIPEDA/ Model Code (referred to above).
	• Operating principles
	  • Right to be left alone
	  • "How would you feel if?"
	  • Tradition of confidentiality.

Values	• Code of Conduct emphasizes honesty, fairness and lawfulness. • Code of Conduct establishes shared commitment to high moral, ethical and legal standards. • Commitment statement requires acting with respect, integrity and trust. • Privacy policy supports the value of "maintaining the rights of customers".
Policies	
Governance & Structure	• Comprehensive policy adopted by Board of Directors incorporates national Model Code (adopted 2002; compliance deadline 2004) • CPO Responsibility – assigned to Senior Manager Audit & Compliance • Provides quarterly reports on privacy compliance matters to the Audit Committee of the Board • Intra-organizational committee meets quarterly to discuss issues
Resources (domestic retail banking only)	• Part of formal responsibility of two staff (Audit & Compliance within Finance division) but not full time responsibility • Access to legal counsel on retainer • No formal budget. • Designated staff in branches (usually an Assistant Branch Manager) • Customer Contact Centre as point of contact for complaints and inquiries if not dealt with at Branch level.
Reviews & evaluation	• No formal privacy assessment prior to implementation (worked through internal committee) • Not formally included in operational audit
Objectives	
Legal	• Overriding objective is sustained legal compliance. • Particular emphasis on obtaining consent.
Technical	• Concern expressed for security, identity theft and related issues. • Safeguards include physical, logical, technical and organizational measures to "protect personal information from loss or theft, unauthorized access, use copying, modification, disclosure or disposal."
Contractual	• Working to ensure 3rd party compliance with vendors, suppliers and affiliates. • No concern for trans-border issues (i.e., Patriot Act and affect on compliance with PIPEDA).
Business	• Audit /compliance issue. • Strong risk management bias (i.e., credit risk management). • Some concern for "reputation" risk management in the event of a privacy breach. • Not using CRM at moment, in planning stages. Unclear what impact will be. • Objective is to render privacy a "non-issue."
Social	• Some suggestion of relationship between privacy and trust. • Some evidence to support privacy as a means to support broader, deeper and

	longer term customer relationships.
Ethical	• Use of term ethical in Code of Conduct but not specifically a reference to privacy. • Board considered adopting Code in advance of compliance deadline the "good and proper thing to do."

Decision rules	• Evidence of deliberate choices made in how privacy is operationalized.
	  • Does not sell customer information.
	  • Does not purchase customer lists.
	  • Does not data mine transaction information in order to directly solicit business.
	  • Does not issue account balances over the telephone to other financial institutions.

Values

Case B's Code of Conduct applies to all Directors, officer and employees of the firm. The Code of Conduct (in which standards for privacy and confidentiality are specifically referenced) states that:

a) Business should be conducted honestly, fairly, and in accordance with the law.
b) There is a shared commitment to high moral, ethical and legal standards.

The firm is also committed to "supporting our communities and valuing our members and employees by acting with respect, integrity and trust." In interviews with a variety of personnel, the emphasis on the firm's tradition of confidentiality and the concern for maintaining customer trust as guiding values was evident. For example, a Branch Manager commented

> ... even before the privacy legislation ... I think it's [privacy] crucial because if you [customer] your money's here regardless of whether they are deposits or credits and you're blabbing it all over the place, who's going to deal with you? And one person can ruin it for ... a company, a branch ... it's an expected requirement when they [customers] come through the door ... everything you've said is confidential.

Customer information privacy is seen to be an extension of historical practice that supports the values of "maintaining the rights of customers". The firm's privacy brochure (distributed to existing customers and available on request at branches and through the on-line banking system) emphasizes the commitment "to the development of policies, procedures and service offerings that maintain these rights." After outlining the actions taken by the firm, the brochure continues "Through these actions, what has been our accepted practice becomes our

documented commitment to you ..." Given that the firm had not previously adopted a privacy policy, I interpreted this latter statement as a renewed commitment to the previous practice of confidentiality within the larger privacy policy context.

Policies

I consider the policies of Case B under three headings – governance, resources and evaluations.

Governance: The firm adopted a comprehensive privacy policy based on the Model Code supplied by the national trade association, in 2002. The Model Code is accompanied by detailed policies and procedures as well as form templates and suggested language for such activities as obtaining consent or ascertaining compliance by third parties. The Model Code's explicit requirements exceed PIPEDA minimums. The Audit Committee of the Board of Directors receives quarterly reports on the bank's privacy compliance. An intra-organizational committee, largely composed of personnel who were associated with the privacy implementation team, meets quarterly to discuss issues and provide a forum for monitoring the privacy compliance of the bank.

The Chief Privacy Officer (CPO) role is occupied by the Senior Manager, Audit and Compliance (who reports to the VP Finance). This person was appointed because "there was a lack of awareness elsewhere in the company" and "I was interested, knew a bit about the issue and was already responsible for compliance." In addition, there was a movement to shift the firm from a "tick and check" to a "compliance organization" so adding privacy to the position seemed a good fit.

Resources: The two staff in the Audit and Compliance group are responsible for the privacy program but this is a part time responsibility. The privacy staff have access to external legal counsel but otherwise have no formal, dedicated privacy budget. At the branch level, there is typically an Assistant Manager who is responsible for handling privacy enquiries. In addition,

the staff at the Customer Contact Centre field complaints and enquiries that have not been directed to branch level personnel.

Evaluations: In keeping with the bank's "no frills" approach to their privacy program, there was no externally conducted privacy assessment conducted prior to the privacy team being assembled in 2001. The CPO consulted with the external legal counsel but largely relied on members of the privacy team to carry out necessary assessments within their operational areas. The bank does not require privacy procedures to be examined during operational audits.

Objectives

I was able to gather evidence in support of all six objectives. While I identified that the overriding objective is to achieve compliance, I discerned that there were secondary objectives as well.

Legal – The primary reason for Case B to develop and implement its privacy program was to comply with the federal law. In response to a question about the goals for the bank's privacy initiatives, all interviewees identified "compliance" as their first choice. In the IPO Survey section that requested respondents to rank a series of privacy statements ("In my company, privacy of customer information is primarily a _____ issue"), the response "legal compliance issue" was ranked first or second by 27 (of 33) respondents. Privacy at this firm is overwhelmingly a legal issue which helps to explain why the Privacy Officer is also in charge of audit and compliance – privacy is considered to be a set of legal rules to be followed in order to avoid legal sanctions.

Technical – There was some limited evidence of information security as an important privacy program objective but within the overall framework of their privacy policy, not as a separate objective. The Model Code (and PIPEDA) refers to "safeguards." Safeguards include physical, logical, technical and organizational measures to "protect personal information from loss or theft, unauthorized access, use copying, modification, disclosure or disposal." Branch

discussions centered mostly on physical safeguards while head office discussions, infrequently, mentioned security. The emphasis appeared to be on following the policy and auditing for compliance. Technical or security provisions were also seen to be something that "we do anyway" and that were highlighted by but not created as a result of the statute or the firm's policy. This posture seems reasonable given the advanced information systems that are a mainstay of most financial institutions and the need for the systems to meet *inter alia* the interoperability and security standards of financial industry consortia such as INTERAC.[4]

Contractual – Contractual objectives are and will be of ongoing importance to Case B because "the companies with whom we have a business relationship with [sic] change over time." As a result, there is a need to constantly review contracts for compliance. Again, this was not seen to be a "new" activity for the firm. The privacy requirements merely underscored the importance of ongoing activities. For example, when asked about how the activities of a particular group was affected by the implementation of the privacy program, the response was

> We weren't hugely affected. It's the nature of our business, we did that anyway especially when it comes to confidential information. We always visited supplier locations before, so that's no difference.

Interestingly, there appeared to be some differences of opinion over the importance of the contractual objective in the grand scheme of firm operations. I asked several participants whether the scrutiny of third parties would provide an opportunity to reduce the number of suppliers or if a privacy breach would be reason enough for contract termination (both of which were suggested in Case A and by the privacy experts I consulted prior to the field research). While a few interviewees suggested that privacy breaches would be treated seriously ("as per the policy"), I also received replies that seemed to indicate a reluctance to hold firms to the letter of their

[4] INTERAC Association [Canada] is a consortium "[that] link[s] enterprises that have proprietary networks so that they may communicate with each other for the purpose of exchanging electronic financial transactions. INTERAC was founded in 1984 and presently has 110 members that provide Shared Cash Dispensing (SCD) and INTERAC Direct Payment (IDP) Canada's national debit card service. (downloaded from http://www.interac.org/en_n1_00_about.html, accessed October 13, 2004). This firm has been a member of INTERAC through the national trade association since the late 1980's.

"privacy representations and warranties." In one example, the firm had terminated a contract with a supplier that provided statement services. The firm failed to ensure that the statements were sealed and a number of statements were mailed with private information clearly accessible. The staff remarked that while the contract was terminated, this was an example of a "Quality Control issue with privacy implications" and not a privacy failure. Another individual claimed that

> "No, privacy policies won't help to "weed out" suppliers. If their privacy polices aren't up to snuff, then we have to go through the process according to our *outsourcing policy*. Best practices is what drives us and *privacy isn't of practical importance* in these cases. Privacy is important but *wouldn't be a reason for cutting off a supplier*." (My emphasis)

Business – Privacy at Case B is a compliance issue. The business goal, if there is one, appears to be to render privacy a "non-issue" so that the firm can focus on more important issues. As a result, there were very few expressions of privacy as a competitiveness issue, other than to avoid negative comparisons with competitor. As one Branch Manager expressed the situation, "It can turn into a competitive positioning if another FI breaches it, then you use that to your advantage. But right now? Let's face it ... We [all financial institutions]'re all following it [privacy law]."

Social – There was evidence of a social goal for the privacy program. The goal combined the desire to create long lasting (and profitable) customer relationships with building customer trust. Some staff articulated a view that with the proper privacy measures in place, the development of the desired "broad", "deep" and "long term" customer relationships might be achieved. For example, when talking about the desired relationship with the customer, it was expressed:

> If you're looking at somebody's financial wellbeing, you have to have a picture of where they are ... and then the conversation can be taken to the next step as to where do they see themselves ... what's holding them back and what can we do to help get them there, that type of thing. So that's really knowing their lives ... because when you [staff person] look ... there are needs that perhaps the [customer] doesn't even know about."

Later on, the same individual commented that the firm's privacy approach might be helpful in achieving these desired conversations because then their customers might think:

> If it was like, yeah, you know what ... that's the place to do your banking. Because they live their values. They're law abiding. They're a genuinely caring institution.

In addition, there was some consideration that creating a trustworthy environment was important for securing customers. Besides which,

> The important thing is to know the journey [customer's life stage and goals] and how we can help you succeed in the journey with that information [that we collect from the customer]. If you don't tell us then we have no way to know it ... we're just order takers.

Ethical – I found some limited evidence to support the ethical goal for privacy. The Privacy Officer asserted that the Board adopted the Model Code without much discussion because it was the "good and proper thing to do." What is unclear is whether "good and proper" refers to following the law (in which case that would be a legal not an ethical decision) or simply doing the right thing regardless of the existence of a law (an ethical position. The Code of Conduct Policy uses the term "ethical" in a general way. There is no specific reference to privacy as an ethical issue. However, in the IPO Survey section that requested respondents to rank a series of privacy statements ("In my company, privacy of customer information is primarily a _____ issue"), the response "ethical issue" was ranked first or second by 21 (of 33) respondents, second only in importance to "legal compliance issue" (27 of 33 responses).

Decision Rules

There was evidence that the firm had adopted decision rules with respect to how their privacy policy would be operationalized across the bank. There were several discrete examples of which I will present three. First, the firm chose not to purchase 3rd party lists (collection principle). This information source was not pursued for two reasons. One, the lists are notoriously unreliable, therefore, the bank was concerned not to be spending time cleaning up lists or making decision on peer quality information. Two, there was concern expressed about potential member

backlash expressed as "where the hell did they get my name?" This could cause both the alienation of existing customers and the loss of new customers. Besides, "we don't have any third party stuff. We just haven't felt it was worth it at this point to do so ... because we did very little of it in the past."

Second, the firm chose not to data mine transaction information (for example, to establish with which other financial institutions a customer does business) in order to directly solicit business (use principle). When I asked a Branch Manager why not undertake this activity, the reply was a) Marketing would not provide that information because b) the Privacy Officer would say no because c) it would violate that spirit of the legislation (if not the letter) and so branches had to find a "softer" approach, a "work around." The point is that rather than take advantage of their customers by exploiting their technological capability "snoop[ing] the files," the staff were learning to obtain information directly from their customers and asking permission to contact them.

Third, this bank was one of the first to stop issuing account balances over the telephone to other financial institutions (disclosure principle). The concern was for the inability to verify the identity of the caller (was it truly an employee of another bank and one whom is entitled to this information?) A branch manager described how difficult the situation was for the staff to adjust to this new policy,

> At first it was hard just because I think old habits die hard and it was harder because ... we were on the bandwagon it seemed first. So we were getting a lot of flack from the customers and the other FIs... I mean it's a combination [of procedural and attitudinal challenges]. You were so used to ... you pick up the phone and they go, "oh it's the [name] Bank and I want a balance on 1234567" and you're doing it without even [thinking] ... and then you do," I'm really sorry. I can't do that" and I found that hard, too, because I've worked for 17 years like this and all of a sudden you can't, you know, and sometimes you feel bad. They just want to know their cheque is okay and you know damn well the cheque's okay just by the name but you can't say anything.

In summary, I was able to apply the IPO definition to Case B. I found evidence of external and internal privacy principles. I was able to discern several values that appear to guide

corporate decision-making generally. The firm adopted a comprehensive Model Code and associated policies and procedures. Five of six privacy goals are in evidence to greater or lesser extents. (I did not discern sufficient evidence to warrant the inclusion of a business principle.) The bank's overriding concern is to be seen to comply with the law and to minimize the implementation costs and disruption to the operational status quo while achieving satisfactory compliance. Several decision rules have been adopted to prevent practices that the Privacy Officer considers in contravention of the law's spirit or letter. Consistent with my findings in Case A (pilot study) I found that the exercise of applying the IPO Definition using all available data was more useful and provided better insights than simply reading the privacy policy. This again demonstrated the necessity of examining more than privacy statements if we are to learn the "why's" of organizational privacy actions. In the next section, I describe Case B's placement on the IPO Continuum.

Case B's Position on the IPO Continuum

I triangulated data from the IPO Survey, the personal interviews, and firm documents to establish Case B's placement on the IPO Continuum. I applied the IPO Continuum to Case B's circumstances in two steps. First, I analyzed the results of the IPO Survey and plotted the firm's initial placement on the IPO Continuum. Then I triangulated the data for each layer of the continuum. I conclude with a reassessment of Case B's placement on the IPO Continuum. I will address each step in turn.

Survey Results

I used the results from Case B's IPO survey to establish a preliminary placement on the IPO Continuum. Appendix L-6 provides the statistical details. Table 9-3 shows the findings organized as an IPO score. Figure 9-1 shows how I plotted the firm's position on the IPO Continuum based on the survey findings. I discuss the findings layer by layer.

Table 9-3: Case B - IPO Survey Findings

IPO Component	Weighting	Mean of Means	Score for Component	Score for Layer	Interpretation
CRSA	-1	2.3	-2.3	6.3 = **6**	"Positive" relationship with respect to obligations owed to customers. **Shared Responsibility**
CRSB	-0.75	4.3	-3.225		
CRSC	0.75	6.3	4.725		
CRSD	1.25	4.7	6.675		
IMSA	-1	3.5	-3.5	2.865 = **3**	"Negative" use of customer information. **Risk Management**
IMSB	-0.75	4.78	-3.585		
IMSC	0.75	5.1	3.825		
IMSD	1.25	4.9	6.125		
PHILA	-1	1.33	-1.33	4.00 = **4**	"Neutral" privacy philosophy No position
PHILB	-0.75	2.51	-1.8825		
PHILC	0.75	2.95	2.2125		
PHILD	1.25	4	5		
BHVA	-1	1.25	-1.25	4.83 = **5**	"Positive" privacy behaviors **Professional or trade association codes**
BHVB	-0.75	4	-3		
BHVC	0.75	5.69	4.2675		
BHVD	1.25	3.85	4.8125		

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			Case B	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
		Case B		
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case B		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case B	
IPO Score	**1**	**2- 3**	**4** **5- 6**	**7**
	Weaker ⟷			***Stronger***

Figure 9-1: Case B's Initial Placement on the IPO Continuum (Based on IPO Survey Results)

Customer Relationship Stance (CRS)

Recall that CRS was defined as *the organizations' predominant characterization of its relationship to its customers based on the definition of its obligations to its customers.* Overall, Case B scored 5 on the IPO Survey and was placed in the "Shared Responsibility" position. This position suggests that the firm has a stronger, positive view of its obligations to its customers. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

There was no evidence from the IPO Survey to suggest that the respondents consider their bank to be operating with a buyer exploitation customer relationship stance (CRSA). Respondents were neutral about the buyer self protection position (CRSB). This may reflect the contractual nature of many banking relationships, and therefore, the legal requirement for customers to inform themselves.

There was evidence to suggest a consumer well-being position (CRSD). The firm was seen to be obliged to help customers make the best decisions (CRS13) and to be proactively advised about business practices (CRS16). Despite that somewhat weaker support for the two statements (CRS14, CRS15) that would require the firm to "give up" something in order to confer benefit to their customers, interview and documentary data suggest that Case B occasionally operates in a manner that benefits customers even if the activity is not profitable in the short term. For example, one Branch Manager suggested that even though it is expensive (i.e., not profitable) to provide certain levels of services to seniors (i.e., weekly individual service at seniors' lodges, "sit down service" at the branch), "what are you going to do? Like I was saying... the community involvement is the cost of doing business and sometimes you have to eat these things [even though] that's not going to generate any new business for us."

In addition, the bank's privacy policy proscribes certain activities (see IPO Definition – Decision Rules for details). The firm has chosen not to sell customer information or data mine transaction reports because they perceive that these would not be in their customers' best interests. This provides some support for a "customer-well being position" but it is less convincing overall than the evidence for the "Shared Responsibility" position.

Respondents agreed with statements that indicated that firms and customers "exist for mutual benefit" (CRS 10) and that they should work together "to maximize customer benefits and firm profits" (CRS 9). In addition, there was agreement for the need for the two parties to "understand their respective responsibilities within the commercial relationship" (CRS 11). Consistent with this stance of mutual responsibility, respondents agreed that customers "deserved

explanations of our business practices if they requested such explanations" (CRS12).This position on the IPO continuum was strongly supported with interview data. For example, a person in credit services emphasized the need to educate customers about decisions that affect them

> It's hard sometimes to say no ... But to say no with advice as to why we said no and how that's in your best interests and have the customer call back and say, 'You know. I thought that was the best advice I've had' ... writing the reasons behind some of the decisions ... I mean that goes back to establishing a relationship with your customers.

In summary, there is survey, interview and documentary data to support Case B's placement in the "Shared Responsibility" position on the IPO Continuum.

Customer Information Management Strategy (IMS)

Recall that IMS was defined as: *The organization's predominant strategy with respect to its objectives for gathering and using information.* Overall, Case B scored 3 and was placed in the "Manage to Minimize Risks" position. This position suggests that the firm has a weaker, negative view of the potential use of customer information. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

There was consistent disagreement with IPO survey items (IMSA) related to the application of customer information to reduce costs. This position is supported by interview and documentary data. Cost management, while almost an article of faith, was not related to the collection and use of customers' personal information. In addition, there was consistent disagreement with statements to the effect that the firm used customer information to "create new realities" (IMSD). No interview or documentary evidence emerged to contradict this position.

Interestingly, two positions (IMSB: Manage to minimize risks and IMSC: manage with information to add value) were both scored 5 on the 7-point Likert scale. This appears to be consistent with industry norms. Financial institutions, by definition, are concerned to manage risk. Personal information is collected to manage credit risk and mitigate against fraud. These are stated purposes for collection and use of personal information (Privacy Policy). At the same time, Case B needs to collect and manipulate personal information to tailor its market offerings and to

provide personal service. Again, this is a stated purpose in the bank's privacy notice. Data from the interviews and documents support this dual IMS emphasis.

When asked in interviews why the bank collected personal information, responses consistently addressed risk issues, particularly credit related ("We do what's called risk-based lending," "It's for credit adjudication") and personal service/cross selling opportunities ("The more we know about our customers the better we can serve them," "Make the customers feel that the information we gathered ... [would] only be used to recommend or develop products that would meet their needs").

It should be noted that the IMS category generated the greatest number of "no opinion" responses. I believe this is likely due to the circumstance that this bank has not yet implemented an integrated customer information management system, such as a CRM. Many participants were limited in their knowledge of the firm's information management activities and answered "I couldn't say" or "I have no idea" to questions related to IMS. Those with an opinion consistently rated the relative sophistication of this financial institution in relation to its competitors as "less than" in terms of their use of customer information. As was noted, "We haven't got there yet [integrated view of the customer] and I know that a lot of financial institutions are already at that point and are able to segment the data ... and to do all sorts of targeted offers. We will get there eventually."

In summary, while the IPO Survey score placed Case B in the "manage to minimize risks" position, interview and documentary data paint a more complex portrait. Case B appears to pursue a dual customer information management strategy, simultaneously "Managing to minimize risks" and "Managing with customer information for value-add".

Customer Information Privacy Philosophy (PHIL)

Recall that PHIL was defined as *the organization's predominant philosophy about the role and impact that customer information privacy norms and laws have on the firm's ability to carry out its business.* Overall, Case B scored 3 and was placed in the "Privacy as Constraint" position. This position suggests that the firm has a weaker, negative view of the impact of privacy legislation on its ability to carry on business. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

The survey, documents and interview data indicated a consistent awareness that the firm (and industry) were required to operate within the terms of a privacy statute. Therefore, there is no evidence to support the placement in PHILA (no concern or awareness).

However, the category of privacy as a constraint (PHILB) required consideration beyond the survey results. Several participants had expressed the view that there "wasn't much of what I would say is an upside." Some suggested that "following the rules" was "a pain." Yet, for others it was simply a matter of "professionalism."

While there was agreement that the law had necessitated some changes in approach, I did not discern that these changes were uniformly unwelcome or perceived only as a legal necessity. The legal necessity had been turned into a virtue – one of "following our traditions" and "protecting our customers' rights." One senior manager suggested that "we're a pretty compliant bunch" so that once the rules were in place, the emphasis became coping within those rules. As a result, I do not think that this position truly reflects the firm's position on the privacy philosophy layer.

The PHILC category offers "privacy as an exchange". Interview data suggests that Case had not previously considered the exchange implications of privacy but was somewhat open to the suggestion that there was more to privacy than compliance. For example, when asked if having the privacy program in place would help to secure information from customers, several

participants remarked "that's a good question" or "I hadn't thought of that." When considered in the light of the firm's ambitions to move into the more lucrative "financial advice" market space, the ability to reassure customers was seen to be potentially important, as the following exchange illustrates:

> Researcher: How might your privacy approach help you address the gap (between customer impressions and the firm's desired positioning)?
>
> Participant 1: No. I don't think we've taken it that far to say okay ... the privacy legislation ... wow ... this is a way that helps me do this ...
>
> Participant 2: No. [Signaling agreement]
>
> Participant 1: I think we have an understanding that people don't like to be called and you always wonder "how the heck did they get my name?" If you are calling from [your financial institution] it's a little different. It's not so much ... most of the time that people call you it's a cold call. When someone .... is calling you it's not, oh, "I think you want to buy this card ... "
>
> Participant 2: You've already got a relationship
>
> Participant 1: Yeah ... we've developed that relationship and it's what I like to call a warm call. but you're right ... the way I phrased it ... you know, I hadn't thought of consent and privacy legislation but yes, it fits ... it fits perfectly.

As a result, I think that the firm could be positioned as moving towards the "privacy as exchange category" mainly because, when the issue was raised, participants did not automatically reject the notion but appeared open to considering the possibility.

PHILD ("privacy as opportunity") was another position that had not really been considered by participants Interviewees considered any "opportunity" strictly in terms of a potential response in the event of a negative privacy event with a competitor. However, I consider it unlikely to be a position that will be pursued by this firm.

In summary, the interview and documentary data support a slightly more positive position the PHIL layer than what was suggested by the IPO survey. "Privacy as a constraint" (the survey positioning) overstates a negative position. A neutral position appears justified.

Customer Information Privacy Behaviours (BHV)

Recall that BHV was defined as *the organization's publicly visible and internal information privacy activities*. Overall, Case B scored 5 and was placed in the "Professional or Trade Group Codes" position. This position suggests that the firm has a stronger, positive view of its privacy behaviors. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

The IPO Survey showed that there was consistent disagreement with BHVA statements that indicated that the firm was non-compliant. Documents and interviews clearly demonstrate that Case B is compliant with PIPEDA. Therefore, there is no reason to place the firm in this position on the continuum.

There was a neutral response to BHVB statements that suggested that the bank was minimally compliant. Documents indicate that the firm has implemented enterprise wide policies that do more than restate the privacy principles outlined in PIPEDA. Interviewees consistently suggested that the firm had done extensive work on privacy and ought not to be characterized as merely minimalist. As a result, I believe that BHVB is not a true representation of Case B's actual position on the IPO Continuum.

The BHVC category (Professional or Trade Group Codes) was the strongest category in the IPO survey results. This position was supported by documentary and interview evidence. The firm adopted, with minor modifications, the Model Code drafted by their national trade association. This Model Code operationalizes the 10 principles contained in PIPEDA beyond simple compliance. When queried, participants perceived, with very few exceptions, that their firm's privacy approach was better than many of their smaller peers' programs ("We get lots of calls about our privacy policy"), or at least as good as their larger peers' and competitors (the nationally chartered banks).

Just as clearly, the firm does not consider itself (and has no aspirations to be) a privacy leader. Responses to the survey category BHVD (enhanced privacy) were, at most, neutral. There was disagreement with statement BHV13 ("Our firm has implemented a privacy policy that is regarded by others as leading in our industry") and only modest support for statements indicating that the firm "goes out of its way" to provide customers with privacy protections beyond that which is offered by competitors (BHV15). There was somewhat stronger support for statements that indicated "we give priority to privacy considerations when developing business initiatives" (BHV14) and "we provide the best privacy practices we have been able to find in our industry" (BHV16). These positions are consistent with documentary and interview data.

It was clearly articulated to me by senior members of the firm that privacy was "more an issue of understanding the rules and applying them." To the extent that they perceive themselves to be a leader among their peers in terms of "best practices," then the firm was prepared to be viewed as a leader in general but not specifically in privacy terms. In relation to their competitors, the firm was not going to be using privacy as a competitive posture other than to shore up any misunderstanding about their service being "second class." The ultimate goal is for privacy to be rendered a "non-issue" and that cannot be accomplished if a firm is attempting to do anything noticeably different in the marketplace. As a result, there were no plans to embark on any privacy initiative beyond what had been accomplished as "the [privacy] project is implemented." In other words, an ongoing privacy activity is strictly for the purposes of maintaining compliance and not seeking competitive advantage. The Privacy Officer explained the firm's privacy aspirations in the following manner:

> Is it [privacy program] perfect? No. But, we're being seen to be trying to do the right thing. We're neither 100% nor are we 20% [in compliance] but the regulator can't accuse us of flaunting the legislation or not doing the best for our customers..."

"Enhanced Privacy" is not a desired position because it appears to represent a level of effort that exceeds any perceived benefits.

In summary, Case B was positioned in the "Professional and Trade Group Code" category on the IPO Continuum. This position is supported by the interview and documentary data.

Repositioning Case B on the IPO Continuum

The initial positioning on the IPO Continuum for Case B was modified after triangulating the results with interview and documentary data. Two positions were confirmed – the Shared Responsibility position on the Customer Relationship Stance layer and the Professional and Trade Groups Codes on the Customer Information Privacy Behaviour layer. Case B appears to occupy two positions on the Customer Information Management Strategy layer – "Manage to Minimize Risks" and "Manage with Customer Information to Add Value." This positioning may reflect the particularities of the financial institutions industry. Case B's Customer Information Privacy Philosophy was originally positioned as "privacy as constraint." However, interview data suggests that there is movement towards the privacy as exchange position, thereby warranting placing the firm in a "neutral" position on this layer. It is unlikely to consider pursuing an "opportunity" positioning. Finally, Case B is solidly located in the "Professional and Trade Group Code" position of the Behaviours layer and does not aspire to becoming a privacy leader. Figure 9-2 shows the redrawn IPO Continuum for Case B.

Theoretical Assessment

In this section, I review Case B's information privacy orientation first using the Institutional Approach and then the Resource-Based View.

Institutional Approach

Case B's information privacy orientation can best be explained using the lens of the Institutional Approach. I briefly apply the attributes of the institutional paradigm (more fully

described in Chapter Five) to demonstrate how this theory explains Case B's approach to their privacy program.

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			Case B	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
			Case B	
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case B	**Case B**	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case B	
	Weaker ◄——————————►			***Stronger***

Figure 9-2: Case B's Final Placement on the IPO Continuum (Based on Triangulated Results)

Organizational goal: Case B's approach to information privacy is to strictly comply with legal requirements. This bank does not appear interested in making changes to their operations other than those dictated by the "rules" (managerial legitimacy) to bring them into compliance with PIPEDA (pragmatic legitimacy). The search for legitimacy is largely expressed as a desire to not be perceived by external audiences as being "offside" in comparison with their competitors, although there is some willingness to forgo certain activities for fear of customer reprisal. As indicated in previous sections, the concern is to "make privacy a non-issue" by adopting the trade

association's model code to satisfy legal and customer expectations. In sum, Case B's organization goal is primarily to seek pragmatic and managerial legitimacy through their privacy program.

Source of Pressure: Case B implemented their privacy program strictly as a response to the PIPEDA requirements (cause). Furthermore, there was very limited internal organizational demand or customer demand for this action (constituency). Privacy norms are as represented by the ten PIPEDA principles which, to some extent, mirror the bank's prevailing norms for the treatment of confidential information (content). The privacy program had been "legally coerced" to the extent that the bank would not likely have adopted a formal, enterprise-wide program if there had not been the law. However, the bank implemented their program at least one year before it was necessary, thus demonstrating some volition with respect to their privacy program (control). Furthermore, the bank recognizes that it is part of the larger financial institutions industry. As such, Case B needs to be able to operate within the industry (interoperability standards) as well as withstand scrutiny from peer organizations (context.) Case C's privacy motivation is best summed up by the phrase "We obey the law." Note that Case B is member of the same national trade association as Case C.

Ability and Willingness to Respond to Pressure: Case B responded to the pressure to implement their privacy program by, on one hand meeting their legal obligations while, on the other, minimizing resource consequences. They operate their privacy function with part time positions and no dedicated budget. The bank is very firmly embedded in a network of similarly sized financial institutions and adopted their trade association's privacy model with few changes. This approach reflects the Chief Privacy Officer's view of privacy as largely a compliance issue.

Response to Pressure: Case B's response to the pressure to implement a privacy program can be characterised as a case of mimetic isomorphism. They attempt to reduce the likelihood of negative responses by providing sufficient information to demonstrate compliance with the law. As well, they rely on a Model Code and have not undertaken an independent search for

alternatives. These attributes combine to strongly argue that Case B's information privacy orientation is based on an "acquiescent" institutional strategy.

In summary, Case B's information privacy orientation can be analyzed and explained using the Institutional Approach. The bank appears to be pursuing an acquiescence strategy.

Resource-Based View

Recall that I theorized in Chapter Five that the Resource-Based View would offer a lens through which to consider IPO heterogeneity. That is, I offered two resource-based interpretations for firms that appeared to be interested in pursuing privacy as a source of sustainable competitive advantage either through a knowledge or relationship based capability.

Case B does not appear to be pursuing a resource based privacy strategy. First, they do not want to differentiate themselves on the basis of privacy. In fact, their goal is the opposite – to make privacy a non-issue. Second, their concern to render "privacy a non-issue" means that they are more concerned with minimizing perceived privacy "downsides" (e.g., trying to avoid privacy problems) rather than attempting to operate with a privacy forward strategy. As a result, Case B has pursued an approach to privacy that is quite indistinguishable from their peer group (as explored with the Institutional lens).

In sum, the RBV offers limited insight into Case B's information privacy orientation.

Chapter Summary

In this chapter, I provided the results of the Case B study. Using a triangulation approach (based on interview, survey and documentary data), I applied the IPO Definition and defined the layers of the IPO Continuum. Then I mapped Case B onto the IPO Continuum. Finally, I considered Case B's information privacy orientation through the competing theoretical lenses and suggested that their IPO is best explained using the institutional approach.

CHAPTER TEN

CASE C

In this Chapter, I describe the results of the second field case study, Case C. This research site was one of the desired sites that I identified in the Privacy Policy Evaluation Study. Briefly, I conducted a four day research site visit at Case C's head office in July 2004. I interviewed 20 executives, managers and staff about how the company had gone about organizing and implementing their customer information privacy program. I also collected 76 documents related to privacy. I was unable to distribute the IPO Survey at this case site.

This study was undertaken to contribute to answering the first two research questions:

R(1) Do firms have an Information Privacy Orientation?

R(2) Is Information Privacy Orientation constructed as I have theorized?

This chapter provides evidence to support an affirmative response to these questions. To demonstrate this support, I assess Case C's information privacy orientation based on the interview and documentary data I collected. While I would have preferred to be able to triangulate data with the IPO survey, I believe that I was able to build a fairly comprehensive privacy portrait of Case C sufficient to address the two research questions. In this chapter, I assess the firm's privacy policy for comprehensiveness, readability and accessibility. Then I review the firm's privacy program against the IPO Definition including principles (external and internal), values, policies (governance, resources, evaluations), objectives and decision rules. Third, I examine the layer by layer (customer relationship stance, information management strategy, privacy philosophy, and privacy behaviours) evidence to support positioning Case C on the IPO Continuum. Note that Appendix M contains a collection of information from Case C's case study database, including interview and document lists. To set the stage for understanding the IPO analysis, I provide a brief background to the development and implementation of Case C's privacy program.

Case C Privacy Program Status: "We're compliant – now what?"

With PIPEDA's proclamation in 2001, Case C pondered how to respond. A subsidiary of the company was mandated to comply January 2001 and had managed to "do what was necessary." The concern for Case C's retail banking management was really the "optics" issue – what would their customers think if one part of the operation claimed to have a "better" privacy approach than another? Furthermore, competitors who would not be considered as "progressive" or "customer-oriented" (as Case C saw themselves) had declared their compliance by the January 2001 deadline. Neither of these scenarios suited the intensely image and reputation conscious Case C. It was decided that Case C's retail network would become compliant by 2003 – at one level behind the chartered banks (compliant in 2001) but ahead of other regional players who were leaving compliance to the 2004 deadline.

Initial Privacy Program Implementation

Case C undertook PIPEDA compliance as a dedicated project under the direction of the Project Management Office within the Marketing and Strategic Planning Division. They did not piggyback their PIPEDA compliance with the Anti-Money Laundering initiative (as did Case B). Case C's privacy implementation project was conducted in three phases during the period of January 2001 to December 2002 as shown in Table 10-1.

There are two particularly interesting aspects of Case C's approach that warrant comment. First, the project team distinguished between Privacy "Service" (Front Office Representation) and Privacy "Administration" (Back Office Representation) activities. While both teams were "charged with developing the policies and procedures to achieve compliance to the 10 key principles of proper management of personal information" the distinction between sales and administration suggests that the project managers viewed their mission in terms of how to manage interrelated but separate processes. The "Sales" team was focused on "scripting." They concerned themselves with "Addressing the main process points where staff has an opportunity to

Table 10-1: Case C - PIPEDA Project Phases

Phase	Timing	Target for completion	Activities
1	2001	Dec.2001	• Conduct Information Audit o Data mapping o Personal information management processes across enterprise • Undertake Gap Analysis o Assess present compliance against 10 PIPEDA principles • Develop Implementation Plan
2	2002	Aug. 2002	• Create and obtain approval for o Project Charter o Detailed Workplan and Budget • Recruit and establish Core Privacy Team o Privacy "Sales" team o Privacy "Administration" team • Review and identify need to change/replace/eliminate o Processes o Forms • Devise/prepare o Staff training program o Customer communication program o Privacy roles and responsibilities
3	2002	Dec. 2002	• Undertake file culling and physical security improvements (branches and head office) • Implement compliance "enablers" o Policies and procedures (including records management) o Processes (such as account initiation) o Forms redesign (content, disclosure, etc,) o Privacy training for new hires o Clearly defined roles & responsibilities (especially Privacy specific positions) • Conduct mandatory staff training sessions • Implement customer communications program
		Jan. 1, 2003	**➔ PIPEDA compliance**

make an introduction regarding the customer/potential customer's privacy rights." Of particular importance was the "privacy conversation" (my term) "on the purpose and obtaining consent for collecting the information and how it will be used." I interpret this to mean that Case C viewed PIPEDA compliance as having a direct bearing on the relationship with their customers and that this necessitated considerations for how to "manage the privacy conversation" with customers – both to assure/reassure them and to create the circumstances for their willing cooperation in the form of consent. In contrast, the "Administration" team focused on the mechanics of compliance.

They addressed the enterprise wide issues of "the collecting, retaining, safeguarding and destruction of the personal information [held by the bank]."

The second interesting feature of Case C's approach was the distinction they drew between the PIPEDA principles they deemed required "mandatory compliance" (no room to maneuver) and those that required "acceptable compliance" (Act provides for tailoring to organizational needs). These distinctions appear in Table 10-2.

Case C's conclusions that PIPEDA was a "floor not a ceiling" (my phrase) underscores their commitment to researching the alternatives and then designing a program that met their particular circumstances. It is interesting to note that even with this approach, Case C developed an apparently "strong" privacy model (as will be demonstrated later in this chapter) for the simple reason that they determined that this was the approach best suited to their needs. The important point is that it was Case C that made this determination through their consideration of alternatives and not the law by its mere existence. PIPEDA compliance for Case C was not simply about applying the rules (as had Case B) but of choosing how to comply in alignment with other corporate considerations. In other words, Case C demonstrates that firms have choices within the framework of PIPEDA if they choose to identify and exercise them.

Next Steps

Case C did not slow their privacy activities with the achievement of PIPEDA "compliance." While the immediate privacy project may have ended, the bank embarked on two new initiatives. First, was a series of evaluation activities which were initiated for "external validation" purposes. Second was a governance review in response to an internal audit.

Table 10-2: Case C - Classification of Compliance Distinctions of PIPEDA Principles

	PIPEDA Principle	Case C characterization of essence of principle and example	Case C Classification of principle:	
			Mandatory Compliance	**Acceptable Compliance**
1.	Accountability	*Organization is accountable for the information under its control*	✓	
		Organization shall designate accountable individual for compliance		
2.	Identifying purposes	*The purposes for which personal information is collected will have to be identified by organization at or before time of collection*	✓	
3.	Consent	*Knowledge and consent of individual will be required for the collection, use or disclosure of personal information, expect where this is inappropriate*	✓	
4.	Limiting Collection	**Collection is limited to that which is necessary for the purposes identified by the organization.**		✓
		Information would be required to be collected by fair and lawful means.		
5.	Limiting Use, Disclosure, and Retention	**Use of information is allowed as long as purpose is disclosed and consented to by customer.**		✓
		Information shall be retained only for as long as it is needed to fulfill the stated purposes.		
6.	Accuracy	**Information has to be as accurate, complete and up-to-date as is necessary for the purposes for which it was collected**		✓
7.	Safeguards	**Security safeguards are required appropriate to the sensitivity of the information.**		✓
8.	Openness	*Organization is required to make specific information about its polices and practices readily available to individuals*	✓	
9.	Individual Access	*Upon request, an individual has to be informed of what information is held about him/her and be given access to the information.*	✓	
		Individual has right to challenge accuracy and completeness of information held about him/her.		
10.	Challenging Compliance	*Individual has right to challenge policies and procedures*	✓	

Evaluations: Three particular evaluation exercises were undertaken in 2003. A "mystery shopper" exercise was carried out in 12 branches coinciding with "official compliance" in January 2003. This exercise was conducted to assess the extent to which the customer service staff had learned how to deal with the "privacy conversation" at the service counter. The evaluation demonstrated an adequate level of knowledge about and enthusiasm for addressing customers' privacy concerns among branch level staff. The Internal Audit department conducted a corporate privacy audit (six months prior to what had been scheduled). The audit examined practices within the Privacy Office as well as privacy compliance within Marketing, Facilities, Human Resources and Wealth Management. The audit showed that the bank had a gap between concept and execution - the "overall design of controls is satisfactory" but the "operations of the controls need improvement." A plan to address the issues identified in the audit was developed and implementation of its recommendations continues. In 2004, the bank completed a bench mark privacy practices survey. This survey, carried out by the Ponemon Institute on behalf of the International Association of Privacy Professionals, asks firms to assess themselves on a series of privacy practices. While I do not know the outcome of this evaluation, the bank's participation indicates a willingness to compare its practices and change them, where warranted. The firm is also considering the costs (likely about $300,000) and the benefits (still be identified) of having an external audit conducted by a large assurance audit firm (such as Deloitte or PriceWaterhouseCooper). There is also some discussion about the merits of enrolling in a "privacy seal" program but no action has been taken to date. At Case C, privacy is an ongoing concern.

Governance Review: A consequence of these evaluation exercises was the identification of the need for a more comprehensive governance framework for managing privacy at Case C. The internal audit report had identified a "lack of comprehensive privacy compliance role descriptions to articulate the responsibilities and authority limits of the Privacy Office. " This observation, flagged as a risk to achieving "compliance effectiveness" sparked a broader policy

debate about what should be the corporate privacy office's mandate, how it should be structured, and what should be the scope of its monitoring role across the Bank and its subsidiaries.

The importance of the governance review, from my perspective, is that it demonstrates that Case C is operating at a different stage than Case B. The short term initial compliance objectives may have been achieved, but now Case C is concerned to tackle the longer term objectives for its privacy program. These include:

1. Articulating how privacy fits into the larger governance framework for the bank.
2. Articulating a specific governance structure to manage privacy consistently across the bank and its subsidiaries.
3. Defining the relationship between its privacy activities and the strategic objectives articulated in the five year plan.
4. Closely aligning its privacy practices with its CRM strategy.
5. Monitoring the relationship between its privacy practices and customer trust and loyalty.
6. Maintaining a watch on developments in other jurisdictions that could affect the bank's operations, such as the U.S. Patriot Act.

These are large issues which will require the attention of the bank's senior executive group and its Board. So far, both groups appear willing to make the investment. It is interesting to me that Case C is undertaking more privacy activity when others, such as Case B, have downplayed the privacy as an ongoing function. The difference in attitude can be summed up in the Privacy Specialist's response to my query about why the bank was interested in participating in my research, "Well, we're compliant. So, what's next?"

In summary, Case C represents a bank that has taken a different approach to implementing their privacy program. I have shown that these differences appear to stem from a perspective that privacy is not merely a short term compliance task but a long term process with significant organizational ramifications.

In the next section, I assess Case C's privacy policy.

Assessing Case C's Privacy Policy

I assessed Case C's privacy policy on the basis of comprehensiveness, readability and accessibility. Table 10-3 summarizes the findings. I assessed the information that is publicly available on the online banking site connected to the privacy link. The overall score generated for the Privacy Code is 12, which would place this firm's privacy approach in 1st place within the rankings of the ten firms examined in the Privacy Policy Evaluation Study (Chapter Seven).

Comprehensiveness – Case C scored 7 for comprehensiveness. The Privacy Code refers to and provides specific information about each of the ten privacy principles contained within the Privacy Code adopted by the firm. These principles directly parallel those articulated in PIPEDA. Key aspects of the policy are easily identifiable through headings and subheadings. The Privacy Officer is identified as the position with "overall responsibility for the protection of personal information, and compliance with this Code" (Section 1: Accountability) and is identified as the contact for complaints and enquiries (Section 10: Compliance and Complaints). Contact information is provided ("Still have questions?").

Readability – Case C scored 3 for readability. This firm's Privacy Code is written at a level that places it in the "hardest" category (Flesch Reading Ease <30). However, this is balanced somewhat by a moderately easier to read FAQ section (Flesch Reading Ease >30). The Code largely uses active voice and is written in what I call "Plain English Legalese." There is a high level of detail and examples. The bank provides good information to help customers understand the privacy policy including FAQs, abbreviations, and examples. Particular attention is given to security and consent issues. A consent form is available through the firm's website.

Table 10-3 Case C - Privacy Notice Basic Assessment

Criterion	Key Questions/Concerns	Case C Results
Policy Comprehensiveness SCORE = 7	• Are all PIPEDA/fair information elements addressed?	• Yes. • PIPEDA (sic) specified • CSA Model Code referenced • PIPEDA principles covered thoroughly
	• Is there a summary of the policy that emphasizes key features?	• Yes. • Privacy Statement describes policy basics including opt-out. • FAQ section offers 11 basic questions and answers about privacy and security.
	• Is responsibility clearly identified?	• Several references to Privacy Officer but not identified by name; contact information provided • Refers to Privacy Representative at each branch for questions, concerns. • Customers are directed to discuss questions with Customer Contact Centre or to contact the Privacy Officer at the Head Office. • Also directed to seek information through online banking website. • Contact information is provided for customer contact centre.
Policy Readability SCORE = 3	• What is the readability score for the privacy policy document(s)? • Is the policy written in accessible language (or in "legalese")?	• Privacy Code: o Flesch Reading Ease = 19.2 ("hardest" category) o Flesch-Kincaid Grade Level = 12 o Written in Plain English legalese • Privacy FAQ o Flesch Reading Ease = 35.6 ("harder" category) o Flesch-Kincaid Grade Level = 12
	• Are key terms explained?	• Yes. • Consent, Disclosure, Use, Personal Information, Third Party.
	• Are examples provided? Are the examples thorough and understandable?	• Many examples provided.
	• Are consent forms provided?	• Yes – through website banking.
Policy Accessibility SCORE = 2	• How easy is it to find the policy? Are there multiple access points?	• Two links from home page • Links from subsequent pages
	• Are there links to other privacy information (external)?	• NO. • Reference to customer ability to contact Privacy Commissioner (unspecified) throughout process. No additional information.
	• Is there a webseal or other "seal of approval"?	• NO.

Accessibility – Case C scored 2 for accessibility. The bank's Privacy Code can be obtained online, from a branch or by contacting the Customer Contact Centre. On the website, it is linked from two points on the homepage as well as from subsequent pages.
There are no external or internal links to additional privacy information. However, reference is made to an unspecified "Privacy Commissioner" but no contact information is provided. There is no privacy webseal.

Summary - Overall, this firm provides excellent privacy policy information to existing and potential customers alike. The policy is demonstrably compliant with PIPEDA and this information is comprehensively conveyed to readers. The score generated for this assessment exercise is 12 which, when compared to the firms in Study One, represents the top position (1st rank) among the range of assessment scores that were generated in the initial evaluation of privacy policies (see Chapter Seven).

Applying the IPO Definition to Case C

I applied the IPO definition by coding the interviews and the privacy documents I was able to obtain. The coding was reviewed and approved by my supervisor. In both instances, I looked for information, quotes and examples of the different aspects of the IPO definition – principles (external and internal, values, policies, objectives and decision rules). Table 10-4 summarizes Case C with respect to the application of the IPO Definition.

Principles

External: There is reference to PIPEDA as the legal statute to which the firm must comply. External Principles, specifically the 10 privacy principles, appear in several public documents, including the Privacy Code, Compliance Summary, and Privacy Governance Framework. The majority of interviewees also referred to the statue as the source for the bank's

Table 10-4: Case C - IPO Definition

IPO Definition Component	Findings: Case C
Principles (external)	• Company Code based on CSA Model Code (Can/CSA-Q830-96) and PIPEDA (10 principles).

Principles (internal)	• The firm's privacy principles are adapted from the CSA and PIPEDA principles – "we have tailored our own ten privacy principles to meet these specific needs and expectations of our customers."
	• Operating principles
	  • Right to be left alone
	  • "How would you feel if?"
	  • Tradition of confidentiality.

Values	• "Our business is, and always will be, guided by the simple and enduring principle of doing what's right."
	• Corporate values include:
	  • Integrity
	  • Innovation
	  • Responsibility
	• Privacy as part of responsibility to provide transparency and accountability in business practices.
	• "Customers have a right to feel secure in the knowledge that the information they provide about themselves will always be used appropriately."

Policies	
Governance	• Initial response to address basic consent issues. Implemented for Jan.1, 2001 compliance deadline. • Comprehensive policy adopted by Board of Directors. Somewhat similar to national Model Code adopted by other firms. Code (adopted 2002). • CPO Responsibility – assigned to Vice President, Business Development (within Marketing and Strategic Planning Division) • Reports on privacy compliance matters to Executive Committee Board of Directors (relevant committee under assessment) • Presently refining Privacy Governance Framework which proposes a Corporate Privacy Council (cross functional, senior level)
Resources (domestic retail banking only)	• Part of formal responsibility of two staff – part time with VP (who functions as CPO); full time Privacy Specialist (day to day responsibility) • Access to legal counsel on retainer • Dedicated budget. • Within each branch – privacy champion has received special training; privacy pamphlet directs customers to branch. • Customer Contact Centre as point of contact for complaints and inquiries.
Reviews & evaluation	• Comprehensive privacy audit and gap analysis conducted internally prior to policy development and implementation. • "Mystery Shopper" study in 12 branches (January 2003). • Internal audit examined practices within Privacy Office as well as privacy compliance within Marketing, Facilities, Human Resources and Wealth Management (2003) • Participated in international "Best Practices" study. • Third party external audit under consideration for 2005.
Objectives	
Legal	• Primary objective is legal compliance, from the perspective of using "[information collection] methods that are lawful." • Particular emphasis on obtaining consent.

Technical	• "Changes in technology necessitate that [the company] continually develops, updates and reviews information protection guidelines and controls to ensure ongoing information security."
Contractual	• Working to ensure 3rd party compliance with vendors, suppliers and affiliates. • Monitoring trans-border issues (i.e., U.S. Patriot Act and affect on compliance with PIPEDA).
Business	• Improved efficiencies and better business practices resulting from the analysis of flows of personal information through the various business units. • Concern for maintaining strong reputation as a progressive financial institution. Privacy actions are seen as contributing positively to reputation. • Privacy needs to be incorporated into CRM strategy. • Aspires to "leadership in sound privacy practices."
Social	• Privacy as a way to build customer trust – "We will do all we can to keep that trust and maintain your confidence that we will keep your personal information between you and us." • Some evidence to support privacy as a means to support broader, deeper and longer term customer relationships – The better we know you, the more able we are to provide the best products and services to meet your financial needs."
Ethical	• After legal compliance, most important objective. • Use of term ethical in privacy policy "ensuring the accuracy, confidentiality, and security" of personal information is "an ethical obligation" • Baseline Ethical Policy includes a statement of Business Practices "We believe that the highest standards of business ethics are a key ingredient in financial success" • Statement of Values and Commitments indicates that "outstanding service and help [to] your financial goals includes "protect your right to privacy" • Privacy included as a "Social Audit" objective
Decision rules	• Evidence of deliberate choices made in how privacy is operationalized. o Does not sell customer information. o Does not purchase customer lists. o Does not issue account balances over the telephone to other financial institutions.

policies. The Privacy Code document expressly identifies the CSA Model Code and PIPEDA as the basis for privacy action by the firm.

Internal: Case C adapted the external (PIPEDA) principles as their own internal privacy principles. These principles were "tailored ... to meet [the] specific needs and expectations of our customers." The principles are referred to in internal documents such the Privacy Project Charter, Compliance Summary, and Privacy Governance Framework as well as various privacy compliance policy and procedures documents. Similar to the other case sites, "confidentiality" of customer information is a fundamental principles. In many ways, confidentiality is used as shorthand term for privacy. As well, the salient operating principle for privacy, particularly at the

branch customer service level, is the litmus test of "how would I feel if ...?" Participants indicated that a combination of "privacy as right to be left alone" (articulated in training), the "how would I feel test" and traditions of confidentiality combine to provide a strong set of internal principles supportive of the bank's privacy objectives.

Values

Privacy features prominently as a value at Case C. The "Statement of Values and Commitments" specifically promises that the bank will "protect your right to privacy" as part of the effort to offer customers "outstanding service and [to] help you achieve your financial goals." In addition, several interviewees indicated that the bank's approach to privacy supported the "Baseline Ethical Policy" that calls for ethical business practices such as "transparency and accountability." Part of the rationale for the approach taken by the bank was to "aggressively implement privacy policies and procedures ... core to [our] commitment to both internal and external stakeholders." The bank is very involved with the "progressive" governance movement and conducts comprehensive social audits. Privacy is viewed as part of a social commitment and a fundamental expression of the firm's values.

Policies

I consider the policies of Case C under three headings – governance, resources and evaluations.

Governance: The Chief Privacy Officer (CPO) role is occupied by a Vice President (Business Development) that is located in the Marketing and Strategic Planning Department. As a result, this is a part time position. The privacy staff are responsible for developing privacy policies and initiatives and, to this point, "driving the processes." Internal audit has supported the initiatives through ongoing monitoring and providing a special internal audit (see "Evaluations" below). As well, a senior Privacy Council is being considered as a communication and coordination for privacy initiatives. The CPO reports quarterly on privacy compliance matters to

Executive Committee Board of Directors. Currently, a governance renewal exercise is underway with the possible consolidation of privacy oversight responsibilities for Case C and its subsidiaries under one CPO. The issue of which Board committee is most relevant to exercise oversight is part if this discussion. As well, privacy is being included in the company's five year plan with direct linkages being established between privacy initiatives and the bank's six strategic areas.

Resources: The Chief Privacy Officer is supported on a day-to-day basis by a full time Privacy Specialist, who occupies a mid-level staff position. The Privacy Specialist has access to external legal counsel and other "for hire" resources. These items are included in a substantial annual dedicated privacy budget. Each branch has a "privacy champion," typically an Assistant Manager, who has received additional training and is responsible for handling privacy enquiries. Most branch staff received specific privacy training sufficient to be able to respond to basic customer questions and explain privacy sections of basic forms. In addition, the staff at the Customer Contact Centre field complaints and enquiries that have not been directed to branch level personnel.

Evaluations: In keeping with the bank's determination to be perceived as a leader in its market area, Case C undertook several evaluations to ensure that it is "getting privacy right." An initial comprehensive internal privacy assessment was conducted through a privacy team mechanism. Later, the bank undertook a "mystery shopping" study in 12 branches (timed to coincide with "official implementation" in January 2003). An internal audit of the privacy office as well as the privacy operations within Marketing, Facilities, Human Resources and Wealth Management was conducted in 2003. This report revealed a number of areas for improvement, especially in governance, records retention and destruction, and training. The bank also participated in an external study of privacy practices undertaken by the Ponemon Institute in cooperation with the International Association of Privacy Professionals (IAPP). The company also includes privacy within its Social Audit report. Finally, the bank is considering whether to

engage an external firm to conduct a "privacy audit" (target date 2005) that could be used to signal the bank's privacy performance to customers and other stakeholders. The Privacy Specialist commented that it was important to the bank to "have external confirmation that we've done all we can, all that's reasonable."

Objectives

I was able to gather evidence in support of all six objectives. While I identified that the overriding objective is to achieve compliance, I discerned that there were secondary objectives as well, primarily ethical and business objectives. All goals appear to be mutually reinforcing. The following quote demonstrates the interweaving of objectives at Case C (from a memo to the Privacy Team from the Project Sponsor who eventually assumed the role of Chief Privacy Officer,

> Our goal with this project is to abide by the legislation outlined by the federal government. But, in doing that there are side benefits. We have the opportunity to enhance customer trust in [BANK], and raise awareness among staff of protecting personal information, both with customers' and staff's personal accounts. And by refining how we collect and use information, we can ensure what we do collect is more relevant to helping meet our customers' needs while reducing the risk of mismanagement.

Legal – The primary reason for Case C to develop and implement its privacy program was to comply with the federal law ("abide by the legislation") as well as to be in position to declare compliance with the anticipated provincial law (Personal Information Protection Act).

Technical – There was evidence of information security as an important privacy program objective but within the overall framework of their privacy policy, not as a separate objective. The Privacy Code (and PIPEDA) refers to "safeguards." Safeguards include physical, logical, technical and organizational measures to "protect personal information from loss or theft, unauthorized access, use copying, modification, disclosure or disposal." Branch discussions centered mostly on physical safeguards while head office discussions more often focused on information security. The emphasis appears to be in crating a information security policy to exist

within the privacy governance framework. Technical or security provisions were also seen to be something that "we do anyway" and that were highlighted by but not created as a result of the statute or the firm's policy ("all our information is secure anyway"). At the same time, the bank has provided considerable information about security for its customers, especially on the website. The overall security posture seems reasonable given the advanced information systems that are a mainstay of most financial institutions and the need for the systems to meet *inter alia* the interoperability and security standards of financial industry consortia such as INTERAC.[1]

Contractual – Contractual objectives are and will be of ongoing importance to Case C. The internal audit revealed the need for the firm to be more proactive in dealing with third parties. Interestingly, the bank's public posture is to deal with businesses that exercise high degrees of transparency and accountability in their operations but the internal audit suggests that there may be room for improvement in using privacy as a specific litmus test. For example, I could not find evidence that suggested that Case C would terminate relations with suppliers over privacy issues. However, neither could I find that this was not an area of concern. Rather, evidence such as the Internal Audit Report indicates that the firm is attempting to strengthen its actions in this area.

Business – Privacy at Case C is more than a compliance issue – it is a business issue with enterprise wide ramifications and multiple goals ("ensure what we do collect is more relevant to helping meet our customers' needs while reducing the risk of mismanagement.") The CPO expressed the overarching goal of "tying privacy directly to the business." The bank's five year plan contemplates how privacy can be used to "deliver on our business objectives" by specifically addressing the link between privacy and its six strategic areas. The ambition is to "move from privacy in the regular course of business to a strategic initiative." In this way, the firm can be seen

[1] INTERAC Association [Canada] is a consortium "[that] link[s] enterprises that have proprietary networks so that they may communicate with each other for the purpose of exchanging electronic financial transactions. INTERAC was founded in 1984 and presently has 120 members that provide Shared Cash Dispensing (SCD) and INTERAC Direct Payment (IDP) Canada's national debit card service. (downloaded from http://www.interac.org/en_n1_00_about.html, accessed October 13, 2004). This firm has been a member of INTERAC through the national trade association since the late 1980's.

to be working towards being seen to operate with "leadership in sound privacy practices" which, it is hoped, will help to solidify the firm's reputation within its market.

The immediate emphasis is more internal. The exercises in data mapping and inventorying information assets conducted in the early stages of the privacy project is leading to "improved efficiencies and better business practices" resulting from the analysis of flows of personal information through the various business units. However, to achieve the real business objectives of "deepening relationships for greater share of wallet" will require the incorporation of privacy into a renewed CRM strategy.

Social – There was evidence of a strong social goal for the privacy program ("enhance customer trust"). The goal combines the desire to create long lasting (and profitable) customer relationships with building customer trust. While the bank's privacy initiatives were initially focused on the legislation, the real issue simply "boils down to a matter of trust." The privacy pamphlet provided to customers acknowledges that when they became customers,

> you trusted us with your personal information. We will do all we can to keep that trust and maintain your confidence that we will keep your personal information between you and us.

This sentiment was repeated throughout my interviews, most strikingly with branch level personnel who very much see their relationships with customers in terms of trust as part of their customer service approach.

Ethical – The ethical goal is in strong evidence in Case C. The firm's Privacy Statement (a distillation of and introduction to their privacy policy) indicates that "privacy is more than simply a legal requirement, it is an ethical obligation." Case C's tradition is to have a strong ethical bias in its operations. Privacy has been incorporated as "table stakes" both in terms of industry activity ("it's not a choice anymore") but also in terms of the firm's identity, it's perception of itself (we'll be seen to "be operating with integrity").

Decision Rules

There was evidence that Case C had adopted decision rules with respect to how their privacy policy would be operationalized across the bank. These rules are consistent with those for Case B – not selling customer information; not purchasing customer lists; and not issuing account balances over the telephone to others purporting to be from financial institutions. In addition, Case C was evolving additional practices, primarily aimed at head office functions to ensure that these rules were being respected. For example, a procedure was implemented in the Marketing department to ensure that information being prepared for disclosure to a third party for processing (such as a "data mining" exercise) was assessed for privacy implications. Of specific concern was the need to assess, classify and document the sensitivity of the data (such as income information) and convey this to the receiving party. The website manager indicated that privacy "provides an additional lens" for the developers when designing, for example, web-based contests.

In summary, I was able to apply the IPO definition to Case C. I found evidence of external and internal privacy principles. I was able to discern several values that appear to guide corporate and privacy decision-making. The firm adopted a comprehensive Privacy Code and revamped their associated policies and procedures. All six privacy goals are in evidence and appear to be mutually reinforcing. While the bank's overriding concern is to be seen to comply with the law, other goals such ethics and business objectives clearly influence the bank's approach to privacy. Decision rules that assist in operationalizing the Privacy Code are also evident.

Consistent with my findings in Case A (pilot study) and B, I found that the exercise of applying the IPO Definition using all available data was more useful and provided better insights than simply reading the privacy policy. This again demonstrated the necessity of examining more than privacy statements if we are to learn the "why's" of organizational privacy actions. In the next section, I describe Case C's placement on the IPO Continuum.

Case C's Position on the IPO Continuum

I applied data from the personal interviews and firm documents to establish Case C's placement on the IPO Continuum. Table 10-5 summarizes the evidence.

Table 10–5 Case C - IPO Evidence

IPO Continuum Layer & Positioning	Evidence
Customer Relationship Stance : **Shared Responsibility**	• Strong evidence of mutual interest ("the better we know you, the more able we are able to provide the best products and services to meet your financial needs"). • There is a great deal of specific information provided to assist customers to understand the reasons for certain actions. • There is limited evidence ("an ethical issue") that suggests that the firm feels obliged to promote customer well being (at its own expense). • No indication of an exploitation or self protection position.
Customer Information Management Strategy: **Minimize Risks and Add Value**	• Risk management strategies ("appropriate security measures are employed in the transfer of sensitive information" and "verify identity"). Specific information about customer information and credit assessment. • Evidence to support add value position ("In order to provide you with a high level of service and an extensive range of products, we need to know who you are and understand your financial needs"). Indications of support for status quo marketing initiatives. • No discussion of cost reduction strategies and no evidence to support "create new reality"
Customer Information Privacy Philosophy: **Privacy as Exchange → Privacy as Opportunity**	• Clearly aware of existence of PIPEDA and the need to comply. • Minimal discussion of constraints ("if you [choose not to provide certain information], we may not be able to provide you with the product, service or information that you requested"). Rejection of "constrained view" at corporate level. • Evidence that customers trade information to receive products and services ("determine your eligibility"), but language is strongly in the mutual exchange vein. • Evidence to suggest that firm is actively considering position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours: **Professional Codes → Enhanced Privacy**	• The company is clearly more than minimally compliant. • Specific reference and clear evidence that their Privacy Code was modelled on professional/trade association CSA Model Code. • Strong governance model and ongoing commitment to privacy across firm's operations. • Some evidence to support considering what "significantly enhanced" position might involve.

Customer Relationship Stance (CRS)

Recall that CRS was defined as *the organizations' predominant characterization of its relationship to its customers based on the definition of its obligations to its customers.*

Case C stands squarely in the "Shared Responsibility" position on the CRS layer. This is not an accidental position but one that appears to be the result of a concerted corporate effort to create "partnerships" with customers. Case C has a proactive approach to supporting its customers ("help you meet your financial goals") but at the same time is realistic in its commercial mission ("we're still a business, after all") that places obligations on its customers. For example, the Privacy brochure has a section headed "What are [your] responsibilities regarding [your] privacy?" This section mostly deals with security issues including protecting identification numbers and access codes ("it is up to you to protect this information and prevent misuse.") In addition, the wording for opting out provides explanations that clearly indicate that customers are responsible to make choices that are in their best interests, and that it is not the bank's responsibility to do so. At the same time, the bank assumes responsibility for its actions (" privacy protection is included in our Statement of Values and Commitments, framework for how we make business decisions.")

There is no evidence to support placing Case C in the "buyer exploitation" position. There is weak evidence of the "buyer self protection" position that appears to have more to do with the need for customers to be aware of their obligations when purchasing "registered" products (i.e., mutual finds within a registered retirement savings plan) or "contracted" services (i.e., personal loans and mortgages). There is weak evidence of a "consumer well being" position. This position could be assumed because of this financial institution's strong community orientation. However, in speaking with bank employees, that community orientation in no way undermines the commercial mission or suggests that the bank acts with any less stringent financial prudence than their competitors.

In summary, there is interview and documentary data to support Case C's placement in the "Shared Responsibility" position on the IPO Continuum.

Customer Information Management Strategy (IMS)

Recall that IMS was defined as: *The organization's predominant strategy with respect to its objectives for gathering and using information.*

Case C, consistent with other financial institutions, operates within a tight risk management framework. To the extent that they gather customer information to "determine eligibility" (i.e, seniors' discounts), "verify identity" (i.e, fraud protection), and evaluate risk itself (i.e, credit worthiness), Case C is using a "Manage to minimize risk" approach. However, also operate with the concern that not providing privacy constitutes a significant operational risk (i.e., opens them to liability) as well as reputation risk (i.e. diminishes their stature with customers and other important stakeholders). Therefore, there is evidence that Case C should be positioned on the "Managing to minimize risks" position on the IMS layer of the continuum.

At the same time, Case C uses customer information in a traditional marketing arrangement: "In order to provide you with a high level of service and an extensive range of products, we need to know who you are and understand your financial needs." They gather customer information in order to determine what products and services they should offer, to target potential customers, and to create promotional campaigns. The CPO and others perceive that the bank is behind their competitors in the ability to use their customer information effectively for "value-add" purposes. As a result, they are working to extract better value from their CRM investments:

> [Bank] has invested in the technological and usage aspects of CRM and needs to continue to focus on how to ensure that the entire workforce collects, uses and discloses personal information in a manner that does not invade the privacy of member

At the same time, the bank understands that

> privacy plays a crucial role in the success of CRM[2] ... and that ... organizations will find that customers want to see why all this data is being gathered, and they will expect the

[2] References a 2002 study by Gartner research group as "Report: Companies must balance privacy with CRM programs" DM Review Jan 2002.

> CRM experience to reflect intelligent use of their personal data. Otherwise, organizations will not be in a position to ask for the data at all.

There is no evidence to support a "manage to minimize costs" position that I could discern. As well, there is no evidence for the "manage with information to create new reality" position. This latter position might be desirable over the longer term but for the present, the bank is focused on managing their current reality.

In summary, interview and documentary data point to Case C as straddling the position between "Managing to minimize risks" and "Managing with customer information for value-add".

Customer Information Privacy Philosophy (PHIL)

Recall that PHIL was defined as *the organization's predominant philosophy about the role and impact that customer information privacy norms and laws have on the firm's ability to carry out its business.*

Case C clearly is aware of the existence of privacy statutes (federal and provincial) and their applicability to the financial institutions industry generally, and the bank in particular. The law supports traditional practices of confidentiality ("we don't talk about our customers outside the bank") and provides the firm with a type of reassurance ("we collect information lawfully").

Case C as clearly, rejects the "privacy as constraint" position, at least at the head office, corporate level. What constraints that were identified were recast as part of an information discipline (my term). For example, more than one interviewee expressed concern that the firm's customer information practices needed the benefit of privacy to bring a "responsible information management" approach to the firm:

> We gather too much information. We have a lot of information already and we collect a lot of information all the time. Our information isn't purged. We need to delete and update our holdings, and we need a more dynamic profiling system. We need the right information, not more information.

This sentiment was echoed by the CPO who remarked that improved information discipline was a benefit of the legislation:

> Yes, [information discipline] ... [it] focused our attention through a legal requirement. For example, it brought to light the need to think about our forms. We needed to tighten up on who was making marketing decisions ... it could be seen as part of business value including operating control systems and thinking about ownership of information. The issue is how to handle information throughout the company.

The privacy legislation itself appears to be seen as a vehicle for improving information exchange with customers, such that "the more confidence a customer has with an organization's privacy policies and strategies, the more information they will disclose to the organization." They substantiate this belief by citing a study conducted in the U.S. that suggested that 50 percent of customers said they would buy more frequently and in greater volume from companies known to have more reliable privacy practices.

The story is a little different in the branches. For example, one Account Manager suggested that "too much privacy doesn't help them [customers] or us [account managers]." This was explained as meaning that the more information the bank was able to gather, the better picture of how the customer has acted with their finances. This improves the bank's decision making ability (ie, if to lend, how much to lend, under what terms to lend). However, there was no indication from this individual that they had, in fact, been constrained in their ability to do their job. It seemed more a matter of finding the "privacy sensitive" (my term) approach to an unwelcome change to a well-established routine. A different branch staffer indicated that while the privacy law was "no biggy" it had required some changes that had not made life easier. For example, the branches were required to stop putting post-its and other notes into client files with anything other than "factual information." (This caution comes from the fact that customers now have the right to access and challenge information about them). Typically, "we used to be able to put messages in the accounts [folders], for example, 'this customer was rude', 'has an issue', etc. We could forewarn other people and be prepared for meetings. We can't do that now, that's a

disadvantage." However, to the extent that the bank appears to have a fairly strong corporate culture, the "disadvantages" of privacy legislation appear to be talked about but not acted upon.

There was no evidence that the bank is currently pursing a "privacy as opportunity position." However, to the extent that they are pursuing a strategy to both better integrate privacy and their CRM strategy and to strengthen the linkage between privacy and their strategic initiatives (five year plan), there is some indication that the bank is not disinterested in a stronger privacy position. They simply have not figured out what that "opportunity" might be and why it might be advantageous to pursue. However, their thinking seems to run along the lines of "match [the]customer strategies with responsible information management. This has the potential to optimize customer relationships and create competitive advantages."

In summary, Case C presently occupies the "privacy as exchange" position but is actively contemplating what pursuing a "privacy as opportunity" position might mean for the firm over the longer term.

Customer Information Privacy Behaviors (BHV)

Recall that BHV was defined as *the organization's publicly visible and internal information privacy activities*.

Case C is more than minimally compliant, thus not occupying the "not compliant" or "minimally compliant" positions on the BHV layer of continuum. Case C appears to very strongly compliant. They have based their privacy policy on the CSA Model Code including a strong governance model and ongoing commitment to embedding privacy throughout the firm's operations.

> The firm appears to reject the "privacy as compliance" approach. It was argued that
>
> privacy is a business issue and if you take a compliance approach you limit yourself in two primary ways. First, it [compliance only] marks privacy as a cost centre rather than as a source of revenue generation. Second, the approach sets customer-based strategies at odds with privacy protection when in fact they are in synch.

However, there is limited evidence that the firm has determined how to operationalize their approach. I was unable to discern the nature of the proposed "revenue generation" but suspect that it supports the privacy as exchange philosophy articulated previously. As to whether Case C will move into an "enhanced privacy" position, there is mixed evidence. It may be that moving to that position is not what is truly desired as much as is cementing and harvesting their present position. However, congruent with their potential for examining "privacy as opportunity" as a position (PHIL layer), Case C will likely refine their approach over time and may identify what "enhanced privacy" they may be able and choose to offer their customers.

In summary, Case C is presently strongly compliant and positioned within the "adhering to external codes" category. However, there is evidence that they are contemplating what they might do to pursue an "enhanced privacy position."

Figure 10-1 locates Case C's position in the IPO Continuum.

Theoretical Assessment

In this section, I review Case C's information privacy orientation first using the Institutional Approach and then the Resource-Based View.

Institutional Approach

Case C's information privacy orientation can best be explained using the lens of the Institutional Approach. I briefly apply the attributes of the institutional paradigm (more fully described in Chapter Five) to demonstrate how this theory explains Case C's approach to their privacy program.

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			Case C⇨	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
			Case C ⇨	
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case C		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case C	
	Weaker ⟷			***Stronger***

Figure 10-1: Case C's Placement on the IPO Continuum (Based on Interviews and Documents Results)

Organizational goal: Case C is pursuing legitimacy through legal and ethical appeals. In this manner, they appear to be interested in achieving pragmatic and social legitimacy. The bank has made significant investments in their privacy program and changed many aspects of their operations to achieve their privacy goals (technical). The search for legitimacy is negatively expressed as a desire to not be perceived by external audiences as being "offside" in comparison with their competitors. Positive expressions include wanting "to do the right thing" to satisfy legal (pragmatic) and customer expectations (social). There is some willingness to forgo certain activities for fear of customer reprisal but also a willingness to communicate in detail in order to educate customers.

Source of Pressure: Case C implemented their privacy program in response to a number of pressures. While they were concerned to meet their PIPEDA obligations, they also had some

internal pressures (social audit, transparency and accountability in business practices) (cause). Privacy norms, as represented by the ten PIPEDA principles, are strongly consistent with the bank's prevailing norms for the treatment of confidential information as well as for ethical business practices (content). The privacy program had been "legally coerced" to the extent that the bank adopted a formal, enterprise-wide program. However, the bank implemented their program at least one year before it was necessary, thus demonstrating volition (Case C would call this "leadership") with respect to their privacy program (control). Furthermore, the bank recognizes that it is part of the larger financial institutions industry. As such, Case C needs to be able to operate within the industry (interoperability standards) as well as withstand scrutiny from peer organizations (context). Case C's privacy motivation is captured by the Chief Privacy Officer's assertion that privacy is more than mere compliance but involves ethics and good business practices. Note that Case C is member of the same national trade association as Case B.

Ability and Willingness to Respond to Pressure: Case C responded to the pressure to implement their privacy program by investing significant resources to design, implement and maintain their privacy function. They operate with dedicated staff and an annual budget. The bank is very firmly embedded in a network of similarly sized financial institutions. However, they implemented a privacy program before their trade association had issued its model privacy code. This approach reflects the bank's view of itself as an "ethical business leader" both within its immediate network and as part of the larger Canadian financial institutions industry.

Response to Pressure: Case C exercised agency in their response to the pressure to implement a privacy program. They undertook an independent search for privacy program alternatives and are engaged in ongoing monitoring and evaluation activities. They provide significant information to customers, provide extensive staff training and engage in external privacy activities. These attributes combine to strongly argue that Case C's information privacy orientation is not simply an "acquiescent" institutional strategy. It appears to more closely resemble the "proactive" institutional strategy (Cashore and Vertinsky 2000) that I had discussed

in Chapter Five. My reconsideration of this response strategy is examined in the cross-case analysis in Chapter Twelve.

In summary, Case C's information privacy orientation can be analyzed using the Institutional Approach. The bank appears to be pursuing a proactive institutional strategy.

Resource-Based View

Recall that I theorized in Chapter Four that the Resource-Based View would offer a lens through which to consider IPO heterogeneity. That is, I offered two resource-based interpretations for firms that appeared to be interested in pursuing privacy as a source of sustainable competitive advantage either through a knowledge or relationship based capability.

Case C does not appear to be pursuing a resource based privacy strategy. First, while they want to be perceived as privacy "leaders" in the sense of being ethical business practitioners, they do not want to differentiate themselves on the basis of privacy if that means they run a negative risk. Their goal is to have privacy as one of their identifiable ethical business practices but not one that sets them too far apart from their peers. Second, this approach means that they engage in symbolic (informational) and material (practices) activities that move forward their privacy agenda while minimizing perceived privacy downsides (e.g., trying to avoid privacy problems). As a result, Case C has pursued a "proactive" approach to privacy that places it at ahead of its immediate peer group but does not differentiate it on the basis of the use of resources for competitive advantage.

It is this latter point, the use of resources, that is most interesting with Case C and suggests that they might move to the RBV approach in future.

In sum, the RBV does not offer much immediate insight into Case C's information privacy orientation. However, should the bank decide to pursue a more aggressive strategy with respect to the use of customer information for building stronger customer ties (relationship strategy), it may be useful to revisit the application of the RBV as an explanatory lens.

Chapter Summary

In this chapter, I provided the results of the Case C study. Using a triangulation approach (based on interview and documentary data), I applied the IPO Definition and defined the layers of the IPO Continuum. Then I mapped Case C onto the IPO Continuum. Finally, I considered Case C's information privacy orientation through the competing theoretical lenses and suggested that their IPO is presently best explained using the institutional approach.

CHAPTER ELEVEN

CASE D

In this Chapter, I describe the results of the third field case study, Case D. Briefly, I conducted a five day research site visit at Case D's head office in August 2004. I interviewed 17 executives, managers and senior staff about how the company had gone about organizing and implementing their customer information privacy program. I also collected or reviewed 20 documents related to privacy. The bank invited 50 personnel to complete the on-line version of the survey (of which 17 were completed and returned for a 34% response rate).

This study was undertaken to answer the first two research questions:

R(1) Do firms have an Information Privacy Orientation?

R(2) Is Information Privacy Orientation constructed as I have theorized?

To answer these questions, I assess Case D's information privacy orientation based on the triangulation of data I obtained through the interviews I conducted, the completed surveys, and the documents I reviewed. First, I assess the firm's privacy policy for comprehensiveness, readability and accessibility. Second, I review the firm's privacy program against the IPO Definition including principles (external and internal), values, policies (governance, resources, evaluations), objectives and decision rules. Third, I position the firm on the IPO continuum. I report the initial positioning based on the results of the IPO Survey. Then I reconsider the positioning layer by layer (customer relationship stance, information management strategy, privacy philosophy, and privacy behaviours) by triangulating the survey, interview and documentary evidence. I provide a final positioning on the continuum for Case D. Note that Appendix N contains a collection of information from Case D's case study database, including interview and document lists, and IPO survey statistics. To set the stage for understanding the IPO analysis, I provide a brief background to Case D's privacy program.

Case D: "Let's talk about information management"

Case D had adopted a privacy code in 1998 based on the Model Code produced by its industry association (which had used the CSA Model Code for its foundation).[1] The adoption of a privacy code in 1998 was a pre-emptive maneuver by this bank (and its competitors) to discourage the possibility of a legislated privacy regime, or, in the face of an inevitably, to influence the shape of the regime. When PIPEDA was proclaimed it incorporated the CSA Model Code as a Schedule, thereby enshrining the ten privacy principles that the banks had already begun incorporating into their operations. Therefore, at the level of compliance, Case D was well on its way to being compliant in 2001. The Legal Department had had initial responsibility for implementing the PIPEDA requirements and had attended to the "immediate exposure" issues such as 3rd party contracting, consent forms and the like. However, privacy was not firmly anchored in the bank and was drifting somewhat when the new CPO was appointed, as was expressed by an executive,

> it started off, I think, as everything else starts off with the view that, oh boy, we better be complying with the law here. So that's why the legal department looked at the law and said, what do we need to do, and let's hurry up. But it ended up in saying, hey, this is more than just about the law. We're the kind of organization that, you know, we believe this stuff. We believe that it's important, it's part of our value system.

A seasoned executive operating at the highest level of the bank, the CPO brought a customer-focused compliance philosophy to bear on the issue of PIEDA compliance and set about creating a higher visibility for the issue across the bank's operations. Since the CPO took up the role, the corporate policy adopted for immediate compliance purposes was reviewed and updated (and is undergoing another review). A comprehensive governance framework is being implemented. Corporate standards (the next level of compliance "rules") have been instituted and the role and mandate of the Privacy Office has been clarified. Currently, the issue is what is to be

[1] It was suggested to me that the Case D had been operating with a privacy code "since the year dot." However, I could not obtain a copy of the policy and so could not verify the statement (although I assume it is factual).

privacy's role as the organization moves into a "post-compliance" environment. As a Privacy Manager suggested,

> I think the privacy office will still be here, perhaps, but their role would be changing more to an assist ... and related to[being] a centre of competency, going forward. We've been doing a lot of things in terms of sort of project mode since we started, which I think will become less and less as time goes on.

Case D appears to evolving to a state of privacy as an enabler of good information management practices.

Privacy as an Information Management Enabler

Case D appears to have made a choice that moves it away from an information privacy "compliance" perspective to an information management "enabler" posture. The different yet complementary disciplines of information privacy, information security, and information resource management are being combined into a "triumvirate" that addresses "information stewardship". The bank is using this information stewardship approach as a way to reconcile the tensions among information management (especially the use and reuse of customer information to improve returns on information technology investments), information security (the emphasis on organizational control of technology assets) and information privacy (the customers' right to exercise control as the information owners). In this way, Case D is firmly entrenching privacy as more than a legal compliance issue. It is creating a role for privacy that attaches it to the core of the business. As was expressed by a senior technology staff person,

> we've been working to develop things like information stewardship to have a better sense of that whole information management life cycle. And of course, to do that properly it bumps up against privacy and information security. Because you can't divorce the issues... we really have to be working in concert, and I don't think it's quite clear yet where one thing starts and stops yet. But, I mean, that's all part of the maturity model is to get, if we get a better sense of information management by – to do that we will get privacy as we've been going through this work, we'll get that done better. As we get information management and information security organized better, it all starts to fit in.

In this new approach at Case D, the role of the information resource is becoming paramount with privacy operating as an important supporting actor. Within its corporate policy,

the bank defines the information resource as "information and the technology-based systems, applications and computing, and network facilities that are used in the management, processing and communication of information." The information resource management policy has three objectives, to ensure,

1. Accuracy and integrity of the information resource.
2. Privacy and confidentiality of private and sensitive information in the Bank's possession or entrusted to third parties.
3. Cost effective measures to limit, to acceptable levels, risks related to the security of the Bank's information resource.

Clearly, privacy is implicated in all three objectives (not just the second one that specifically refers to privacy). Accuracy and integrity are seen by the CPO and Privacy Managers as outcomes of strong privacy practices that create a virtuous trust circle with customers. The third objective (cost effective security) speaks directly to the PIPEDA principle that calls on organizations to adopt safeguards that match the sensitivity of the information. AS the CPO expressed the privacy relationship to the information management initiative,

> So it's my job to look at that privacy slice, at a say – because if you think of it – you start with the broad umbrella of good information management ... the things you do around managing information well really would not suffice, but would *address* the nine out of ten, or eight out of ten requirements of the legislation. So, because you'd be interested in accuracy and data retention and quality and security and all those things, and of course you can have those other components. So my job is to work with the places in the organization that entrench the privacy attitude, and the privacy processes into the way in which we work. And it cuts across a lot of things, a lot. Everything from ... who gets access ..., to ensuring that access to information is properly decided and defined and managed and monitored, to data classification system, to project development methodology and ... what privacy questions to ask. So there's a lot of places that I have to find, and that's been part – part of the challenge is sort of getting yourself everywhere, making sure you're in the bowels of the organization, if I can put it that way. Because it's got to get designed into processes.

The information management initiative being pursued by Case D is a long term project that, it is hoped, will "create an environment and culture that recognizes the value of data as it is processed through the organization" and is turned into "valuable information." The role of the privacy staff is to ensure that privacy is "built into processes at the start" so that the true value of the information resource can be unlocked with certainty (accuracy and integrity objective) and

assurance (that customer information privacy has not been violated). In this was, privacy becomes the "reminder of why you need [data] discipline" so that the organization does not fritter away the opportunity to gain value from "personal information as a scarce resource." According to the participants at Case, competitive differentiation is difficult to achieve in Canada's small, tightly regulated, and interdependent financial institutions industry. The three pronged, "holistic, stewardship approach" to information, featuring a prominent role for information privacy, is one way that Case D is considering as a differentiator.

In summary, Case D represents a firm that is beginning to contemplate entry into a new phase of managing customer information privacy. The bank appears to be adopting privacy as part of a fundamental movement to an information stewardship approach based a foundation of information management bolstered by a strong information security practice and a robust privacy management regime.

In the next section, I assess Case D's privacy policy.

Assessing Case D's Privacy Policy

Consistent with my practice in all cases, I assessed Case D's privacy policy on the basis of comprehensiveness, readability and accessibility. Table 11-1 summarizes the findings. I assessed the privacy policy information contained on the bank's website in the section entitled "Your Privacy".

The overall score generated for the Privacy Notice is 8.5, which would place this firm's privacy approach in 4th place within the rankings of the ten firms examined in Chapter Seven.

Comprehensiveness – Case D scored 3.5 for comprehensiveness. The Privacy Code does not refer to PIPEDA or the CSA Model Code. Information is provided about each of the ten principles. However, the information is not organized to parallel the ten principles nor are the

Table 11-1: Case D - Privacy Notice Basic Assessment

Criterion	Key Questions/Concerns	Case D Results
Policy Comprehensiveness SCORE = 3.5	• Are all PIPEDA/fair information elements addressed?	• PIPEDA not specified • Information principles within PIPEDA are covered thoroughly.
	• Is there a summary of the policy that emphasizes key features?	• Provides a summary of the information contained on the site more than a summary of the policy.
	• Is responsibility clearly identified?	• Several references to Privacy Officer but not identified by name; general privacy office contact info provided • Summary provides overview of CPO responsibilities
Policy Readability SCORE = 3	• What is the readability score for the privacy policy document(s)? • Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 34.3 (harder category) • Flesch-Kincaid Grade Level = 12 • Written in Plain English, not too legal
	• Are key terms explained?	• Yes. • Definition of "Personal Information" in linked section – "What is personal information?" • Definition of technical terms in linked section – "Security".
	• Are examples provided? Are the examples thorough and understandable?	• Many. • Section "What is Personal Information" provides examples for every section. • Most explanations clear but some a little vague.
	• Are consent forms provided?	• No.
Policy Accessibility SCORE = 2	• How easy is it to find the policy? Are there multiple access points?	• Home page and subsequent pages
	• Are there links to other privacy information (external)?	• External organization (Privacy Commissioner of Canada) identified but not linked, contact info provided • Ombudsman for Banking Services and Investments
	• Is there a webseal or other "seal of approval"?	• No.

sections referred to as such. Key aspects of the policy are easily identifiable through headings and subheadings. The existence of the Chief Privacy Officer position is identified as the responsible

person for "privacy governance" and contact information is provided. As well, a brief description of the Privacy Officer's duties is provided,

> [Bank] has a Chief Privacy Officer who oversees privacy governance including policy, dispute resolution, education, communications activities and reporting to our Board of Directors and Senior Management. The Chief Privacy Officer can be contacted at ...

Readability – Case D scored 3 for readability, which is consistent with the majority of firms reviewed in the Evaluation Study. The Reading Scores place it in the "harder" category (Flesch Reading Ease >30). The Notice is largely uses active voice and is written in what I call "Plain English Legalese." Several definitions are provided, most importantly one for "personal information",

> The term "personal information" refers to information that specifically identifies you as an individual and is provided to or collected by us. In includes information that you provide or that we collect from other sources with your permission, for example: your name and address, age and gender, personal financial records, identification numbers including your social insurance number, personal references, and employment records.

Additional terms are provided in the section on Security. Many examples are provided throughout the document. A consent form is not provided.

Accessibility – Case D scored 2 for accessibility. The privacy information is easily accessed from anywhere on the website. Information is also obtainable from branches and customer contact centers. External organizations are identified under the "Dispute Resolution" section including the Privacy Commissioner of Canada (contact information but no link) and the Ombudsman for Banking Services and Investments (link provided). There is no privacy webseal.

Summary - Overall, this firm provides good privacy policy information to existing and potential customers about information privacy. The policy appears to be compliant with PIPEDA. The score generated for this assessment exercise is 8.5 which, when compared to the firms in Study One, places Case D in the 4th rank among the range of assessment scores that were generated in the initial evaluation of privacy policies (see Chapter Seven).

Applying the IPO Definition to Case D

I applied the IPO definition by coding the interviews and the privacy documents I was able to obtain or review on site. The coding was reviewed and approved by my supervisor. With both data sources, I looked for information, quotes and examples of the different aspects of the IPO definition – principles (external and internal, values, policies, objectives and decision rules). Table 11-2 summarizes Case D with respect to the application of the IPO Definition.

Table 11-2: Case D - IPO Definition

IPO Definition Component	Findings: Case D
Principles (external)	• Model Code provided by national trade association based on CSA Model, (adopted in 1998) • Revised to reflect PIPEDA (adopted 2001)

Principles (internal)	• Enterprise-wide privacy policy (adopted 2003, currently under revision) articulated fundamental premise: individual right to control personal information.
	• Operating principles
	  • "Customers own the information they provide to the bank."
	  • Is it fair? right? legal?
	  • Tradition of confidentiality

Values	• Code of Business Conduct and Ethics emphasizes "ethical standards beyond reproach" and 'honesty beyond question"
	• Code specifically refers to "respecting and protecting information"
	• Privacy Philosophy (articulated in Corporate Privacy Policy):
	  • Respect an individual's private information
	  • Protect an individual's private information
	  • Resolve disputes surrounding an individual's private information

Governance & Structure	• Initial response handled by Legal department, primarily to address consent issues. Already operating within industry model code (adopted 1998). New provisions implemented for Jan.1, 2001 compliance deadline. • Comprehensive policy adopted by Board of Directors (adopted 2003). • CPO Responsibility – assigned to an Executive Vice President (privacy not a full time responsibility but fits within overall mandate) • Provides quarterly reports on privacy compliance matters to the Conduct Review Committee of the Board. (primarily). Also reporting to Risk Review and Operational Risk committees. • Operates with Privacy Executive Committee (enterprise wide executives) as well as Privacy Working Groups (management and staff).
Resources (domestic retail banking only)	• Three full time professional staff with day to day responsibility. • Services of in-house legal counsel. • Additional senior staff positions with privacy compliance responsibilities. • Dedicated budget. • Privacy mandate in Information Security and Information Resource positions

	• Assistance Managers handle compliance issues in branches. • Customer Contact Centre as point of contact for complaints and inquiries if not dealt with at Branch level.
Reviews & evaluation	• No formal privacy assessment prior to 2001 implementation (staff in Legal department handled initial issue) • Participated in third party privacy study examining "automating privacy" • Internal Audit examined practices within Privacy Office (2004) • Privacy Policy currently under review as part of privacy governance framework initiative
Legal	• First and foremost is legal compliance. However, importance of privacy practices goes beyond legal compliance. • Emphasis moving from consent to information management.
Technical	• "New technology (allows for data collection and management) requires new strategy for leveraging value of personal information. • Information Security is part of governance triumvirate incorporating Information Privacy, Information Security, and Information Resource management.
Contractual	• Working to ensure 3rd party compliance with vendors, suppliers and affiliates. • Monitoring trans-border issues (i.e., U.S. Patriot Act and affect on compliance with PIPEDA).
Business	• Working with Information Security and Information Resource Management to ensure that data and information are seen as a critical organizational resource – actually more an asset. • Privacy as component of information discipline. • Privacy has strategic value (ill defined). • Privacy as subset of Operational Risk Management. • Privacy implicated in Reputation risk management. • Aspires to enterprise-wide "Information Stewardship" to leverage value of the information asset.
Social	• Privacy as a way to build customer trust – "the more your customers trust you, the more they allow you to use their information." • Some evidence to support privacy as a means to support broader, deeper and longer term customer - Benefits of "quality customer information" - • Improved marketing information – right products/services to meet [customer]needs plus appropriate pricing based on reliable information
Ethical	• Use of term ethical in Code of Conduct but not specifically a reference to privacy. • CPO refers to privacy as an essential "ethical information practice" but concept is not developed elsewhere in other policies.

Decision rules	• Evidence of deliberate choices made in how privacy is operationalized.
	  • Does not sell customer information.
	  • "If we obtain client lists from other organizations, we first require that the organizations to confirm that they comply with all relevant privacy legislation."
	  • Does not use certain publicly available information (i.e, mortgage renewal data available form Registry Offices) to directly solicit business.

Principles

External: There is reference to PIPEDA as the legal statute to which the firm must comply as well as to the CSA Model Code External Principles were articulated in several documents (such as the national trade association's Model Code) as well as by most interviewees (typically referred to as the "guidelines"). The corporate policy documents expressly identify the CSA Model Code and PIPEDA as the basis for privacy action by the firm.

Internal: The bank's Corporate Privacy Policy subscribes to the "fundamental premise" of the individual right to control personal information. This premise is operationalized in three manners. First (and differing from what I observed at at least two other case) is the principles that "customers own the information they provide to the bank." Second, employees are encouraged to adopt a default question set when confronted with a new problem that asks if the contemplated action is "fair? Is it right? Is it legal?" Third, and consistent with the other financial institutions in this study, Case D operates within a strong tradition of "confidentiality."

Values

There are two sources of values to guide privacy decision making at Case D. First, there is the set of values articulated in the Code of Conduct and Ethics that emphasizes "ethical standards beyond reproach" and "honesty beyond question." This Code also includes the requirement that employees "respect and protect privacy." Second, and more specifically, the Corporate Privacy Philosophy articulates a three pronged "Privacy Philosophy" of respecting and protecting, and resolving disputes surrounding an individual's private information.

Policies

I consider the policies of Case D under three headings – governance, resources and evaluations.

Governance: The firm adopted a comprehensive privacy policy based on the CSA Model Code supplied by the national trade association, in 1998. The privacy policy was updated to more directly address PIPEDA requirements in 2001 and a new privacy corporate policy on privacy was adopted by the Board of Directors in 2003. The bank's policies and procedures have been updated (including the articulation of corporate privacy standards)

The Chief Privacy Officer (CPO) role is occupied by an Executive Vice President. While privacy is not the full time focus of this position, it fits well with the mandate. The CPO operates with an enterprise wide Privacy Executive Committee as well as with privacy working groups (composed of managers and staff from functional areas as well as the lines of business). The CPO reports quarterly to Board of Director's Conduct Review Committee (primarily) as well the Risk Review and Operational Risk Committees (occasionally on an exception basis).

Resources: The Privacy Office operates with three full time professional staff in support of the CPO, and a dedicated budget. As well, the privacy staff have access to internal legal counsel resources. Additional senior staff positions within the lines of business (e.g., Senior Manager, Compliance in Retail Banking; Director of Compliance, Private Banking), and functional areas (e.g., Privacy Specialist within Corporate Audit Team; Business Consultant within Technology division) have privacy responsibilities.. At the branch level, there is typically an Assistant Manager who is responsible for handling compliance initiatives. In addition, the staff at the Customer Contact Centre field complaints and enquiries that have not been directed to branch level personnel.

Evaluations: Case D has employed some evaluations to assist them with developing their privacy approach. Staff have participated in a study about "automating privacy" (conducted by a major vendor). An internal audit was conducted on 2004 into the practices and procedures of the Privacy Office and recommendations were made for improvement. The Corporate Privacy Policy itself is under review presently as part of the privacy governance framework initiative. Case D

believes that it can continue to evolve its privacy program to meet its organizational needs and address a somewhat "volatile" external privacy environment.

Objectives

I was able to gather evidence in support of all six objectives. While I identified that the overriding objective is to achieve compliance, I discerned that there were secondary objectives as well.

Legal – The primary reason for Case D to develop and implement its privacy program was to comply with the federal law. In response to a question about the goals for the bank's privacy initiatives, many interviewees identified "compliance" as their first choice.

Technical – There was some evidence of information security as an important privacy program objective but within the overall framework of their information management approach, not simply as a support to privacy goals. At the same time, the technical goals go beyond the firm as the Information Security Manager is participating in discussions to establish data classification standards to support security and privacy of customer files as they pass through the highly integrated Canadian financial institutors system.

Contractual – Case D is working to ensure 3rd party compliance with PIPEDA in contracts with vendors, suppliers and affiliated organizations. Of potentially increasing importance is the application of the U.S. Patriot Act to customer information that may be sent to the U.S for processing. This may raise compliance issues.

Business – Privacy at Case D is a increasingly seen as a business issue as is expressed as such. There appears to be several business goals. At the level of the individual customer, the goal is to make privacy a "non-issue" (in the positive sense that the customer is not concerned, trusts the Bank is doing the right thing, and continues to do business). At the enterprise level, there are several privacy related goals. As previously discussed, there is the long term goal in which information privacy reinforces an information management approach that delivers good financial

results. In more immediate terms, good privacy practices are seen to be a means to mitigating various risks including operational and reputation risk.

Social – There was evidence of a social goal for the privacy program. Privacy is considered to be an important vehicle for building and sustaining customer trust, as illustrated by this excerpt from a conversation with the CPO,

> focused a little bit about on trust and the building of trust, the maintaining of it, and how easily reputations can be impacted. And the issue, or the point of privacy was seeing as a way in which to build that trust, create – create and build that trust between the organization and the … the client. And the point is that – the belief that you handle personal information properly, in terms of from the client's perspective, and you create a level of trust that you, it's causal-like, it's circular, one feeds the other. So the trust is enhanced, therefore – and in fact, therefore the more that they trust, they more you can actually use the information, so it's not unselfish. It's selfish. It's actually smart business to demonstrate that you can be trusted, do the right thing, demonstrate that you can be trusted, because then they'll let you do more, they'll trust you. And they'll trust you to use it [appropriately].

This shows that Case D believes that providing customer information privacy creates the circumstances under which customers share more information because they believe that they will benefit from the sharing, not be exploited by it.

Ethical – I found some limited evidence to support the ethical goal for privacy. The CPO refers to privacy as an essential "ethical information practice" but the concept is not well developed. The Code of Conduct refers to Protecting privacy but does not really discuss the ethical issues that might be involved. However, in the IPO Survey section that requested respondents to rank a series of privacy statements ("In my company, privacy of customer information is primarily a _____ issue"), the response "ethical issue" was the marked as most important (combined first and second choices) by 7 (of 33) respondents, ahead of information management" (6) and legal, marketing and risk management (5 each).

Decision Rules

There was evidence that the firm had adopted decision rules with respect to how their privacy policy would be operationalized across the bank. There were several discrete examples of

which I will present three. First, the firm does not sell its customers' information. (as was suggested to me, "why sell that particular asset. The real value comes from being able to use it over and over again.") Second, while the firm may purchase 3rd party lists, they only do so from firms from whom they have received assurances are PIPEDA compliant. The third example is particularly interesting because it involves the decision not to use a form of publicly available information. Case D has stopped a practice apparently still used by certain competitors. The practice involves accessing publicly available information through the Land Registry about mortgage renewal data. This information source was not pursued because the bank was concerned about the potentially negative reputation effects of the practice.

In summary, I was able to apply the IPO definition to Case D. I found evidence of external and internal privacy principles. I was able to discern several values that appear to guide corporate decision-making generally. The firm adopted a comprehensive Model Code and implemented a comprehensive corporate policy and standards. All six privacy goals are in evidence to greater or lesser extents. While the primary objective is legal compliance, the other five goals all featured prominently in Case D. Several decision rules have been adopted to prevent practices that contravene the spirit of the law if not its letter.

As with the previous cases, I found that the exercise of applying the IPO Definition using all available data was more useful and provided better insights than simply reading the privacy policy. This again demonstrated the necessity of examining more than privacy statements if we are to learn the "why's" of organizational privacy actions. In the next section, I describe Case D's placement on the IPO Continuum.

Case D's Position on the IPO Continuum

I triangulated data from the IPO Survey, the personal interviews, and firm documents to establish Case D's placement on the IPO Continuum. I applied the IPO Continuum to Case D's circumstances in two steps. First, I analyzed the results of the IPO Survey and plotted the firm's

initial placement on the IPO Continuum. Then I triangulated the data for each layer of the continuum. I conclude with a reassessment of Case D's placement on the IPO Continuum. I will address each step in turn.

Survey Results

I used the results from Case D's IPO survey to establish a preliminary placement on the IPO Continuum. Appendix N provides the statistical details. Table 11-3 shows the findings

Table 11-3: Case D - IPO Survey Findings

IPO Component	Weighting	Mean of Means	Score for Component	Score for Layer	Interpretation
CRSA	-1	2.3	-2.3	5.075 = **5**	"Positive" relationship with respect to obligations owed to customers. **Shared Responsibility**
CRSB	-0.75	4.3	-3.225		
CRSC	0.75	6.3	4.725		
CRSD	1.25	4.7	5.875		
IMSA	-1	3.5	-3.5	2.865 = **3**	"Negative" use of customer information. **Risk Management**
IMSB	-0.75	4.78	-3.585		
IMSC	0.75	5.1	3.825		
IMSD	1.25	4.9	6.125		
PHILA	-1	1.33	-1.33	4.00 = **4**	"Neutral" privacy philosophy No position
PHILB	-0.75	2.51	-1.8825		
PHILC	0.75	2.95	2.2125		
PHILD	1.25	4	5		
BHVA	-1	1.25	-1.25	4.83 = **5**	"Positive" privacy behaviors **Professional or trade association codes**
BHVB	-0.75	4	-3		
BHVC	0.75	5.69	4.2675		
BHVD	1.25	3.85	4.8125		

organized as an IPO score. I followed the same methodology as with cases A and B. Figure 11-1 shows how I plotted the firm's position on the IPO Continuum based on the survey findings. I discuss the findings layer by layer.

Customer Relationship Stance (CRS)

Recall that CRS was defined as *the organizations' predominant characterization of its relationship to its customers based on the definition of its obligations to its customers.* Overall, Case D scored 5 on the IPO Survey and was placed in the "Shared Responsibility" position. This position suggests that the firm has a strong, positive view of its obligations to its customers. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			Case D	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
		Case D		
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case D		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case D	
IPO Score	**1**	**2- 3**	**4**	**5- 6** **7**
	Weaker ◄——————————►			***Stronger***

Figure 11-1: Case D's Initial Placement on the IPO Continuum (Based on IPO Survey Results)

There was no evidence from the IPO Survey to suggest that the respondents consider their bank to be operating with a buyer exploitation customer relationship stance (CRSA). Respondents were neutral to slightly positive about the buyer self protection position (CRSB). This may reflect the contractual nature of many banking relationships, and therefore, the legal requirement for customers to inform themselves.

The respondents were neutral to slightly positive about customer well-being obligations. The firm was seen to be obliged to help customers make the best decisions (CRS13) and to be proactively advised about business practices (CRS16). There was no support for the idea that the firm would forgo profitability (CRS14) and only neutral to slightly positive support for the idea that the bank would place its customers' interests ahead of its own (CRS15). These responses are consistent with interview and documentary evidence. The bank's privacy policy proscribes certain activities (see IPO Definition – Decision Rules for details). This provides only very insubstantial support for a "customer-well being position."

Respondents agreed with statements that indicated that firms and customers "exist for mutual benefit" (CRS 10) and that they should work together "to maximize customer benefits and firm profits" (CRS 9). In addition, there was agreement for the need for the two parties to "understand their respective responsibilities within the commercial relationship" (CRS 11). Consistent with this stance of mutual responsibility, respondents agreed that customers "deserved explanations of our business practices if they requested such explanations" (CRS12).This position on the IPO continuum was strongly supported with interview data.

In summary, there is survey, interview and documentary data to support Case D's placement in the "Shared Responsibility" position on the IPO Continuum.

Customer Information Management Strategy (IMS)

Recall that IMS was defined as: *The organization's predominant strategy with respect to its objectives for gathering and using information.* Overall, Case D scored 3 and was placed in the

"Manage to Minimize Risks" position. This position suggests that the firm has a weaker, negative view of the potential use of customer information. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

There was consistent disagreement with IPO survey items (IMSA) related to the application of customer information to reduce costs. This position is supported by interview and documentary data. Cost management, while important I any enterprise, was not related to the collection and use of customers' personal information.

Interestingly, three positions - IMSB: Manage to minimize risks (mean = 4.78); IMSC: manage with information to add value (mean = 5.1); and IMSD: manage with information to create new reality (mean = 4.9) appear to have some salience for Case d RESPONDENTS. The straddle position between IMSB and IMSC has already been shown in previous cases to be consistent with industry norms. Financial institutions, by definition, are concerned to manage risk. Personal information is collected to manage credit risk and mitigate against fraud. These are stated purposes for collection and use of personal information (Privacy Code). At the same time, Case D needs to collect and manipulate personal information to tailor its market offerings and to provide personal service. Again, this is a stated purpose in the bank's privacy notice. Data from the interviews and documents support this dual IMS emphasis.

What is interesting is the strong "hint" that IMSD may be emerging as an information strategy option. Respondents agreed with statements that the "primary purpose of our information management strategy is to position the firm for the future" (IMS13) and "it is most important to my firm to use customer information for innovation" (IMS 15). There was less agreement with statements that "customer information is primarily useful as a means to create new competitive realities" (IMS14) and the "overriding information management priority is to apply customer information to the creation of new opportunities" (IMS16). These statements are substantiated to a certain degree by interview and documentary data. As was discussed in the section "Let's talk about information management," Case D is embarking on an information management initiative

that, it hopes, will deliver support new ways to use and manage customer information. To the extent that this is the bank's stated intention, these statements are understandable. But to the extent that the project is really still in the planning stages, it is premature to suggest that the IMSD "manage with information to create new reality" is the IPO position right now.

In summary, while the IPO Survey score placed Case D fairly evenly across three positions, it would appear that the dual "Manage to minimize risks" and the "Managing with customer information for value-add" are the best indicators of the bank's current position. However, there may be a future shift to "Managing with customer information for create new reality."

Customer Information Privacy Philosophy (PHIL)

Recall that PHIL was defined as *the organization's predominant philosophy about the role and impact that customer information privacy norms and laws have on the firm's ability to carry out its business.* Overall, Case D scored 4 and was placed in the "Neutral" position. This position suggests that the firm has not developed a consistent view of the impact of privacy legislation on its ability to carry on business. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

The survey, documents and interview data indicated a consistent awareness that the firm (and industry) were required to operate within the terms of a privacy statute. Therefore, there is no evidence to support the placement in PHILA (no concern or awareness). Neither is there data to support placement within the PHILB (privacy as constraint category).

Interestingly, the PHILC category "privacy as an exchange" was also not embraced. Interview data suggests that Case D operates with the exchange perspective on privacy. Indeed, the CPO expressed the belief that good information privacy practices underpinned the ability of the bank to establish and sustain valuable relationships. In addition, the firm's privacy policy specifically addresses the uses of personal information including "to understand your financial

service requirements," "to determine the suitability of products and services and offer them to you," and to "set up and manage products and services you have requested." All of these purposes are premised on information exchange between customer and the bank. As a result, I think that the firm should be positioned more strongly in the "privacy as exchange category" based on a preponderance of evidence.

Interestingly, the PHILD ("privacy as opportunity") position was the strongest (although still "neutral") of the PHIL components. The strongest statement was PHIL14 in which respondents agreed that "Privacy legislation has improved our firm's decision-making regarding what personal data to gather and how best to use that data." The rest of the statements in this category were less well received, especially those related to being better positioned than competitors (PHIL15) or assuming industry leadership (PHIL16). The argument for the "Privacy as opportunity" position is interesting in light of the previous discussion concerning the Information Management Strategy positioning with respect to "create new reality" also the strongest potential position on the IPO Continuum. I believe that the data supports consideration of this position as a future "option" for the firm but I am unconvinced at the moment whether the positioning would be noticeable to anyone other than a handful of senior head office personnel.

What might be the real message of this layer of the continuum for Case D is that the "privacy program as a response to a legislative initiative" while still real may no longer be the driving force it once was. The bank has been complying with a privacy regime for several years (since at least 1998 officially). "Compliance with the law" or "responding to legislation" may not resonate at the same intensity of frequency with Case D as it does with other firms that are more recent privacy players. This experienced firm may now be in a position to reap some benefit from their compliance activities including using their approach to "attract and retain customers" (PHIL13) and "improving decision making" (PHIL14). However, it is still too early to assess if this is a lasting position.

In summary, Case D appears not to strongly respond to any category on the PHIL layer of the continuum. This may be a consequence of their experience in managing under the PIPEDA legislation.

Customer Information Privacy Behaviours (BHV)

Recall that BHV was defined as *the organization's publicly visible and internal information privacy activities*. Overall, Case D scored 5 and was placed in the "Professional or Trade Group Codes" position. This position suggests that the firm has a stronger, positive view of its privacy behaviors. I will now discuss the extent to which this initial placement is consistent with triangulated data (survey items, interviews and documents).

The IPO Survey showed that there was consistent disagreement with BHVA statements that indicated that the firm was non-compliant. Documents and interviews clearly demonstrate that Case D is compliant with PIPEDA. Therefore, there is no reason to place the firm in this position on the continuum.

There was a neutral response to BHVB statements that suggested that the bank was minimally compliant. Documents indicate that the firm has implemented enterprise wide policies that do more than restate the privacy principles outlined in PIPEDA. Interviewees consistently suggested that the firm had done extensive work on privacy and ought not to be characterized as merely minimalist.

The BHVC category (Professional or Trade Group Codes) was the strongest category in the IPO survey results. This position was supported by documentary and interview evidence. The firm adopted in 1998, then updated in 2001 the Model Privacy Code drafted by their national trade association (that was based on the CSA Model Code). This Model Privacy Code operationalizes the 10 principles contained in PIPEDA beyond simple compliance. When queried, participants consistently perceived that their firm's privacy approach was either "middle of the pack" (as in average compliance for the industry) or slightly better then some of the competitors

but not a particular privacy leader. Just as clearly, the firm does not consider itself (and has no aspirations to be) a privacy leader.

Responses to the survey category BHVD (enhanced privacy) were, at most, neutral. There was disagreement with statement BHV13 ("Our firm has implemented a privacy policy that is regarded by others as leading in our industry") and only modest support for statements indicating that the firm "goes out of its way" to provide customers with privacy protections beyond that which is offered by competitors (BHV15). There was somewhat stronger support for statements that indicated "we give priority to privacy considerations when developing business initiatives" (BHV14). Respondents were only neutral about whether the firm provided the best privacy practices we have been able to find in our industry" (BHV16). These positions are consistent with documentary and interview data. "Enhanced Privacy" is not a desired position because it appears to represent a level of effort that exceeds any perceived benefits.

In summary, Case D was positioned in the "Professional and Trade Group Code" category on the IPO Continuum. This position is supported by the interview and documentary data.

Repositioning Case D on the IPO Continuum

The initial positioning on the IPO Continuum for Case D was modified after triangulating the results with interview and documentary data. Two positions were confirmed – the Shared Responsibility position on the Customer Relationship Stance layer and the Professional and Trade Groups Codes on the Customer Information Privacy Behaviour layer. Case D appears to occupy two positions on the Customer Information Management Strategy layer – "Manage to Minimize Risks" and "Manage with Customer Information to Add Value." This positioning may reflect the particularities of the financial institutions industry. At the same time, the information management initiative that is getting underway at Case D suggests that they may be "creating a new reality" but it is premature to assess its impact on their information strategy at this stage.

Case D's Customer Information Privacy Philosophy was originally positioned as "neutral." However, interview data suggests that there is clear evidence that the firm operates with a "privacy as exchange" approach. It is unlikely that Case D would consider pursuing an "opportunity" positioning, but that may depend on the success of the information management initiative helping to create the new realities that the firm could seize as opportunities. Finally, Case D is solidly located in the "Professional and Trade Group Code" position of the Behaviours layer and does not aspire to becoming a privacy leader. Figure 11-2 shows the redrawn IPO Continuum for Case D.

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			Case D	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
			Case D	
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case D⇨		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case D	
	Weaker ⟷			***Stronger***

Figure 11-2: Case D's Final Placement on the IPO Continuum (Based on Triangulated Results)

Theoretical Assessment

In this section, I review Case D's information privacy orientation first using the Institutional Approach and then the Resource-Based View.

Institutional Approach

Case D's information privacy orientation can be explained using the lens of the Institutional Approach. I briefly apply the attributes of the institutional paradigm (more fully described in Chapter Five) to demonstrate how this theory explains Case D's approach to their privacy program.

Organizational goal: Case D appears to be pursuing legitimacy primarily through legal appeals (compliance with PIPEDA) which indicates a concern for managerial legitimacy. However, the bank made significant investments in their privacy program and changed certain aspects of their operations to achieve their privacy goals thereby indicating a concern for technical legitimacy also. In addition, the search for legitimacy is both positively and negatively expressed. On one hand, the bank does not want to be perceived by external audiences as being less complaint than their competitors. At the same time, the bank is positively interested in demonstrating that it is doing the right things to satisfy legal (pragmatic) and customer expectations (social). There is some willingness to forgo certain activities for fear of customer reprisal but also a willingness to communicate in detail in order to educate customers.

Source of Pressure: Case D implemented their privacy program in response to a number of pressures. They were chiefly concerned to meet their PIPEDA obligations (cause). Privacy norms, as represented by the ten PIPEDA principles, are strongly consistent with the bank's prevailing norms for the treatment of confidential information, for ethical business practices, and the privacy code that was in place prior to the federal legislation (content). The privacy program had been "legally coerced" to the extent that the bank adopted a formal, enterprise-wide program.

publishing of the CSA and CBA model privacy codes. In this instance, Case D exercised volition with respect to their privacy program (control). Furthermore, the bank recognized that it is part of the larger financial institutions industry. As such, Case D needs to be able to operate within the industry (interoperability standards) as well as withstand scrutiny from peer organizations (context). Case D's privacy motivation is captured by the expression that "we are a compliant organization." Note that Case D is member of the same national trade association as Case A.

Ability and Willingness to Respond to Pressure: Case D responded to the pressure to implement a PIPEDA-compliant privacy program by building on their previously existing privacy program. To do so, the bank invested significant resources to design, implement and maintain their renewed privacy function. They operate with several dedicated staff and an annual operating budget. The bank is very firmly embedded in a network of similarly sized financial institutions both nationally and internationally. This embeddedness in an external network is reflected by their initial decision to implement a version of the CBA model privacy code well before PIPEDA was enacted. However, a stronger sense of embeddedness comes from the internal network of the firm itself. Case D determined the shape of their PIPEDA privacy program largely as an internal exercise and they continue to modify the program with minimal reference to external organisations.

Response to Pressure: Case D exercised agency in their response to the pressure to implement a privacy program. A key example of is the appointment of a very senior executive to lead the totality of the bank's privacy initiatives (domestic and foreign operations) who is engaged in ensuring the adequacy of monitoring and evaluation activities. Case D provides a good level of information to customers, continues to training staff, and engages in external privacy activities. These attributes combine to strongly argue that Case D's information privacy orientation is not simply an "acquiescent" institutional strategy. Rather, the accumulated evidence suggests that the bank is attempting to manage the external audience's view of its privacy

program through "impression management" initiatives. In summary, Case D's information privacy orientation can be analyzed and explained using the Institutional Approach.

Resource-Based View

Recall that I theorized in Chapter Four that the Resource-Based View would offer a lens through which to consider IPO heterogeneity. That is, I offered two resource-based interpretations for firms that appeared to be interested in pursuing privacy as a source of sustainable competitive advantage either through a knowledge or relationship based capability.

Of all the firms examined for this dissertation, Case D appears to be the closest to pursuing a resource based privacy strategy. In this section, I apply the elements of the RBV to a consideration of Case D.

Organizational Goal: Case D does not presently articulate their privacy initiatives in terms of competitive differentiation. As a result, it is unclear that if they were to choose this path, whether differentiation would be based on superior customer insight or superior customer trust (as I outlined in Chapter Five). I believe that the evidence suggests that the bank is pursuing a customer insight focused approach (regardless of whether they acknowledge this as a competitive differentiator).

Resource: Case D views customer information as a Level 3 resource (supporting organisational learning). The relative sophistication of this particular bank is such that it recognises the value of the information resource it has at its disposal and is wrestling with the best way to harness it. At the moment, the thrust of the information management initiative appears to be internally focused on issues such as the best way to capture customer preferences and to operationalise a single view customer file. The organisational objective is much more concerned with obtaining organisational efficiencies (internally focused innovation) than with developing effective external innovations (such as improved customer privacy management processes) which would be seen as externally oriented innovation.

Process: The bank is currently reviewing its privacy policies and practices for two purposes. First, as a governance exercise, Case D is examining how best to coordinate and manage enterprise-wide privacy policies that cut across markets (e.g., retail banking, investment banking or wealth management) and jurisdictions (e.g., Canada, U.S. and U.K). The goal appears to be to achieve a *de facto* enterprise-wide privacy policy that can be successfully applied regardless of market or jurisdiction. Second, it is concerned with the relationship among the organisation's information privacy, information security and information management processes. The goal appears to be a tighter integration of these different yet complementary aspects of managing the information resource. However, the relationship between the bank's information privacy and customer relationship practices appears to be of secondary concern.

Capability: Overall, Case D appears to be attempting to create their information privacy approach as a source of efficiently and internally derived and applied innovation that provides superior customer insight. In other words, there is evidence to suggest that Case D is seeking a customer knowledge capability rather than a customer relationship capability.

In sum, I have shown how the RBV might be used to describe and evaluate Case D's information privacy orientation. It is premature to suggest that there is a definitive RBV stance at the Bank. However, it would be useful to revisit Case D's information management initiative to assess the extent to which the bank continues to move to differentiate itself through a customer knowledge capability.

Chapter Summary

In this chapter, I provided the results of the Case D study. Using a triangulation approach (based on interview, survey and documentary data), I applied the IPO Definition and defined the layers of the IPO Continuum. Then I mapped Case D onto the IPO Continuum. Finally, I considered Case D's information privacy orientation through the competing theoretical lenses and suggested that while their IPO is presently best explained using the institutional approach, the

RBV also offers valuable insights that may point to a future repositioning of information privacy at Case D.

CHAPTER TWELVE

CROSS-CASE ANALYSIS

To this point, I have focused on describing the three case studies I undertook. Now I turn to the cross-case findings. As was outlined in Chapter One, the overarching question driving my research was ***How can we understand the different choices organizations make in the treatment of customer information privacy?*** The case studies I conducted helped to describe the information privacy orientation of three Canadian financial institutions. In this chapter, I specifically address how we can make sense of the observed similarities and differences among the three cases. This chapter addresses the following research questions:

R3) To what extent does the Institutional Approach (IA) help us to explain homogeneity in information privacy orientation across firms in the same industry?

R4) To what extent does the Resource-Based View (RBV) help us to explain heterogeneity in information privacy orientation across firms in the same industry?

In Chapter Five I theorized that both the Institutional Approach and the Resource-Based View of the firm provided useful frameworks for analyzing similarities and differences among firms' information privacy orientations. Recall that privacy legislation in Canada is broad, allowing firms to exercise choice in the development of their privacy programs as long as they address the 10 privacy principles laid out in the statute. In this chapter, I will show that the Institutional Approach is useful in analyzing IPO homogeneity. I also discuss the application of the RBV to one case. There are three sections to this chapter. First, I provide an overview of the relative IPO Continuum placement for each firm (see Table 12-1). Then, I apply the IA framework to explain the similarities among the three firms. Last, I use the RBV framework to consider the different direction in IPO that one firm appears to be taking.

Placing the Case Studies on the IPO Continuum

The three case studies show variance in IPO across all four layers of the continuum, as illustrated in Figure 12-1. The firms are closest in IPO on the Customer Relationship Stance layer. There is greater variance in the Privacy Philosophy and Privacy Behavior layers, with Case B exhibiting weaker IPO than either Case C or Case D. However, the most significant difference

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Adhering to External Codes	Enhanced Privacy
		Case B ***Case C*** ⇨ ***Case D***		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Opportunity
		Case B ***Case C*** ⇨ ***Case D***		
Customer Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		Case B ***Case C*** ***Case D*** ⇨		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			Case B ***Case C*** ***Case D***	
	Weaker ⟷ ***Stronger***			

Figure 12-1: Cross Case Analysis – IPO Continuum

appears with the relative positions on the Customer Information Management Strategy layer. I discuss each layer in turn.

Customer Relationship Stance (CRS)

All three firms are located in the "Shared responsibility" category. Case C was slightly stronger than Case B which, in turn, was slightly stronger than Case D. However, no evidence could be discerned to place any firm in a different CRS position on the continuum. This position means that these firms commonly viewed their obligations to their customers in terms of a mutual responsibility for consumer well-being. This position is characterized as being on the "strong" side of the continuum.

Customer Information Privacy Philosophy (PHIL)

There was no evidence to support placing any of the firms in either the "no awareness" or "privacy as opportunity" positions at this time. All firms were well aware of the existence of the privacy law and its application to the financial institutions industry. As well, they view the law as supportive of their traditions (especially maintaining confidentiality) and as a reassurance they can offer customers ("you can provide this information with confidence that it will be treated appropriately"). However, the cases are positioned differently with respect to the "privacy as constraint" versus "privacy as exchange" positions.

Case B straddles the "constraint" and "exchange" positions. Like the pilot case, Case B views privacy legislation as a "must do," nothing less and certainly nothing more. Privacy success means no complaints and no significant ongoing effort.

Case C and Case D occupy the "privacy as exchange" position." This suggests that neither firm views the predominant implications of privacy legislation as necessarily constraining their ability to pursue their business. There is some limited support for the idea that privacy legislation may support their ability to obtain better information from their customers. These two

cases differ in their interest in pursuing the "privacy as opportunity" position. Case D is not interested in pursuing any publicly visible opportunity position.

Case C appears to be tentatively considering what pursuing a "privacy as opportunity" positioning might entail. Although they are unclear on the operational details, they have not abandoned the notion of possibly doing something innovative within their privacy regime that will confer some advantage, even if only temporarily.

Customer Information Privacy Behavior (BHV)

All three banks do more than simply comply with PIPEDA. Case B adopted an industry Model Privacy Code almost without modification. Case D updated their privacy policy (which was based on a previous industry model code/CSA Model Code). Only Case C conducted a search for alternatives to better suit their perceptions of what privacy actions they ought to offer their customers. I interpret this to mean that all three firms provide appropriate levels of control and procedural justice in their privacy behaviors. In addition, no firm could be considered a privacy leader at this time and no one interviewed necessarily claimed to be interested in actually offering enhanced privacy. In fact, there was considerable discussion at all three firms about why a competitor had apparently pursued this positioning. A few Case C representatives spoke about what being a privacy leader might mean. Case B and Case D staff suggested that "not being leaders" was more in line with their privacy visions.

Case B is positioned slightly weaker than the other two because they did not evaluate and adapt the Model Code; they simply incorporated it in to their operations. At one level, this exemplifies efficiency, but it also underscores the extent to which this was a compliance exercise undertaken to protect the firm as opposed to advancing the interests of its customers. In addition, the information provided to existing customers is well prepared, albeit minimal.

Case D provides a good level of publicly accessible information and undertook some search for alternatives even as it updated its existing Code (at the time that PIPEDA was mandated). The

CPO speaks frequently in public. The firm appears concerned to deliver a message that is more than "we comply."

Case C provides very comprehensive publicly accessible information about privacy, generally, and its privacy program, specifically. They sponsor privacy conferences for their not-for-profit customers, and their CPO has spoken publicly on privacy matters related to the financial institution.

Customer Information Management Strategy (IMS)

The firms differ the most in their information management strategies. While all three firms appear to simultaneously pursue Risk Minimization and Add-Value strategies, the relative emphasis placed on the strategies differs. Case B was primarily concerned to manage risks. Case C, while equally interested in risk minimization, was attempting to become more adept at using customer information for improving customer offerings, especially through the integration of privacy into their Customer Relationship Management (CRM) strategy. Case D likewise had a strong "manage to minimize risk" orientation as well as an "add value" orientation. Case D was the most sophisticated of the three in their ability to harness customer information to improve the customer value proposition.

I interpret that this lack of a definitive positioning on the IMS layer of the continuum may be an industry effect. While I was interested in isolating the firms' primary use for customer information, it appears that financial institutions generally must vigorously pursue both the "Manage to Minimize Risks" strategy (for regulatory, reputation and capital market reasons) and the "Manage with Information to Add-value" strategy (for competitive and customer satisfaction reasons). Currently, no firm was pursuing a "Manage with Information to Create New Reality" posture. However, I discuss this position in terms of Case D and the Resource-Based View later in this chapter.

In summary, while the three cases are all compliant and offer more than a minimal privacy program, they vary in the strength of their privacy commitment, as demonstrated by their different positions on the IPO continuum. I now apply the Institutional Approach to explain these IPO positions.

Institutional Theory and IPO: Explaining Similarities

My research demonstrates that the IPO for all three firms can be explained by the Institutional Approach. Table 12-1 identifies the different elements of the theory and their application to Information Privacy Orientation. These elements adapt Oliver's (1991) typology (explained in Chapter Five). In this section, I apply the Institutional Approach to the three cases by examining their respective organizational goals, sources of pressure, ability and willingness to respond to pressure, and response strategies.

Table 12-1: Institutional Approach and IPO

Element	**Institutional Approach**	**Information Privacy Orientation Application**	
		Weaker IPO	***Stronger IPO***
Organizational Goal	Survival through the search for legitimacy	• Pragmatic • Managerial	• Social • Technical
Source of pressure	• Cause (threat) • Constituency • Content • Control • Context	• Efficiency • Dependence • Constraint • Coercion • Uncertainty	• Legitimacy • Multiplicity • Consistency • Diffusion • Interconnectedness
Ability and willingness to respond to pressure	Influence of social network	Embeddedness	Agency
Responses to pressures	• Acquiescence • Manipulation	• Acquiescence (compliance with legal model) • Imitation of minimalist organizations	• Manipulation (impression management) • Imitation of benchmark organizations

Organizational Goal

In Chapter Five I argued that firms operating within an institutional frame pursue survival through the search for legitimacy as their organizational goal. Recall that legitimacy was defined as "a generalized perception or assumption that the actions of an entity are desirable, proper or appropriate within some socially constructed system of norms, values, beliefs and definitions" (Suchman 1995: 574). In general IPO terms, this is translates into an organizational goal of defending reputation or managing reputation risk. Table 12-2 presents the summary of evidence and interpretation for each firm.

Table 12-2 shows that each case pursued the organizational goal of legitimacy, chiefly expressed as compliance with PIPEDA. The cases were very similar in how they implemented their privacy programs, with the following exceptions. Case C pursued ethical objectives almost as vigorously as they did legal ones, thereby having somewhat stronger social legitimacy. While Case B undertook the minimum changes in operations to comply with the law (managerial legitimacy), both Cases C and D pursued technical legitimacy through extensive changes to business processes. Case C made changes largely in support of their privacy compliance, while Case D increasingly used privacy to complement other information management initiatives.

In summary, there is evidence to support my theorizing that these firms pursued legitimacy in the implementation of their privacy programs. All three pursued a combination of pragmatic and social legitimacy while one constrained its activities to managerial legitimacy and the other two concerned themselves with technical legitimacy.

Table 12-2: Summary of Evidence for Organizational Goal (IA)

Organizational Goal: Survival through the search for legitimacy	Findings: Case B	Findings: Case C	Findings: Case D
Evidence	Legal compliance overarching privacy objective (P)	Legal and Ethical objectives of primary importance (P, S)	Legal compliance overarching privacy objective (P)
	Minimum changes in operations to comply with law (M)	Thorough review(s) and significant changes to operations, primarily privacy related (T)	Thorough review(s) and significant changes to operations, increasingly information management related (T)
	Some willingness not to pursue certain activities for fear of customer reprisal (P)	Some willingness not to pursue certain activities for fear of customer reprisal (P)	Some willingness not to pursue certain activities for fear of customer reprisal (P)
	Compliance concerns expressed as "reputation risk' (P, S)	Compliance concerns expressed as "reputation risk" as well "customer expectations" (P, S)	Compliance concerns expressed as "reputation risk" as well "customer expectations" (P, S)
	Legitimacy appeals through adoption of Model Code that should satisfy legal and customer expectations (P, S)	Legitimacy appeals through creation of stringent Code that should satisfy legal and customer expectations (P, S)	Legitimacy appeals through creation of stringent Code that should satisfy legal and customer expectations (P, S)
Exemplar quote	"Make privacy a non-issue"	"Privacy is the right thing to do"	"Demonstrate that we are a compliant organization"
Interpretation	• **Pragmatic** ⇨ Social • **Managerial**	• Pragmatic ⇨ **Social** • **Technical**	• **Pragmatic** ⇨ Social • **Technical**

Note: P= Pragmatic legitimacy; M=Managerial legitimacy; S=Social legitimacy; T=Technical legitimacy

Source of Pressure

Another element of the Institutional Approach that pertains to IPO homogeneity is the source of the pressure to implement a privacy program. Recall that I had adapted the five sources identified by Oliver – cause, constituency, content, control and context. Table 12-3 presents the summary of evidence and interpretation for each firm.

Table 12-3: Summary of Evidence for Source of Pressure (IA)

Source of pressure	Findings: Case B	Findings: Case C	Findings: Case D
Cause: why do organizations perceive pressure to conform?	Primarily Legitimacy: PIPEDA	Primarily Legitimacy: PIPEDA	Primarily Legitimacy: PIPEDA
Constituency: who is pressuring?	Primarily Government (no apparent internal demand)	Primarily Government, some internal (social audit, transparency & accountability in business practices)	Primarily Government (no apparent internal demand)
Content: what norms are to be adopted?	Norms as represented by PIPEDA principles Not inconsistent with prevailing corporate norms	Norms as represented by PIPEDA principles Strongly consistent with prevailing corporate norms	Norms as represented by PIPEDA principles Consistent with prevailing corporate norms (already had a privacy code)
Control: how is pressure brought to bear?	Voluntary + Legal coercion (implemented prior to 2004)	Voluntary + Legal coercion (implemented privacy 2001 when others said not until 2004)	Voluntary + Legal coercion (model code since 1998)
Context: what is the environment from which the pressure emanates?	Environmental interconnectedness: Financial institutions industry as well as particular segment of the industry (same trade association as Case C)	Environmental interconnectedness: Financial institutions industry as well as particular segment of the industry (same trade association as Case B)	Environmental interconnectedness: Financial institutions industry as well as particular segment of the industry (different trade association)
Exemplar quote	"We obey the law."	"It's the law."	"We are a compliant organization."
Interpretation	Overwhelmingly the source of pressure was the federal privacy statute.	Overwhelmingly the source of pressure was the federal privacy statute.	Overwhelmingly the source of pressure was the federal privacy statute.

Table 12-3 shows that the source for pressure to develop and implement a privacy program (in other words, to conform) was the Canadian government's passing of PIPEDA. In all three cases, the pressure came from the federal government, and the content was the statute (i.e., ten privacy principles within the schedule). There were two apparent differences in how firms responded. First, in all three cases, the firms both responded to legal coercion and behaved voluntarily, for very similar reasons. Case B voluntarily adopted their privacy program prior to the PIPEDA deadline of January 2004 for two reasons. The firm had to respond to another legal

requirement (Anti-Money Laundering legislation) and decided to pursue both implementation projects simultaneously. They also thought that implementation would go smoother and that the learning curve could be managed easier if they did not have to rush implementation. Case C, while part of the same trade association as Case B, decided that they were, in fact, to be compliant by 2001. They initiated a significant enterprise-wide effort and declared themselves compliant by 2003. In this way they "volunteered" to be "legally coerced." Case D had implemented a voluntary Privacy Code in 1998 based on an industry Code that had been developed in the wake of the CSA Code process. However, the firm had to make changes to their voluntary code to meet the revised requirements set out in PIPEDA, thus having to respond to legal coercion.

The second difference is the environmental context of the pressure. Cases B and C belong to the same trade association and are considered among its leaders. This part of the Canadian financial institution sector is highly integrated in terms of systems, suppliers and governance. There tends to be a great deal of cooperation among the firms who do not regard each other as competitors because they operate in different locales. This level of integration severely limits the ability to behave independently with an issue of legal consequence. On the other hand, Case D is similarly located in a highly interdependent environment which explains, to some extent, their voluntary adoption of the Privacy Code in 1998. Most other significant actors in their environment were making similar decisions. The national banking system as a whole requires this level of interdependence in order to function efficiently.

In summary, there is strong evidence to support my theorizing that there was a common source of pressure to conform by implementing a privacy program. The source of the pressure was the federal government's requirement that all firms comply with PIPEDA. The only real difference among the firms was their perception of when they were required to comply.

Ability and Willingness to Respond to Pressure

The third element of the Institutional Approach that pertains to IPO homogeneity is the ability and willingness of firms to respond to coercive pressure. I theorized that the strength of IPO would be related to a firm's approach to crafting their response. Table 12-4 presents the summary of evidence and interpretation for each firm.

Table 12-4 shows that the three firms had different abilities and levels of willingness to respond to the pressure to develop an information privacy program. Part of the explanation comes from the extent to which the firms were embedded in their social networks, and part comes from agency explanations. I also argue that part of the explanation comes from the perceptions of the ability and willingness based on who was championing the privacy case in the respective firm.

Table 12-4: Summary of Evidence for Ability and Willingness to Respond to Pressure (IA)

Ability and willingness to respond to pressure: Influence of social network	Findings: Case B	Findings: Case C	Findings: Case D
	Desire to minimize resource consequences – i.e., Part time positions, no dedicated budget (E)	Commitment of significant human and financial resources to ongoing privacy issue (A)	Commitment of significant human and financial resources to ongoing privacy issue (A)
	Reliance on Model Code, no search for independent alternatives (E)	Independent Development of Code based on search for alternatives (A)	Adaptations to existing Code (E)
Influence of Chief Privacy Officer (CPO)	Narrow view of issue as an "audit" issue	Broader view of issue as a "business issue" with potential for positive outcomes	Broader view of issue as a "business issue" with potential for positive outcomes
Exemplar quote	"This is a compliance issue"	"This is a significant business issue"	"We are trying to take a holistic and integrated approach"
Interpretation	Embedded	Agency	Agency

Note: E=embedded; A=agency.

Case B was firmly embedded in their social network (through the national trade association). The bank used the voluminous materials provided by their trade association and followed the recommendations very closely. The Board of Directors adopted policies without

changes and with little discussion. The privacy "champion" (subsequently appointed the Chief Privacy Officer) was the Senior Manager for Audit and Compliance, who took a narrow view that privacy, while important, was mainly a matter of implementing and complying with a defined set of rules. I interpret this as Case B's being embedded as a firm within an environment that did not choose to expand the notion of privacy beyond its narrowest legal implications. This view fit with and was reinforced by the CPO's training and orientation as an audit and compliance manager.

Case C, while as firmly embedded in the same social network as Case B, asserted agency in the development and deployment of their privacy program. More resources were accorded the privacy project and a greater effort was embarked on to raise the level of awareness among staff and customers. The privacy champion in this firm happened to be the Vice President for Business Development, who assumed the role of CPO in order that the issue not be relegated to a mere compliance initiative. He indicated that privacy was a "significant business issue" that deserved and was receiving strong and sustained organizational attention. Thus, Case C demonstrated agency in not simply following the models and recommendations of the trade association. At the same time, by appointing a CPO with a new business orientation, privacy was elevated to position of greater importance to the organization.

Case D is another example of embeddedness within a social network, but one that is predominantly internal to the firm. This bank had operated with a Privacy Code for several years before having to comply with PIPEDA. To the extent that the firm adapted their existing Code without significant consultation beyond the boundaries of the firm, this suggests a decision to be restricted in compliance. However, the CPO is a very senior executive who requested responsibility for the privacy portfolio because of a combination of background, skills and interest. Significant resources were allocated to the initiative largely because of the attention that this senior individual could bring to the issue. This firm continues to update their privacy program and does not necessarily following compliance models that have been implemented by competitors (and members of the same trade association).

In summary, there is strong evidence to support my theorizing about the impact of social networks on the approach to developing privacy programs. Case B is an example of an embedded firm that assumed a narrow compliance posture. Cases C exercised agency and developed broader programs that addressed privacy as a "significant" and "enterprise-wide" initiative. Case D took a similar approach to Case C in practical terms but operated within an embedded, social network bounded by the firm. I extended this analysis by suggesting that each firm's privacy champion was instrumental in the definition of its privacy program.

Response to Pressure

This is the final element of the Institutional Approach that I theorize assists us in understanding how firms are similar in information privacy orientation. While Oliver argued that firms could choose from a repertoire of five possible responses, I identified two responses to support information privacy orientation. Table 12-5 presents the summary of evidence and interpretation for each firm.

Table 12-5 shows that all three firms primarily adopted acquiescence responses. This is not surprising given that regulated financial institutions are not in the habit of flouting the law. Each firm appears to have adopted this response primarily to reduce the likelihood of negative responses from important stakeholders, including regulators and customers. Only one firm, Case B, engaged in what could be described as "mimetic isomorphism" by adopting the policies and procedures suggested by the national trade association almost without exception. The privacy initiative was carried out as a project which was declared largely completed at the time of initial implementation.

Table 12-5: Summary of Evidence for Responses to Pressure (IA)

Responses to pressure	Findings: Case B	Findings: Case C	Findings: Case D
	Mimetic isomorphism: Reliance on Model Code, no search for independent alternatives		
	Concern not to look different from other financial institutions (reduce likelihood of negative responses)	Some aspirations to privacy leadership but remain concerned not to be too far out of step from peers (reduce likelihood of negative responses)	Concern not for privacy leadership per se but to be really focused "to do things right" (reduce likelihood of negative responses)
	Provide sufficient information to demonstrate compliance	Provide as much information as possible to demonstrate compliance and create positive impression	Provide sufficient information to demonstrate compliance
Exemplar quote	"Privacy project is complete"	"Ongoing business concern"	"Not an end state, always more we can do"
Interpretation	Acquiescence	Acquiescence + Manipulation	Acquiescence + Manipulation

Both Case C and Case D took a predominantly acquiescent approach, although with somewhat more independence. Both engaged in "impression management" to strengthen their public privacy profile. Case C supported publicly visible privacy activities, such as privacy conferences. Once Case D perceived that they had achieved satisfactory compliance, they focused not on being seen to be different from peers but to be seen to be "doing things right," partially through the CPO accepting public speaking engagements.

The Case C findings offer an alternative explanation. Recall that in Chapter Five, I argued against the inclusion of the "proactive" institutional response strategy proposed by Cashore and Vertinsky (2000). However, it appears that this strategy may be the best explanation for Case C's simultaneous pursuit of privacy "leadership" but not "privacy as a strategic differentiator." I explore this issue in more depth in the concluding chapter.

In summary, the predominant response strategy pursued by the firms can be characterized as "acquiescence." Case C and Case D also appear to have engaged in some impression management.

Section Summary

I have demonstrated how, despite apparent differences as captured on the IPO Continuum, the Institutional Approach serves as a useful framework for explaining Information Privacy Orientation. Table 12-6 summarizes these findings. In the next section, I discuss the applicability of a contrasting theoretical framework, the Resource-Based View of the firm, to a consideration of why firms might pursue significantly different approaches.

Table 12-6: Summary of Cross Case Analysis – IPO and the Institutional Approach

Element	**Institutional Approach**	**Information Privacy Orientation Application**	
		Weaker IPO	***Stronger IPO***
Organizational Goal	Survival through the search for legitimacy	Case B Case C Case D	
Source of pressure	Cause		Case B Case C Case D
	Constituency	Case B Case D	Case C
	Content	Case B Case C Case D	
	Control	Case B Case C Case D	
	Context		Case B Case C Case D
Ability and willingness to respond to pressure	Influence of social network	Case B Case D	Case C
Responses to pressures	• Acquiescence • Manipulation	Case B Case C Case D	

Resource-Based View and IPO: Explaining Differences

Case D presents an opportunity to examine the potential for the RBV to explain IPO heterogeneity. I do not claim that this bank is currently pursuing a privacy approach that is sufficiently different to place them outside the IA explanatory framework. However, Case D appears to have reached a decision point. They have concluded that the ongoing privacy efforts should enter a new phase. Their "privacy project" per se is concluded. In contrast to Case B, which chose to halt resource expenditures on additional privacy initiatives after the project was concluded, Case D continues to pursue three streams of privacy related activity. One stream is the effort to embed, routinize and automate privacy processes wherever possible. Another stream is to implement an updated governance framework and give thought to the structure of the privacy program and emerging issues such as how it deals with trans-jurisdictional privacy issues. The third stream involves an information management initiative that combines the efforts of three of the firm's key information players – the Chief Privacy Officer, the Chief Information Security Officer, and the Information Resource Management Officer. This initiative has been established to develop the information capability that, it is hoped, will deliver improved performance across the enterprise. (The initiative is not limited to retail banking.) An important aspect of this initiative is the declaration by several interviewees that "this is not about technology, it's about business."

I will use the four elements of the RBV framework - Organizational Goal, Resource, Process, and Capability (as shown in Table 12-7) to examine the relationship between Case D's information management initiative and their information privacy positioning. I will demonstrate that Case D is beginning to consider how to leverage information privacy into a different operational dimension – that is, although they do not "Manage with Information to Create New Reality" (a category contained in Figure 12-1), they are nonetheless grappling with some of the

inherent possibilities. Note that there is insufficient empirical evidence to categorize the initiative as representing weaker or stronger IPO.

Table 12-7: Resource-Based View and IPO

Element	Resource-Based View Approach	Information Privacy Orientation Application	
		Weaker IPO	*Stronger IPO*
Organizational Goal	Sustainable Competitive Advantage	Strategic differentiation based on superior customer insight	Strategic differentiation based on superior customer trust
Resource	Customer Information as Level 3 resource	Support efficiency focused internal innovation	Support effectiveness focused external innovation
Process	Privacy policies and practices	Information Privacy as an intellectual/knowledge management practice	Information Privacy as a social/relationship management practice
Capability	Information Privacy as a source of information and innovation	Customer Knowledge Capability	Customer Relationship Capability

Organizational Goal

The overarching organizational goal within the RBV framework is the attainment of Sustainable Competitive Advantage (SCA) through fundamental strategic differentiation. Currently, Case D does not differentiate on the basis of privacy, and they are unlikely to do so in future. ("We're in the middle of the pack and that suits us.") At the same time, the bank is attempting to become more "customer-centric" and the information initiative is one effort to support this positioning. As a result, the information initiative must take customer information privacy into consideration (otherwise the customer-centric positioning becomes open to information abuse). Figure 12-2 shows the balance that information privacy brings to the information initiative. Information Privacy operates as a brake, slowing momentum to ensure that issues are addressed. It also operates as a filter through which uses of customer information may be tested.

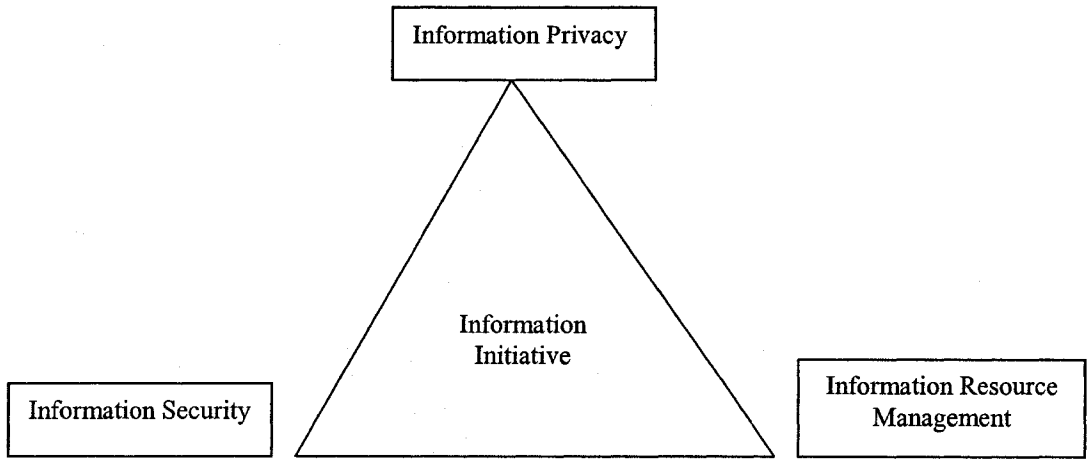


Figure 12-2: Information Initiative

This suggests that information privacy on its own will not likely be a source of sustained competitive advantage for Case D. However, it does offer the opportunity to consider the mutually reinforcing effects of the "information triumvirate" (as it is dubbed by the CPO). Information privacy may not by itself be sufficient for sustaining competitive advantage in Case D. However, there is evidence to suggest that it is a necessary consideration if the firm hopes to achieve SCA through its information initiative.

It is premature to presume to suggest whether the SCA will be in the form of "superior customer intelligence" or "superior customer relationships" as I theorized in Chapter Five. However, the relationship that appears to exist between information privacy practices and the willingness of customers to provide information is important. The Chief Privacy Officer articulated the relationship as a virtuous circle: the more times the firm is able to demonstrate its trustworthiness through good information privacy actions, the more clients are be able to trust the firm, and, as a consequence, the more willing they are to provide more and better quality (meaning commercially useful) information. My inclination at this stage is to suggest that the firm is more interested in leveraging the information than in the relationship itself.

In summary, there is some support for the idea that the information privacy can be used as an enabler of Sustainable Competitive Advantage.

Resource

Case D personnel appear to identify customer information as a very valuable resource for the firm. Currently, customer information appears to operate as a Level 2 resource – it provides information that is primarily useful for improving marketing offerings. However, some of the "information initiative" personnel view customer information as more in line with a Level 3 resource. At this point, I could not characterize the focus of the Level 3 resource as internal or external. However, the kinds of uses for the information using advanced data mining and other analytical techniques were based on the ability to assess huge amounts of very detailed transactional information to produce complete financial profiles for customers and offer a wide range of products and services tailored to specific needs. The ability to engage in this level of activity, however, is as much a function of privacy safeguards and knowledgeable consent as it is of advanced information technologies.

The need to preserve the integrity of the information and, hence, to provide customers with strong privacy assurances, goes to the heart of the value of the customer information resource to the firm. Several interviewees characterized the value of the resource as "inestimable", "huge", and "everything". Others characterized customer information as a firm asset that simply has yet to be valued. Both characterizations were made with the understanding that the firm had adopted the position that the personal information was owned by the customer. The ability to create new sources of value for the customer and wealth for the firm depends to a great extent on the firm's ability to properly value the resource.

In summary, the opportunity to leverage the customer information resource will depend to a great extent on the firm's ability to deploy information exploiting technologies within a privacy environment that maintains the value of the information for both the firm and the client.

Process

The firm is at the very early stages of the information initiative. There is no evidence to support any characterization of the processes that the firm intends to pursue. However, given the interdependence of the financial institutions industry, some of the challenge of creating a single client identifier that would contain key information and privacy consents is being addressed through an industry committee of the national trade association. Case D is extensively involved with this activity.

Capability

I argued in Chapter Five that Information Privacy could serve as a capability in the firm. This capability could be deployed either as a customer knowledge capability or a customer relationship capability. I expect that the information initiative will develop and subsume any privacy capability. Despite the apparent commitment to the "customer-centric" positioning, there is little evidence to suggest that the information initiative will operate to sustain relationship capabilities as much as it will support the knowledge capability. The influence of executives such as the CPO may be instrumental in assisting the firm to find an appropriate balance.

In summary, the process and capability elements of the RBV framework are underdeveloped with respect to Case D since the firm is in the early stages of its information initiative.

Section Summary

I used the RBV framework to consider how Case D may be beginning to differentiate itself through an information management initiative. The role of information privacy appears to be an enabler of this initiative. As such, the development of an information privacy capability may offer important support for achieving sustainable competitive advantage through this initiative.

Chapter Summary

In this chapter I reviewed the competing theoretical explanations for IPO homogeneity and heterogeneity in response to research questions R(3) and R(4). I showed that the Institutional Approach provides a suitable lens through which to consider the Information Privacy Orientations for the three cases I researched, and I used Case D to illustrate how the RBV might be used to explain differences in IPO. I now turn to the concluding chapter which considers the contributions and implications of this research.

CHAPTER THIRTEEN

CONCLUSIONS

I opened Chapter One of this dissertation with a quote from a research firm that argued that concerns for information privacy would place *"once-routine business practices under the microscope"* (Forrester Research 2001)[1]. My exploratory research into the customer information privacy orientations of three Canadian financial institutions provides some insight into what my "microscope" revealed. This chapter has four sections. First, I discuss my research findings. Second, I identify the implications of this dissertation for researchers and managers. Third, I discuss the study's limitations. Finally, I identify its contributions.

Dissertation Findings by Research Question

In this section I discuss the dissertation findings according to the specific research questions (R1 – R6) I used to frame this research. Included in the discussions are future research opportunities. Table 13-1 summarizes the dissertation findings and additional research requirements.

R1: Do Firms Have an Information Privacy Orientation?

The response to the question of whether I was able to identify an "Information Privacy Orientation" is a definite yes. This dissertation demonstrated that there is support for the broad proposition that Information Privacy Orientation exists as an organizational phenomenon. Furthermore, even within a highly regulated industry (financial institutions) operating under a specific legal privacy statute (Canada's PIPEDA), there was room for firms to choose their responses. The Privacy Policy Evaluation Study carried out as Phase One of this research program showed a range of approaches to customer information privacy. The Phase Three field research showed that while the four case sites(pilot and three main cases) themselves might

[1] As quoted in Cavoukian and Hamilton 2002: 91.

Table 13.1: Summary of Dissertation Findings and Future Research Opportunities by Research Question

Research Question	Findings	Future Research
1. Do firms have an Information Privacy Orientation?	• Demonstrated. • Phase One – Privacy Policy Evaluation Study: ten firms displayed different approaches to customer information privacy. • Phase Three – Field Research (Case Studies): four firms displayed variance in "principles, values, decisions rules, policies and desired objectives."	• Case studies suggested a "stages" model for information privacy. • Information privacy "stages" model needs to be refined (i.e., what are demarcation points between stages? Are firms consciously making decisions to move to different stages?) • Stages model needs to be assessed across a broader sample of industries, firms and jurisdictions. • IPO Typology requires further refinement.
2. Is Information Privacy Orientation constructed as I have theorized?	• Partly demonstrated. • Evidence of customer relationship stance, information management strategy, privacy philosophy, privacy behaviors. • Mixed evidence to support horizontal classification within each component. • Mixed evidence to support vertical relationships among components. • Revised definition.	• Requires further analysis. • Three models to be considered: 1. "Vertical Logic" model – strong vertical relationships connect the four layers. 2. "Horizontal Independence" model – greater independence among the layers. 3. "Grouped" model – customer relationship stance and information management strategy are connected strongly and relate as a group to the strongly connected privacy philosophy and privacy behaviors layers. • Need to investigate relative strength of the different layers.
3. To what extent does the Institutional Approach help us to explain homogeneity in information privacy orientation across firms in the same industry?	• Demonstrated. • The Institutional Approach (organizational goals, sources of pressure, ability and willingness to respond to pressure, and response strategies) can be applied to explain IPO in firms within the same industry.	• Requires further case studies of industries and firms collecting and using less "sensitive" personal information. • Specific investigation into information privacy as a source of legitimacy, both at the firm and industry/sector levels. • Further investigation of the competing versus complementary aspect of these theoretical approaches in different industries and firms.

4. To what extent does the Resource-Based View help us to explain heterogeneity in information privacy orientation across firms in the same industry?	• Partly demonstrated. • Case D presented evidence to suggest that RBV might be useful. • Suggests that Information Privacy Orientation might serve as an enabler for information management initiatives to become a source for sustained competitive advantage.	• Requires further case studies of industries and firms collecting and using less "sensitive" personal information. • Specific investigation into information privacy as an information management enabler. • Further investigation of the competing versus complementary aspect of these theoretical approaches in different industries and firms.
5. What is the effect of the firm's overall context (external and internal environment) on its Information Privacy Orientation?	• Not specifically tested in the thesis research. However, there is evidence to support a relationship between antecedent variables and IPO. • Variables appear to include: national culture (ownership of customer information), regulatory environment (existence of statute), and industry practice (codes of practice, concern to appear to conform); strategic positioning (perceptions of leadership), market orientation (customer centric), and slack resource availability (no frills versus ongoing budget), organizational culture (compliant culture), ethical climate (is privacy defined as an ethical issue), interfunctional values (where privacy responsibility is located), and top management preferences (privacy governance approach). • Potential additional variable: technology strategy (such as deployment of CRM).	• Further analysis of collected data to specifically identify relationship between antecedents and IPO continuum positioning. • Development of coding schema for individual variables. • Development of "technology strategy" variable.
6. What is the effect of IPO on firm performance?	• Not specifically tested in the thesis research. Some evidence to support a relationship between IPO and outcomes. • Variables appear to include: intellectual capital (quality and quantity of customer information), trust (enables customers to divulge additional information), and reputation (operates as a brake on organizational excesses). Possible indirect relationship to financial outcomes.	• Further analysis of collected data to specifically identify relationship between IPO Continuum positioning and outcomes, both desired (articulated) and unforeseen (unarticulated). • Development of coding schema for individual variables.

not refer to IPO specifically, there was strong evidence that each had "principles, values, decisions rules, policies and desired objectives" that collectively described their approaches to the collection and use of customers' personal information. What I called "IPO", the firms were more likely to refer to as their "privacy project," "privacy program," or "privacy policies and procedures."

There were two additional and unanticipated findings related to the first research question. First, the case study firms appear to represent three different stages of privacy program development. Second, these stages appear to be the result of decisions made at key points. Figure 13-1 illustrates how the firms in this study appear in relation to a basic privacy stages model. A pattern that seemed to indicate the presence of a "Stages" approach emerged when I considered the different levels of "privacy sophistication" within the four firms (the pilot site is included in this observation). Case A (pilot study) was at an early stage of development in their privacy program. They were asking basic questions about "how do we manage our immediate exposure" and undertaking immediately obvious tasks such as drafting basic statements to place on the website, establishing the business case (objectives, processes, resource requirements, etc.), and assembling a privacy team to carry out the broad initiative focused on achieving basic compliance with the privacy statute. The key motivation for the firm was to comply with a minimum of cost, disruption and exposure to the firm. Case B had completed its "privacy project" and had moved into a maintenance mode. It had successfully implemented the trade association's Model Privacy Code and did not feel compelled to undertake additional activities (unless they could be seen to minimize legal exposure). Case C was also compliant, but appeared to have determined that mere compliance was no longer a satisfactory goal. They were actively pursuing ways of harnessing privacy to other organizational objectives. Finally, Case D appears to have moved to a completely different set of questions. Having achieved an initial set of organizational goals, they assume privacy to be largely in place. However, they seem to be hovering at the entry to a potential third

stage in which privacy moves from being a focus in its own right to becoming an enabler of other organizational activities.

	Stage One: Meet Privacy Legal Objectives	**Stage Two: Meet Privacy Organizational Objectives**	**Stage Three: Recast Privacy Role in Organization**
Example of Objectives by stage	1. Legal Compliance 2. Technological security	1. Compliance / Security (assumed) 2. Ethical 3. Social	1. Compliance / Security (assumed) 2. Business
Visibility	1. Internal focus 2. Minimize external expectations	1. External focus 2. Meet external expectations	1. Internal focus 2. Leverage privacy as organizational enabler
Key Decision	Can we / do we desire to achieve other outcomes beyond compliance? If "NO" → maintain status quo If "YES" → Move to Stage 2		Can/ how can privacy activities be harnessed to improve other organizational processes? If "NO" → maintain status quo If "YES" → Move to Stage 3
Exemplar Firm	**Case A** **Case B**	**Case C**	**Case D**
Potential Theory Base	Institutional Approach		RBV

Figure 13-1: Privacy Stages Across the Cases

This "stages" model for information privacy requires further investigation. Clearly, a multiple case study is not generalisable. More research is required to assess the applicability of a stages approach across a range of industries and firms. As well, the stage demarcation points need to be addressed. Of particular interest would be the extent, not only of the existence of stages/demarcation points but also of whether firms are conscious of these? To what extent are firms deliberately and knowingly following a programmed approach to privacy program development?

In summary, this research has established that Information Privacy Orientation is an identifiable organizational level phenomenon. However, IPO might be manifested in different ways depending on the stage of IPO in a firm. This is an area that requires further research.

R2: Is Information Privacy Orientation Constructed as I Have Theorized?

The response to this research question is a qualified yes. This dissertation demonstrated that firms did have various and, to certain extents, discernibly different customer relationship stances, information management strategies, privacy philosophies and privacy behaviors. Chapter Twelve (Cross-Case Analysis) identified and discussed the similarities and differences among the firms on each layer. I believe that part of the explanation for the similarities is that all the firms are financial institutions, thus a tangible industry effect is discernible. Overall, financial institutions appear generally to characterize their customer relationship stance as a "shared responsibility"; jointly manage customer information to "minimize risks" and to "add value"; view privacy legislation not necessarily as a "constraint" but only somewhat as an "exchange"; and while doing more than "minimally comply", vary somewhat in the strength of their "adherence to codes".

However, four questions remain unanswered by this initial research. First, is there a particular vertical logic to the model? Figure 13-2 illustrates the opposing models. The first model (Model 1: Vertical Logic) suggests that the four layers of the IPO continuum connect up through the discrete positions. By triangulating the IPO Survey, interview and documentary data, I was able to construct the IPO Continuum to hold to a vertical logic. That is, my original conceptualization of IPO as a set related layers (Model 1) was partially demonstrated. The positions on each layer (corresponding to a sub-construct of IPO) roughly corresponded. For example, the third position "Shared Responsibility" on the Customer Relationship Stance was connected to position 3 in subsequent layers).

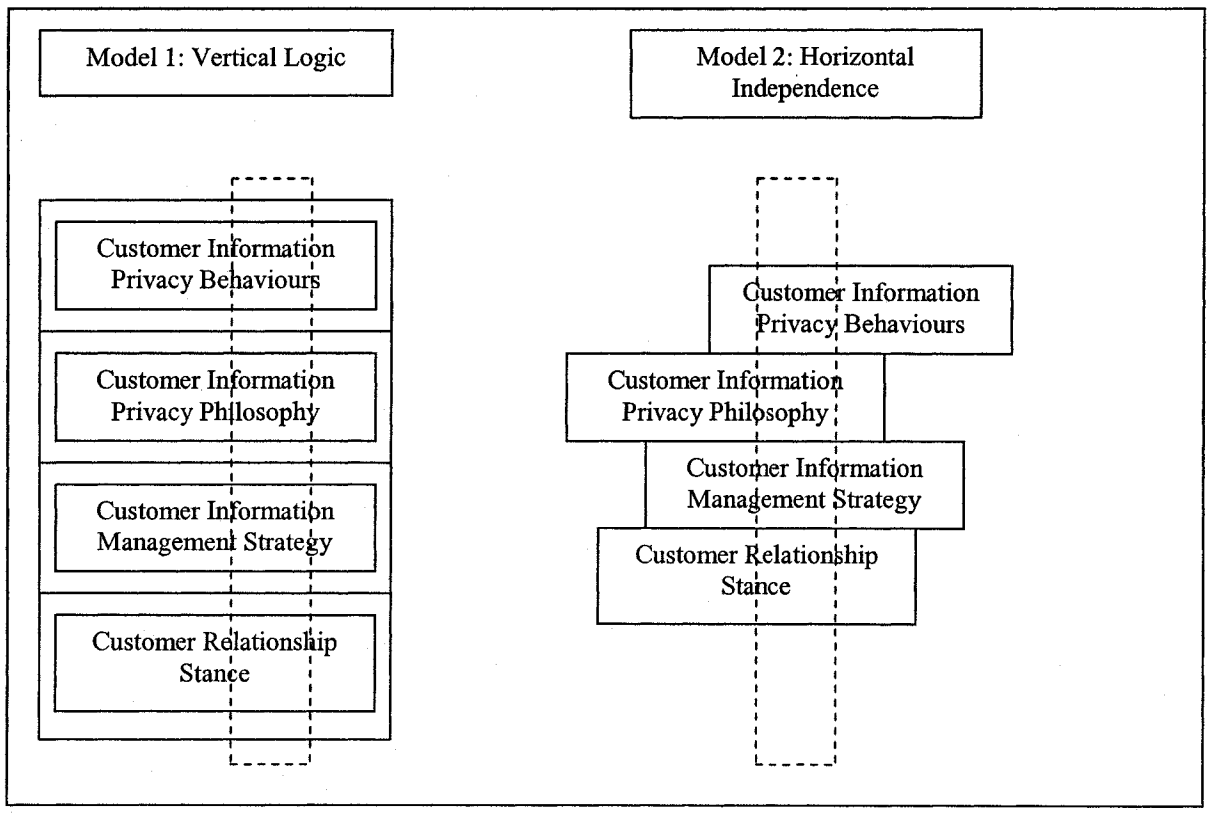


Figure 13-2: Competing IPO Models (1)

However, Model 2: Horizontal Independence may also be viable. In such a case, the layers would act with greater independence and firms would hold positions on one layer that would not necessarily correspond to the same position on a different layer. There was some evidence that, for example, using IPO Survey data alone might deliver this result. The challenge of this model would be to interpret mixed findings (i.e., findings that mixed weaker and stronger positions) in order to categorize a firm's IPO. However, I would expect that industry effects would play a role in every model, thus supplying the unique vertical logic within a given collection of firms that would help to explain variations within the horizontal placements.

The second challenge is to improve the understanding of the positions within the separate constructs, that is, the horizontal logic. As discussed above, there appears to be an industry effect operating so that discrete positions on each layer were sometimes difficult to discern. The issue is to be able to more authoritatively describe the positions and their effect as indicators of IPO

strength. Only additional research using both an expanded sample of financial institutions as well as companies in other industries will provide further insight.

Consequently, there are is another potential model for IPO as illustrated in Figure 13-3.

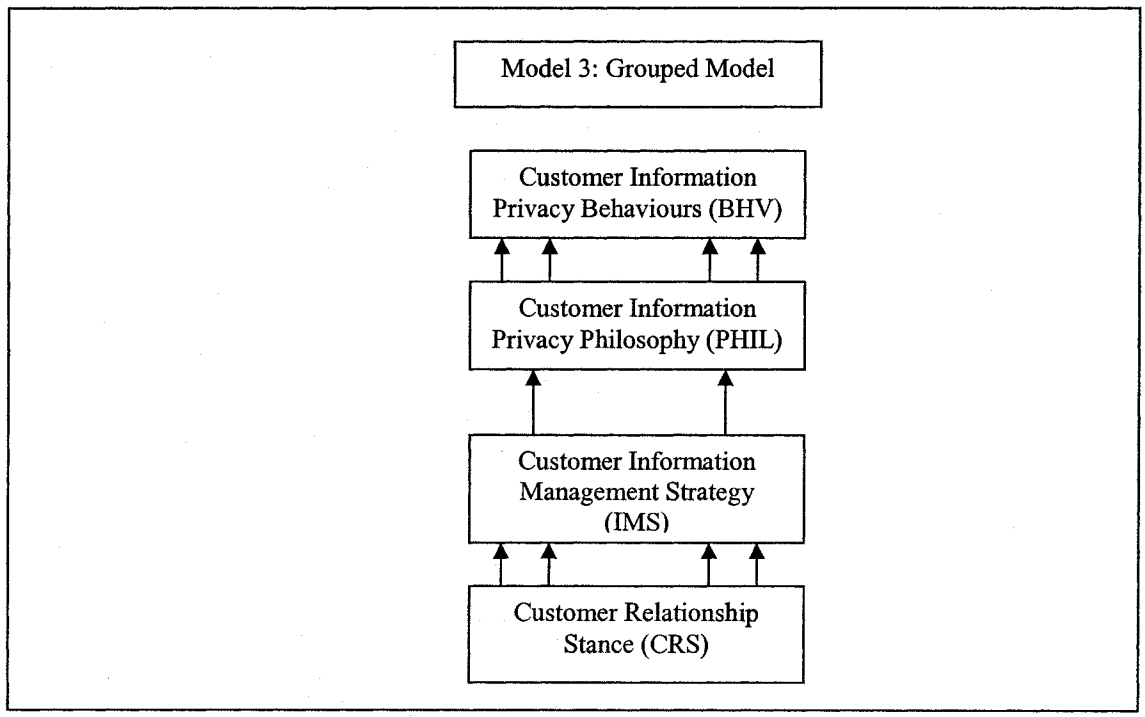


Figure 13-3: Competing IPO Models (2)

This third or "grouped model" argues that the four sub-constructs are actually two sets of related components. Customer Relationship Stance and Customer Information Management Strategy form one group, and Customer Information Privacy Philosophy and Customer Information Privacy Behaviors form a second group. I thank a committee member for suggesting that I consider that Customer Relationship Stance and Customer Information Management Strategy are "large" components (i.e., relate to more than simply information privacy) while Customer Information Privacy Philosophy and Customer Information Privacy Behaviors are "smaller" components (i.e., relate specifically to information privacy).The research issue for this third model would involve establishing a tight connection between, for example, a "shared responsibility" customer relationship stance and an "add value" information management

strategy. Interestingly, this model might serve to demonstrate the Resource-Based View (RBV) in action in an information privacy context. For example, the capability to implement processes that tightly link CRS and IMS and those that tightly link PHIL and BHV may be a source of sustainable competitive advantage (more than a reflection of institutional constraints).

Third, and regardless of the model selected, there is a need to consider the relative strength of the different layers. In my triangulation approach, I was able to balance the strength of the different sources for evidence. For example, I used the qualitative data to supplement the survey findings and so did not "privilege" the quantitative data. However, I did not consider the strength of the individual layers of the continuum and how they contributed to the overall IPO. For example, I did not assess whether the privacy philosophy, overwhelmed the customer relationship stance in a firm. I treated all the layers as equal and this may not be the best way to develop the firm's position. This is another opportunity for further research.

A final issue involves the relationship between the IPO Definition and the IPO Continuum. Committee members had challenged me at various stages of the process to both clarify the phenomenon and more strongly link the definition to the continuum. I revisited a variety of literatures and concluded that the definition I had been using accurately described the process I had engaged to investigate the firms' privacy behaviours. Therefore, I revised the IPO definition as follows:

> *Information Privacy Orientation characterizes an organisation's disposition with respect to how it protects its customers' personally identifiable information.*

This is the short version of the revised definition. The explanatory version expands the definition to specifically identify the four components that constitute the IPO Continuum, specifically

> *Information Privacy Orientation (IPO) characterises an organization's disposition to deliver consistent, transparent privacy protection to its customers. The privacy protection afforded customers is composed of an organisation-wide expression of its ethics-based customer relationship stance, predominant strategy for using customer information, articulated response to external pressures for customer information privacy, and the customer information privacy policies that are manifest throughout the organization.*

This definition connects strongly to the IPO continuum and reflects both the actual data gathering and as well the conclusions I arrived at using the tools I developed (the various diagnostic instruments). Revising the definition in no way undermines the results of this research. Rather, the revised definition reflects the learning from the research journey, strengthens the connection between the concepts and the tools, and provides an improved basis from which to launch further research.

The revision to the IPO Definition is further justified by the changes to the definitions of the sub-constructs that resulted from the card sort exercise described in Chapter Six (research methods). Table 13-2 summarizes the original and revised sub-construct definitions.

Table 13-2: Sub-Construct Definitions (Revised)

Sub-construct	Original Definition	Revised Definition
Customer Relationship Stance	The firm's perspective on the obligations it owes its customers.	How your firm describes its obligations to its customers.
Customer Information Management Strategy	The organization's predominant strategy with respect to its objectives for gathering and using information.	Your firm's predominant purpose for collecting and using customers' personal information.
Customer Information Privacy Philosophy	The firm's view about the need to and rationale for engaging in privacy activities.	Your firm's view of the effect privacy laws have on your ability to carry on business.
Customer Information Privacy Behaviours	What privacy actions are taken by the firm.	Your firm's privacy policies that guide your privacy actions.

The final definitional consideration is to specifically identify that the phenomenon under investigation is related to customer information and not employee, state or other groups' information. Thus the revised construct will be identified in future work as CIPO (customer information privacy orientation).(However, to maintain clarity , I will continue to refer to IPO for the rest of the manuscript).

In summary, this research established that the components of information privacy orientation – customer relationship stances, information management strategies, privacy philosophies and privacy behaviors – were evident in all cases. In addition, there was some indication that the so-called "layer cake model" had some validity. However, further research is required to better establish both the horizontal and vertical dimensions of the IPO construct and to finalize the model. One of the important outcomes of this research is a revised construct definition.

R3: Does the Institutional Approach Explain IPO Homogeneity?

I demonstrated in the cross-case analysis that the Institutional Approach provided a good general explanation for IPO across the cases researched for this dissertation. At one level, the response by the financial institutions could be seen to be inevitable – a law was passed and so the firms followed the law. However, as was acknowledge by several participants in different firms, PIPEDA is "flexible" in its requirements of firms and "broad" in the interpretation of compliance. As long as the ten principles are respected, firms are able to tailor their information privacy programs to their specific competitive situations.[2] Therefore, there was the opportunity, largely taken, to design specific privacy programs (and hence establish an information privacy orientation) that was unique and amenable to individual circumstances.

Why then were the firms' IPO not as divergent or variable as one might have thought? Why did no firm in the field study simply meet the minimum compliance? And why did no firm seek to strongly differentiate itself on the basis of information privacy? The Institutional Approach showed that strong currents within the financial institutions industry constrained firms' perceived freedom to behave too differently from their competitors. The acknowledged sensitivity of the information to which they have access (e.g., financial and health information), the innate

[2] I used the analogy of the statute as a "floor" upon which firms built their privacy structures and not a "ceiling" the defined the upper limits of compliance. Participants accepted this analogy. For example, in Case D, an interviewee wondered aloud if they had constructed a "10 storey building when a 7 storey one would have been enough."

conservatism of the industry (e.g., tradition based and risk averse), and the fear of a loss of reputation in the event of a "privacy breach" are powerful disincentives to independent behaviour for these firms. At the same time, there is little apparent incentive to adopt a privacy program that would place the firm as visibly more compliant than their competitors.

However, there were indicators, for example with Case C, that firms may pursue privacy leadership within institutional constraints. My original conceptualization was that differentiation within the Institutional Approach would represent externally oriented "impression management." The inclusion of the impression management category was challenged by a committee member who suggested that impression management would lead to weaker, not stronger IPO. There are two ways to look at the role impression management might play. First, the IPO Continuum assumes that to be considered for a "stronger" categorisation, the firm already would be compliant. Therefore, a pure impression management approach would not place the firm in the strong category. To accommodate this approach would require an addition of a "decoupling strategy." Recall that "decoupling" was suggested by Oliver as a response strategy in which a firm publicly engaged in activities that would lead one to believe that it was compliant, engaged in the issue (or whatever the case may be) but which preserved the technical core of the firm. In other words, there would be no actual significant changes to the way the firm handled customers' information privacy only "public relations" about information privacy. I have no evidence that any of the firms in this study were engaged in decoupling approach but it is a valid theoretical issue. Second, in my institutional framework, compliance is considered an "internal activity." However, I'm arguing that compliant firms may also undertake externally oriented activities (such as additional information on websites about privacy related issues, sponsorship of conferences, etc.) This could be interpreted as "impression management" (firms aren't doing anything substantively different, just appear to be.)

Alternatively, (and with thanks to another committee member who urged a reconsideration), the Cashore & Vertinsky (2000) contribution that there is such a thing as a

"proactive" institutional category could be considered here. I had argued that "proactivity" is more appropriately considered within the RBV paradigm. However, the data suggest that a firm can be proactive (such as Case C) by engaging in considerably more activity internally (beyond basic compliance) and externally (as a legitimacy based exercise) without seeking sustained competitive advantage (the RBV paradigm.) I think this may be a more persuasive interpretation of the data for three reasons. It makes sense with the present data, logically fits the framework, and likely can be observed. My experience from Study One suggests that firms are engaged in a limited amount of impression management. Firms either comply and go on about their business, or engage in some additional substantive activities to which they draw attention.

In summary, the Institutional Approach was demonstrated to be applicable to explaining IPO homogeneity across the three firms in this research. However, there was a need to reconceptualise the repertoire of response mechanisms upon which firms drew.

R4: Does the Resource-Based View Explain IPO Heterogeneity?

No cases in this research were sufficiently different in their IPO that the Resource-Based View could be used alone to explain heterogeneous behavior. However, I illustrated how RBV might be used to explore Case D's decision to create the "information management triumvirate" (incorporating information privacy, information security and information resource management) into an enterprise-wide information management governance initiative. This discussion suggested that Information Privacy Orientation may not in itself confer sustainable competitive advantage, but may operate as an enabler of other processes.[3]

It may be that Canada's financial institutions did not present the most useful industry for theorizing information privacy using the RBV. First, the industry has relatively few major players, is heavily regulated, and operates with a high degree of interdependence. It may not be

[3] In contrast, Case C appeared to be investigating a privacy leadership positioning. However, I am not convinced that this positioning would represent a shift best explained by the RBV. Rather, I think the positioning is more likely an example of stronger IPO within an institutional framework.

possible for a single financial institution to achieve a sustainable competitive advantage through information privacy. (One financial institution that I had identified in the Phase One Privacy Policy Evaluation Study as potentially differentiating on information privacy declined to participate in this research.) Second, the RBV is a more difficult theory to assess than is the IA because it requires intimate knowledge of internal organizational activities. There may be a need to refine research approaches to isolating information privacy processes, resources and capabilities. A third reason is a consequence of my decision to restrict my investigations to retail banking. I did this to keep the project to a manageable scope. However, over the course of the research, it became apparent that these firms operate broader businesses, incorporating several lines of business such as wealth management (i.e., registered plans such as retirement savings), investment banking (i.e., brokerage), insurance, credit card, and private banking (high net worth retail accounts) in addition to their retail networks. The strategic thrust common to all firms is to increase the "share of wallet" through the establishment of deep "relationships." The challenge of managing customer information privacy across multiple lines of business may produce more variance in privacy processes such that privacy based sustainable competitive advantage is both possible and detectable.

Therefore, my inability to apply the RBV well in this research may be a consequence of the industry I selected for my investigations. I believe that the RBV still provides the opportunity for gaining different insights into IPO and will be a worthwhile pursuit in future studies.

At the same time, I believe that there is a need to further reflect on the appropriate juxtaposition of the RBV with the Institutional Approach. Recall that, in the discussion (Chapter Five) of the two theories I employed to explain the variance in firms' IPO, I cast the IA and RBV in competing roles. That is, I argued that these theories offered discrete lenses through which to evaluate corporate privacy actions. I believe that the findings from these case studies support the view of IA and RBV as complementary theories that overlay a single continuum (not modeled as separate continua), as illustrated in Figure 13-4. However, further research is required in other

firms and other sectors to ascertain whether there is a constant relationship between these theories (either competing or complementary regardless of sector) or whether there is an industry effect. I perceive that the industry effect may result from the level of "sensitivity" of the customer information involved. An additional effect may arise from the firm's specific characterization of its customer information as a specific resource that it harnesses through deliberate processes to achieve specific outcomes. There is much more research needed to understand these two issues.

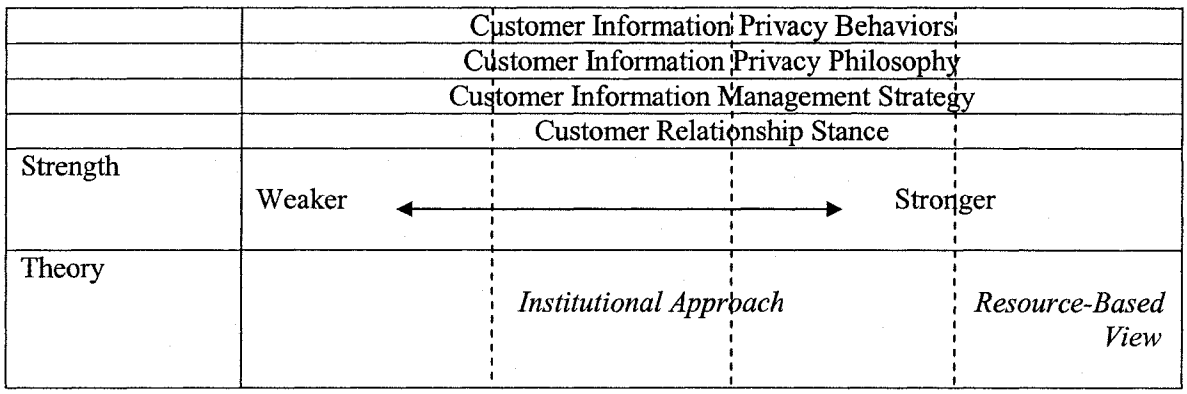


Figure 13-4: Complementary Theories to Explain IPO

In summary, I was able to find evidence to support my theorizing that the Institutional Approach (R3) would explain IPO homogeneity. I was able to discern a potential for theorizing the RBV (R4) to explain IPO heterogeneity. There was evidence to support both a "competing" and a "complementary" theories approach. More research is required to untangle the relationship between these two theoretical explanations for IPO behaviour.

R5: What is the Effect of the Firm's Context on Its IPO?

This research question was not a priority or focus of the current research. However, as a result of the analysis of the interview transcripts and documentary evidence, I can make some comments about the antecedent variables contained in the Information Privacy Orientation Contingency Framework that I presented in Chapter Three.

Recall that the framework distinguishes among external variables (national culture, regulatory environment and industry practice) that I argued influence the firm's decisions on and approach to privacy program implementation. Further, I proposed two sets of internal variables: those that support the achievement of the firm's economic mission (strategic positioning, market orientation, and slack resource availability), and those that support other goals (organizational culture, ethical climate, interfunctional values, and top management preferences).

I identified some support for the three external variables. National culture was most evident in the general agreement with the proposition that customers own their information. This was particularly evident in Case C (which was more inclined to view ownership as an ethical precept) and Case D (which had incorporated customer ownership within its corporate policy). This attitude to information ownership appears to be a Canadian legislative and business norm that stands in contrast to the views held, for example, by American business people. Clearly, the regulatory environment itself is an antecedent. The existence of PIPEDA influences corporate responses by definition. Similarly, the effect of being in an industry with several strong national trade associations that have provided Model Privacy Codes appears to affect firm behaviors.

I also identified some support for several of the internal variables. Strategic orientation appeared to influence the extent to which firms were willing to be seen to be different from their peers. Only Case C appeared to possibly desire a "strategic privacy position" and even then, the positioning was only modestly different from the other firms in the study. Market orientation was not specifically tested. All firms characterized themselves as being sensitive to the customer, but I could not easily discern from the data whether a classic market orientation influenced IPO. There appeared to be some influence exerted by the perception of the availability of slack resources. Despite the consistent understanding that implementing privacy was mandatory, the firms provided different levels of resource support. Organizational culture, expressed largely in terms of the "compliance cultures", was a consistent theme. Different ethical climates were discernible among the cases. No firm could be characterized as unethical, but the specificity with which

information privacy was identified as an ethical issue varied. Interfunctional values and top management preferences largely dictated the location of the privacy responsibility, the level of organizational investment, and the seniority of the Chief Privacy Officer role. At the same time, differences appear to exist between head office and branch personnel that indicated a potential for conflict or missed opportunity.

I identified a potential additional variable – "technology strategy." I differentiate technology strategy from information strategy in two ways. First, technology strategy focuses attention on the "containers" of customer information rather than on the "content" of the information (which is the concern of an Information Strategy). Second, technology strategy addresses the "back office processes" within a firm (as suggested by Porter's Value Chain model), while an information strategy moves the organizational conversation into a more strategic space. (I thank an executive in Case D for alerting me to these distinctions.) The technology strategy variable would incorporate the deployment of Customer Relationship Management (CRM) systems that are specifically designed to collect and manipulate large volumes of detailed customer information. Another example would be the deployment of mobile technologies. The technology strategy variable is missing from much of the literature on information privacy. Researchers refer to the "marketing databases" but my research suggests that it is the enterprise-wide initiatives (that are very costly to deploy and difficult sources of satisfactory financial returns) that likely present the greatest incentive to weaken a firm's privacy orientation. The challenges to deploy a system such as CRM while adhering to strong IPO is another area requiring research.

In summary, while the IPO Contingency Framework was not the focus of this dissertation, I was able to identify supporting evidence for the antecedent variables sufficient to justify more in-depth and systematic analysis of the present data as well as future research. I identified an additional potential variable to be included in this effort to identify organizational influences on IPO.

R6: What is the Effect of IPO on Firm Performance?

I was also able to identify support for the inclusion of outcome variables that I proposed in the IPO Contingency Framework in Chapter Three. The importance of the customer information that is gathered and used by all firms was evident across the cases. Respondents characterized the value to the firm of customer information as "huge," "invaluable," "we'd be out of business without it" and similar expressions indicating high importance. All firms place a high, if intangible, value on this form of intellectual capital. Likewise, I perceived that social capital in the form of customer trust and firm reputation were important outcomes identified by the banks. In addition, my distinction between trust supporting mechanisms (privacy based) and distrust minimizing actions (security based) appears to have some salience in these organizational settings. However, in all cases, the firms are struggling to measure the actual value of these outcomes. Presently, their value is characterized largely in speculative terms – "It would be hard to recover from a privacy breach" and "You can't get back trust once you've lost it."

In addition, the relationship between IPO and financial outcomes is undetermined. Some firms (Cases A and B) argue that there is no "upside" ("where's the revenue from privacy?"), just costs to be limited. Case C is still attempting to develop a positive way to think about the financial implications of privacy. This is an important challenge to them as they appear committed to the idea that privacy action is not about compliance but about business objectives. Case D appears to have shifted their financial outcomes conversation to the realm of their information privacy initiative and away from a pure privacy concern.

In summary, my research shows that there is likely some connection between IPO and the outcome variables identified in the contingency framework. This is another rich source for future research that will be appreciated by business organizations striving to make sense of the effect of their IPO on firm performance.

Section Summary

In this section I reviewed my findings against the specific research questions that I had established to frame my dissertation research program. I also identified areas where future research is required to deepen our understanding of the Information Privacy Orientation phenomenon in organizations. In the next section, I outline the implications of this dissertation research.

Implications

By its very nature, exploratory research such as is represented by this dissertation raises almost as many questions as it answers. Despite this, there are inferences that clearly can be drawn from this preliminary investigation into Information Privacy Orientation. In this section, I discuss the implications of this dissertation for researchers and managers.

Implications for Researchers

My research into Information Privacy Orientation revealed a complex, organizational level phenomenon. As such, it raises implications for information systems, marketing, and public policy researchers.

Information Systems Research – There are eight major implications of this research of interest to information systems researchers. First, information privacy is a business issue that has major ramifications across an enterprise, depending on how the organization perceives the challenges and opportunities of implementing their information privacy programs. Researchers thus need to involve a variety of organizational participants and use a variety of methods in order to build a comprehensive portrait of how the phenomenon is being handled. It is insufficient to interview the privacy personnel (who may know too much about privacy and too little about the enterprise) and read the privacy statement on the website. Instead, researchers need to interview a sample of organizational actors from different departments – including "IT" personnel – and

review a variety of documents that deal with privacy, including the firm's technology strategy and information strategy.

Second, information privacy initiatives may support information security and information management initiatives that would otherwise exist in organizational isolation. Information systems researchers should investigate the influence of privacy initiatives when studying Information Management Strategies or Information Resource Management in firms.

Third, requirements engineering researchers should include "ethical" objectives within their typologies. Information privacy has been identified as an ethical issue within the information systems privacy research tradition. However, privacy needs to be included as something that is "built in" at the beginning of processes, and what constitutes "building in" should be extended to include ethical objectives. Researchers can use the adapted information privacy objectives approach contained within the IPO Definition to support these efforts.

Fourth, the extension of the marketing ethics continuum into the MIS realm in order to underpin the IPO Continuum provides researchers with a practical way to incorporate the idea of ethics into their research. Previous IS research has identified privacy as an ethical issue (Mason 1986) and employed an ethics-based theoretical lens (Smith and Hasnas 1999). However, I characterised the ethical problem in terms of the relationship between a firm (the collector and user of customer information) and its customers (the suppliers, and either beneficiaries or victims of firm behaviour) in testable terms (Smith 1995). This provides a practical base upon which other researchers can build their privacy discussions.

Fifth, and following on the previous three points, IS researchers should consider the implications of treating information privacy not simply as an outcome (social impact) of information technology decisions, but potentially as an antecedent to information management decisions. Shifting the emphasis from the technology implications to the information opportunities presented by information privacy programs may offer a more complete picture of information privacy as an organizational level phenomenon. As was suggested to me by an MIS

researcher, the IS discipline has succeeded in resolving the information storage and information retrieval problems. My research appears to begin to address the information use problem.

The sixth implication is that the Information Privacy Orientation construct should be used in studies of information privacy at the organizational level of analysis. The IPO Definition provides a comprehensive but bounded approach to defining how a privacy initiative is constructed in a firm. This offers a basis for insight within a firm and comparison across firms. The IPO Definition helps to set the context for additional information privacy investigations.

Seventh, the influence of industry norms through the expression of, for example, Model Privacy Codes, has strong implications for information systems based privacy research in two ways. One, the current research was conducted in a single industry with strong norms for customer relations (i.e., traditions of confidentiality), and common information technology standards (i.e., interoperability). The presence or absence of such norms should be identified, and their likely impact on information privacy approaches theorized prior to undertaking any organizational level privacy studies in order that "industry" effects can be properly captured. Two, the presence of industry codes may influence the ability of firms to "automate" privacy. Privacy compliance automation studies need to be conducted within appropriate organizational contexts.

Last, the expansion of business into the mobile commerce space has important implications for future research. If we understand that the development of ubiquitous computing capability involves interactions with customers that are far more highly individual and location-aware than is the case with electronic commerce, privacy becomes an even greater concern for organizations (Keen and Mackintosh 2001). The opportunity for mobile commerce (as a technology strategy) to undermine IPO strength through the deliberate exploitation of customers must be acknowledged in information systems research. A good starting point might be to map mobile computing initiatives to the IPO Continuum.

Marketing – There are three major implications of this research for marketing researchers. First, information privacy orientation is a complex phenomenon that strongly connects customer information to firms' actions. Enterprise-wide information management strategies that support marketing decision-making need to incorporate some aspect of information privacy (for example, consent). However, marketing researchers may want to examine how information privacy programs can be harnessed to explicitly facilitate advanced marketing initiatives that would support either "value-add" or "create new reality" information management opportunities. Second, the adapted Marketing Ethics Continuum, which underpins the IPO Continuum, offers marketing researchers an approach to considering other ethics informed issues.

Third, there is a need to consider the explicit relationship between "market orientation" and "information privacy orientation." The present research is insufficient to make the case one way or the other. However, the findings that firms do have customer relationship stances (how firms view their obligations to customers) and information management strategies (the overriding reason for collecting customer information) suggests that a firm's market orientation may offer a significant context to IPO. Market orientation may provide particular insight into the constraints on firms (what is acceptable privacy practice) as well as the opportunities (how does the firm learn from/employ its customer information resource for competitive advantage)?

Public Policy – There are three primary public policy implications stemming from this research. First, this dissertation showed that companies used the latitude offered by PIPEDA to craft different privacy programs. This provides support to the contention that firms choose responses to external stimulus (as theorized by Oliver). Researchers need to investigate privacy programs in other industries in order to assess the degree to which responses to legislation is a function of the industry or of the company. My research suggests that there is a positive industry effect with financial institutions since they are heavily regulated and therefore have evolved processes for complying with legislative initiatives. This effect may be reduced in industries that

lack this tradition and capability. Research is needed across industrial and commercial sectors to understand IPO formation in different types of firms.

A second public policy implication involves the desirability for the development of a common international privacy regime to support firms that operate across legal jurisdictions. The ability to monitor and coordinate responses to the plethora of privacy statutes and agencies may jeopardize the willingness of firms to attempt anything beyond the most minimal compliance they assess they can get away with. While I restricted my research to the domestic sphere, one firm was already grappling with how to reconcile the operational strains of managing information privacy across three international jurisdictions. They were aware that their corporate policy was not, in fact, company-wide as it had a number of exemptions for operations in another jurisdiction. Privacy staff indicated a growing frustration with this state of affairs but were uncertain how this incongruity could or would be reconciled. Further research is needed to understand how firms that operate globally cope with these competing demands.

In summary, I described various implications of the dissertation for researchers in information systems, marketing and public policy. I now consider the implications of this research for managers.

Implications for Managers

This dissertation documented the different approaches to information privacy taken in three firms. While case studies, by definition, are not generalizable (in the traditional statistical sense of generalizability), these case studies do offer insights that illustrate the challenges for managers.

The first insight is that a firm contemplating implementing a privacy program has choices, even when operating within a legally constrained environment (such as under Canada's PIPEDA). This legislation provides a floor, and the firm must decide whether the privacy structure they erect is a "bungalow" (meeting basic privacy requirements) or a "mansion"

(providing a more elaborate privacy program). Managers responsible for privacy programs should be clear on what they choose to build and why. The Information Privacy Orientation Continuum offers a structured way for managers to think about the opportunities and implications of different privacy postures.

Second, organizational choices reflect the priority accorded the privacy initiative and the resources assigned to it. Managers need to carefully define the nature of their initiative (whether a threat or opportunity, an identity or image issue, or an opportunity for technical or administrative innovation) in order to assign appropriate resources. For example, an important choice involves the role of the Chief Privacy Officer/ Privacy Manager. As with any organization-wide initiative, where the position is placed matters. As one CPO expressed it, the position will have greater or lesser access (to senior decision-makers), profile (visibility to promote the initiative) and impact (capability to influence decisions). It appears to be important to align the position of the CPO with the objectives for the privacy initiative.

Third, managers may want to attend to longer term issues even as they strive to meet short term "compliance" objectives. While a firm can obviously choose not to connect their information privacy initiatives to their information management strategy, this may prove to be a lost opportunity. Information Privacy helps to connect information management practices to customer information and, as a result, reinforces important information management disciplines that could support overall business objectives beyond mere compliance with the law.

Fourth, and following on the previous implication, Information Privacy initiatives offer opportunities to reinforce other desirable initiatives. For example, the integration of information privacy with information security and information management supports "building in privacy" at the beginning of processes rather than rendering it an afterthought. Information privacy concerns by customers are not expected to diminish over time. Firms that develop integrated approaches may be better able to match their privacy capabilities to customer expectations even if they do not do so to pursue competitive advantage. Managers in the case studies affirmed that good (as

opposed to weak or very strong) information privacy programs constituted "table stakes" in the competition for customer attraction and retention. Integrated programs may offer the opportunity to maintain a place at the table even as the stakes are raised.

Last, information privacy increasingly represents a multi-jurisdictional challenge for organizations. Managers need to carefully consider the implications of simply managing customer information privacy according to the minimum standards of each country in which they operate versus developing, implementing and enforcing a consistent over-arching set of privacy principles to which all divisions of the organization are bound. The latter approach speaks to the need for managers to consider privacy as an enterprise-wide business challenge that requires resources and attention beyond what might typically be made available for "compliance projects." The IPO Continuum offers a visual decision tool for managers to use to map their various privacy initiatives and contemplate a comprehensive, enterprise-wide privacy program.

Section Summary

In this section I discussed the implications of the dissertation for information systems, marketing, and public policy researchers. Then I identified some considerations for managers of privacy initiatives in organizations. I turn now to a discussion of the limitations of the thesis research.

Limitations

As with any research undertaking, there are several limitations to this multiple case study. The first limitation, and arguably most important, is that which is presented by the methodology itself. There are two major ways to assess this kind of qualitative research, which is located within a postpositivist paradigm (Guba and Lincoln 1994) and possesses strong interpretivist leanings (Orlikowski and Baroudi 1991). I assess my research using Yin's (1994) approach to establishing validity and reliability in case studies, and Lincoln and Guba's (1984) criteria for

judging qualitative research. Table 13-3 integrates the two approaches and itemizes the procedures I used to address these concerns. However, for the sake of clarity, I present each approach separately.

Table 13-3: Two Approaches to Evaluating Case Studies

Positivist: Yin (1994)		Interpretivist: Lincoln and Guba (1985)		
Threat	Concern	Issue	Concern	Procedures to address concerns
Construct Validity	Is what I think I am studying what is actually being addressed?	Confirmability	Is what is being presented "real" and "objective"?	• Triangulation of multiple sources of evidence • Chain of evidence • Key informants
Internal Validity	Is there a relationship among the variables, themes, ideas?	Credibility	Is there a fit between what is represented in the research and what is known by the respondents?	• Statistical analysis • Explanation-building through iteration • Key informants
External Validity	Is it possible to generalize understanding to other cases?	Transferability	Is it possible to generalize understanding to other cases?	• Replication logic in design of multiple case studies
Reliability	Is the process used to obtain the findings documented appropriately to facilitate understating?	Dependability	Is the process used to obtain the findings documented appropriately to facilitate understating?	• Case study protocol • Case study database

"Positivist" Case Study Assessment

Yin's (1994) approach to the difficult task of establishing validity and reliability in case method research involves using the language of positivist and quantitative studies (i.e., Cook and Campbell, 1979 "threats to validity") to discuss methodological limitations and procedures for addressing them. My research met most of Yin's (1994:33) criteria. Construct validity was primarily addressed by triangulating the data I collected from three sources (interviews, documents and surveys). In addition, I made extensive use of the key informants during the

course of the research visits to ask questions and develop ideas. Unfortunately, I was unable to require (i.e., to force) staff at the firms to review the draft manuscript. Their primary interest lay in receiving a management report and to minimize the demands on their time. While this is unfortunate, I stand by my research based on the number of interviews (transcripts), documents and surveys I was able to secure. Internal validity was addressed through statistical analysis, pattern matching and explanation building in analyzing the qualitative data. Again, completed questionnaires were not provided by one case site, despite repeated requests for the data. However, I believe that the thoroughness of the interview process at this site, along with the many documents I obtained, reduced the threat to internal validity. Reliability was established through the case study database. This database included all the interview transcripts and handwritten interview notes; documents that I secured from the companies and independently; the websites that I captured for the first study; my notes, emails and sundry correspondence with the research sites; and assorted articles, research reports and similar materials that I obtained over the course of this research. Many of these materials are catalogued in various appendices to this dissertation.

External validity, that is generalizability beyond the three case sites, is of course difficult to address even using the logic of theoretical replication (in which different cases are selected to provide different results for theoretically predicted reasons, Yin 1994:46). Since this research is largely exploratory and theory building in nature, the lack of external validity is not of critical concern. However, to the extent that I engage in "theory testing" by applying the competing logics of the institutional approach versus the resource-based view to my findings, external validity is an issue. However, it cannot be addressed fully given the restricted sample of firms (three Canadian financial institutions). The interpretation of the study findings using the two theories, at best, provides insight into the possibility of using these competing logics in other settings rather than providing conclusions broadly applicable to other organizations.

"Interpretivist" Case Study Assessment

Lincoln and Guba (1985) offer a different, if complementary, approach to assessing the quality of qualitative research. Similar to Yin, they offer a qualitative "spin" to what are essentially quantitative research concepts. However, their language is somewhat more flexible and may be more useful to apply to the "intensive" research approach I took in this dissertation. Again, they have four basic assessment criteria that, taken together, comprise a study's "trustworthiness", which is defined as "the quality of an investigation and its findings that makes it noteworthy to audiences" (Lincoln and Guba 1985: 300). Confirmability addresses the extent to which the data and its interpretation demonstrate understanding. This was addressed primarily through the triangulation of multiple sources of information. Credibility involves the "fit" between the researcher's interpretation and the respondents' views of reality. This was addressed primarily through the use of key informants to provide context and insight to challenge my interpretations. As indicated previously, I was unable to secure the review of interview transcripts by the respective respondents. However, I believe that since the majority of transcripts were taped (or transcribed from detailed notes), I took detailed notes throughout each interview, and I followed to the greatest extent possible an interview guide supports more than subtracts from the credibility of my findings.

Transferability is similar to external validity (generalizability). It was addressed through the replication logic employed within the study design. Dependability is similar to reliability and was addressed through both the case study protocol and the case study database established for this research project. My supervisor reviewed my progress at regular intervals to provide a quality assurance perspective to the research project.

An additional potential limitation of this research involves social desirability bias among the participants I interviewed. I believe this was addressed successfully through the multiple interviews and other data collection approaches I undertook. I found the participants to be

cooperative and interested in telling me about information privacy in their firms. I worked throughout the interviews to feed back, rephrase and employ other techniques to ensure understanding and offer opportunities to clarify and challenge. Most participants did not appear to hesitate to correct me, ask for clarification, indicate no opinion, or similarly manage their participation rather than be managed by me.

In summary, I identified the potential threats to this research at the outset of my research program and developed a set of procedures for addressing these threats. While I cannot claim to have addressed each individual threat, I believe that the totality of the research methods I used was appropriate and adequate to minimizing these threats. In the final section of this chapter, I discuss the contributions made by this dissertation research.

Contributions

In this section I review the specific contributions my dissertation makes to our understanding of information privacy as an organizational level concern.

I contribute to the broad literature on information privacy by defining and demonstrating the existence of an organizational level construct called Information Privacy Orientation. As indicated in the Review of the Privacy Literature (Chapter Two), there is a serious gap in understanding information privacy actions within organizations. This study provides a modest first look at customer information privacy as the outcome of deliberate organizational action.

My dissertation also contributes the Information Privacy Orientation Continuum. The IPO Continuum adapts and extends the Marketing Ethics Continuum proposed by Smith (1995). The Marketing Ethics Continuum was adapted to serve as the Customer Relationship Stance layer of the IPO Continuum. This is a contribution to the marketing literature on information privacy and marketing ethics. The IPO Continuum also adapts Marchand's Strategic Use of Information framework (1998) by specifying it as the Information Management Strategy layer of the continuum. This is a contribution to the information systems literature.

This dissertation also constitutes the first study (to my knowledge) of the responses by Canadian financial institutions to the federal government's passage of the PIPEDA. The examination of the privacy policies that ten firms had posted to their websites documents the range of publicly visible responses to the privacy statute. As well, I provide the first industry specific examination (again to my knowledge) of privacy practices in selected financial institutions. Finally, this study is one of the few (since Smith 1989, 1993) to investigate deeply what firms do about privacy as opposed to what they say they do (via their websites). Milne and Culnan (2002) argue for more in-depth studies of information privacy practices because of the "limited insights" offered by privacy website surveys. These are contributions to both the privacy research literature and public policy.

I developed specific tools that can be used by privacy investigators interested in examining organizational level privacy phenomena. The revised IPO Definition is operationalized through the IPO Continuum. The IPO Continuum provides a means for assessing both the strength of IPO in individual firms as well as the relative IPO positioning of a collection of organizations. I extended the Privacy Objectives typology originally proposed by Earp et al. (2002) by specifying an "ethics" objective. This contributes to the information systems and requirements engineering literature. The IPO Survey provides a vehicle for quantitatively assessing the IPO of a firm. While the survey requires additional work to establish and refine its psychometric properties, it was demonstrably useful as part of a triangulation process in the current research.

I also contributed the IPO Contingency Framework, in which a firm's IPO mediates the relations between external and internal antecedent as well as outcome variables. While the framework was not a focus of the dissertation research, my initial analysis supports the existence of these contextual variables and identifies an additional internal variable. This framework offers privacy researchers from a variety of disciplines a basis for pursuing systematic organizational level privacy studies.

Finally, I contributed to the growing literature on institutional theory by demonstrating the impacts of institutional pressures on privacy decision-making in these firms. As well, I demonstrated how the RBV might be applied to privacy studies.

Chapter Summary

In this chapter, I discussed the findings from this dissertation and I identified the implications for researchers and managers. I also identified the limitations and concluded by discussing the contributions made.

Concluding Thoughts

The relevance of this dissertation and the need for a sustained program of information privacy research was underscored by an event that occurred a few days prior to my defense of this research. A Canadian financial institution (not included in the case research) came under investigation by the Canadian government's Information Privacy Commissioner. The Commissioner took the highly unusual step of publicly naming the firm and indicating (on the homepage of the Commission's website) that it was investigating "an incident concerning CIBC [the bank] and misdirected faxes to an organization in the United States."[4] The bank's "routine business practice" of faxing transaction information to a central processing office had come under scrutiny. It is alleged that the bank had known for several years that some faxes, containing detailed sensitive personal and financial information, were ending up in the office of a scrap yard in West Virginia. The scrap yard owner alleged that this problem had been going on since July 2001, despite his having alerted CIBC to this issue. It is suggested that the bank did not take appropriate steps to stop the problem. A flurry of highly damaging newspaper reports followed the story including ones that reported that customers had or were thinking of moving their accounts to other banks (Stewart and Akin 2004). Interestingly, the bank's positioning statement

[4] http://www.privcom.gc.ca/index_e.asp accessed November 26, 2004.

"CIBC. For what matters." As a privacy researcher, I can only conclude that customer information privacy is not what matters to this firm. And I wonder why. Clearly, more research is required.

REFERENCES

Akaah, I.P. (1993). "Organizational Culture and Ethical Research Behavior." *Journal of the Academy of Marketing Science* (21:1), 59-63.

Alexander, P.S. (2001). "The Interface Between Consumers and Commercial Internet Sites: Information Privacy Concerns and Fair Information Practice/Privacy Statements." Unpublished dissertation. University of Memphis.

Ang, S. and L.L. Cummings. (1997). "Strategic Response to Institutional Influences on Information Systems." *Organization Science* (8:3), 235-256.

Aragón Correa, J.A. (1998). "Strategic Proactivity and Firm Approach to the Natural Environment." *Academy Of Management Journal* (40:2), 556-567

Bacharach, S.B., P.A. Bamberger, and W.J. Sonnenstuhl. (1996). "The Organizational Transformation Process: Micro-Politics of Dissonance Reduction and the Alignment of Logics of Action." *Administrative Science Quarterly* 40(3), 487-506.

Bantel, K.A. and S.E. Jackson. (1989). "Top Management and Innovations in Banking: Does the Composition of The Top Team Make a Difference?" *Strategic Management Journal*, (10:Special Issue Summer),107-124.

Barney, J.B. (1991). "Firm Resources and Sustained Competitive Advantage." *Journal of Management* (17:1), 99-120.

Barney, J. and R. Griffin. (1992). *The Management of Organisations: Strategy, Structure, Behavior.* Boston: Houghton Mifflin.

Barney, J.B. and M.H. Hansen. (1994). "Trustworthiness As a Source of Competitive Advantage." *Strategic Management Journal* (15), 175-190.

Baron, J.N., F.R. Dobbin, and P.D. Jennings. (1986). "War and Peace: The Evolution of Modern Personnel Administration in U.S. Industry." *American Journal of Sociology* (92:2).

Baum, J.A.C. and C. Oliver. (1992). "Institutional Embeddedness and the Dynamics of Organizational Populations." *American Sociological Review* (57), 540-559.

Benbasat, I., D.K. Goldstein, and M. Mead. (1987). "The Case Research Strategy in Studies of Information Systems." *Management Information Systems Quarterly* (11:3), 369-386.

Bennett, Colin J. (1992). *Regulating Privacy.* Ithaca, NY: Cornell University Press.

Bennett, C.J. and R. Grant. (1999). "Introduction". In *Visions of Privacy,* C.J. Bennett and R. Grant (Eds.), Toronto: University of Toronto Press, 3-16.

Blodgett, J.G., L. Ly, G.M. Rose, and S.J. Vitell. (2001). "Ethical Sensitivity to Stakeholder Interests: A Cross-Cultural Comparison." *Journal of the Academy of Marketing Science* (29:2), 190-202.

Bloom, P.N., G.R. Milne, and R. Adler. (1994). "Avoiding Misuse of New Information Technologies: Legal and Societal Considerations." *Journal of Marketing*, (58:January), 98-110.

Bordoloi, B., K. Mykytyn, and P.P. Mykytyn. (1996). "A Framework to Limit Systems' Developers Legal Liabilities." *Journal of Management Information Systems* (12), 161-185.

Bowen, F. (2002). "Organizational Slack as a Facilitator of Operational Level Environmental Initiatives." *Academy of Management*, Denver, Colorado, August 2002.

Bower, J.L. (1970). *Managing the Resource Allocation Process*. Graduate School of Business Administration, Boston: Harvard University Press.

Bradburn, Norman N. (1983). "Response Effects." Chapter 8 in *Handbook of Survey Research*, Peter H. Rossi, James D. Wright and Andy B. Anderson (Eds.). New York: Academic Press, 289-328.

Brown, T.J. and P. Dacin. (1997). "The Company and the Product: Corporate Associations and

Consumer Product Responses." *Journal of Marketing* (61:January), 68-84.

Brumagin, A.L. (1994). "A Hierarchy of Corporate Resources." *Advances in Strategic Management* (10A), 81-112.

Buenger, V., R.L. Daft, E.J. Conlon, and J.Austin. (1996). "Competing Values in Organizations: Contextual Influences and Structural Consequences." *Organization Science* (7:5), 557-576.

Burt, Ronald. S. (1992). *Structural Holes.* Cambridge, MA: Harvard University Press.

Cadogan, R. (2001). "The Ethics of Data Privacy in an Electronic Marketplace: A Multiple Case Study of the Privacy Policy Notice and the Incorporation of Fair Information Practice Principles." Unpublished dissertation. Viterbo University.

Canadian Federation of Independent Business (CFIB). (2002). "Draft Legislation Concerning Privacy of Personal Information." Letter to Hon. Norm Sterling, Minister of Consumer and Business Services, Government of Ontario, dated Thursday March 28, 2002.

Canadian Marketing Association (CMA). (2002). "Compliance Guide for Members Concerning the Use of Opt-Out Consent: Amendments to Code of Ethics and Standards of Practice and Privacy Code November 2002," Downloaded from: http://www.the-cma.org/privacy/compliance.cfm, Accessed: Sept. 23, 2003.

Cashore, B. and I. Vertinsky. (2000). "Policy Networks and Firm Behaviors: Governance Systems and Firm Responses to External Demands for Sustainable Forest Management." *Policy Sciences* (33:1), 1-30.

Caudill, E.M. and P.E. Murphy. (2000). "Consumer Online Privacy: Legal and Ethical Issues." *Journal of Public Policy and Marketing* (19:1), 7-19.

Cavoukian, A. and T.J. Hamilton. (2002). *Privacy Payoff: How Successful Businesses Build Customer Trust.* Toronto: McGraw-Hill Ryerson.

Cespedes, F.V. and H.J. Smith. (1992). "Database Marketing: New Rules for Policy and Practice." *Sloan Management Review*, Summer, 7-22.

Chan, Y. (2003). "Competing Through Information Privacy." In *Competing in the Information Age Align in the Sand* (2nd ed.), J.N. Luftman (Ed.), New York: Oxford University Press, 350-361.

Charters, D. (2002). "Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience." *Journal of Business Ethics* (35), 243-254.

Chattopadhyay, P., W.H. Glick and G.P. Huber. (2001). "Organizational Actions in Response to Threats and Opportunities." *Academy of Management Journal* (44:5), 937-955.

Chen, C. (1999). "The FORTUNE e-50." *Fortune* (140:11), Dec. 6, 1991, 41. Downloaded from http://www.fortune.com/fortune/articles/0,15114,377351,00.html; accessed May 19, 2003.

Christensen, E. and G. Gordon. (1999). "An Exploration of Industry, Culture, and Revenue Growth." *Organization Studies* (20:3), 397-422.

Clarke, R. (1999). "Internet Privacy Concerns Confirm the Case for Intervention." *Communications of the ACM* (42:2), 60-67.

Coff, R. (1999). "When Competitive Advantage Doesn't Lead to Performance: The Resource-Based View and Stakeholder Bargaining Power." *Organization Science* (10:2), 119-133.

Cohen, D.V. (1995a). "Creating Ethical Work Climates: A Socioeconomic Perspective." *The Journal of Socio-Economics* (24), 317-343.

Cohen, D.V. (1995b). "Moral Climate in Business Firms: A Conceptual Framework for Empirical Research." *Academy of Management Best Paper Proceedings*, 55th Annual Meeting of the Academy of Management, Vancouver, BC.

Coleman, J.R. (1990). *Foundations of Social Theory*. Cambridge, MA: Bellknap Press.

Collis, D.J. and C.A. Montgomery. (1995). "Competing on Resources: Strategy in the 1990s." *Harvard Business Review* (73:4), 118-128.

Cook, T.D. and D.T. Campbell. (1979). *Quasi-Experimentation: Design and Analysis Issues for Field Settings*. Chicago: Rand McNally.

Creswell, J.W. (1994). *Research Design: Qualitative and Quantitative Approaches*. Thousand Oaks: Sage.

Creswell, J.W. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Thousand Oaks: Sage.

Cullen, J.B., B. Victor, and J.W. Bronson. (1993). "The Ethical Climate Questionnaire: An Assessment of Its Development and Validity." *Psychological Reports* (73), 667-674.

Culnan, M.J. (1993). "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use." *Management Information Systems Quarterly* (17:2), 341-363.

Culnan, M.J. (1995). "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing." *Journal of Direct Marketing* (9), 10-15.

Culnan, M.J. (1999a). *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission.*

Culnan, M.J. (1999b). *Privacy and the Top 100 Websites: Report to the Federal Trade Commission,* prepared for the Online Privacy Alliance.

Culnan, M. J. and P. Armstrong. (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* (10:1), 104-115.

Culnan, M.J. and R.J. Bies. (1999). "Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-first Century." In *Visions of*

Privacy: Policy Choices for the Digital Age, Colin J. Bennett and Rebecca Grant (Eds.), Toronto: University of Toronto Press, 149-167.

Culnan, M.J. and R.J. Bies. (2003). "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* (59:2), 323-342.

Cyert, R.M. and J.G. March. (1963). *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice-Hall.

Dacin, T., M.J. Ventresca, and B.D. Beal. (1999). "The Embeddedness of Organizations: Dialogue and Directions." *Journal of Management* (25), 317-356.

Daft, R.L. (1978). "A Dual-Core Model of Organization Innovation." *Academy of Management Journal* (21), 193-210.

Davenport, T.H. and L. Prusak. (1998). *Working Knowledge*. Boston, MA: Harvard Business School Press.

Davis, F.D., R.P. Bagozzi, and P.R. Warshaw. (1992). "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace." *Journal of Applied Social Psychology* (22:14), 1111-1132.

Day, G.S. (1997). "Aligning the Organization to the Market." In *Reflections on the Futures of Marketing,* D.R. Lehmann and K. E. Jocz (Eds.). Cambridge, MA: Marketing Science Institute, 67-93.

Day, G. S. (2001). "Learning About Markets." In *Using Market Knowledge,* R. Deshpandé (Ed.). Thousand Oaks, CA: Sage, 9-30.

Day, G.S. and R. Wensley. (1988). "Assessing Advantage: A Framework for Diagnosing Competitive Superiority," *Journal of Marketing* 52 (April), 1-20.

Deal, T.E. and A.A. Kennedy. (1982). *Corporate Cultures*. Reading: MA: Addison-Wesley.

Deephouse, D. (1996). "Does Isomorphism Legitimate?" *Academy of Management Journal* (39), 1042-1039.

Dechamps, J. (1998). "From Information and Knowledge to Innovation." In *Competing with Information: A Manager's Guide to Creating Business Value with Information Content,* D. Marchand (Ed.). London: Wiley.

Department of Commerce (DOC). (2002). "Welcome to the Safe Harbor." Downloaded from http://www.export.gov/safeharbor, accessed September 2003.

Deshpandé, R. (2001). "From Market Research Use to Market Knowledge Management." In *Using Market Knowledge*, Rohit Deshpandé (Ed.). Thousand Oaks, CA: Sage, 1-8.

DeVellis, Robert F. (1991). *Scale Development: Theory and Applications*. (Applied Social Science Research Methods Series Vol. 26). Newbury Park, CA: Sage.

Dhillon, G., J. Bardacino, and R. Hackney. (2002). "Value Focused Assessment of Individual Privacy Concerns for Internet Commerce." *Twenty Third International Conference on Information Systems*, Barcelona, Spain, 705-709.

Dickson, P. (1992). "Toward a General Theory of Competitive Rationality." *Journal of Marketing* (62:January), 69-83.

DiMaggio, P.J. and W.W. Powell. (1983). "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* (48).

Dinev, T. and P. Hart. (2003). "Privacy Concerns and Internet Use – A Model of Trade-off Factors." Presentation to 2003 *Academy of Management,* Seattle, Washington, August 2003.

Dobbin, F.R., J.R. Sutton, J.W. Meyer, and W. R. Scott. (1993). "Equal Opportunity Law and the Construction of Internal Labor Markets." *American Journal of Sociology* (99), 396-427.

Doty, D.H. and W.H. Glick. (1994). "Typologies as a Unique Form of Theory Building: Toward Improved Understanding and Modeling." *Academy of Management Review* (19:2), 230-251.

Dutton, J.E. and S.E. Jackson. (1987). "Categorizing Strategic Issues: Links to Organizational Action." *Academy of Management Review* (12:1), 76-90.

Dyer, J.H. and H. Singh. (1998). "The Relational View: Cooperative Strategy and Sources of Interorganizational Competitive Advantage." *Academy of Management Review* (23:4), 660-679

Earp, J.B., A.I. Antón, and O. Jarvinen. (2002). "A Social, Technical, and Legal Framework for Privacy Management and Policies." *Eighth Americas Conference on Information Systems*, 605-612.

Edelman, L. (1992). "Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law." *American Journal of Sociology* (97), 1531-1576.

Eisenhardt, K.M. (1989). "Building Theories from Case Study Research." *Academy of Management Review* (14), 532-550.

Fink, A. (1995). *How to Design Surveys*. Thousand Oaks: Sage.

Frey, J.H. and S.M. Oishi. (1995). *How to Conduct Interviews by Telephone & in Person.* Thousand Oaks: Sage

Elsbach, K.D. and R.M. Kramer. (1996). "Members' Responses to Organizational Identity Threats: Encountering and Countering the Business Week Rankings." *Administrative Science Quarterly* (41:3).

Elsbach, K.D. and R.I. Sutton. (1992). "Acquiring Organizational Legitimacy through Illegitimate Actions: A Marriage of Institutional and Impression Management Theories." *Academy of Management Journal* (35), 699-738.

Equifax, Inc. (1992). *The Equifax Report on Consumers in the Information Age.*

Ferrell, O.C. and S.J. Skinner. (1988). "Ethical Behavior in the Bureaucratic Structure in Marketing Research Organizations." *Journal of Marketing Research* (25), 103-109.

Fligstein, N. (1985). "The Spread of the Multidivisional Form Among Large Firms, 1919-1979." *American Sociological Review* (50).

Fombrun, C.J. and M. Shanley. (1990). "What's in a Name? Reputation Building and Corporate Strategy." *Academy of Management Journal* (33:2), 233-258.

Fombrun, C.J. (1996). *Reputation: Realizing Value from the Corporate Image.* Cambridge MA: Harvard Business School Press.

Foxman, E.R. and P. Kilcoyne. (1993). "Information Technology, Marketing Practice and Consumer Privacy: Ethical Issues." *Journal of Public Policy and Marketing* (12:1), 106-119.

Friedman, Batya, Peter H. Kahn Jr., and Daniel C. Howe. (2000). "Trust Online." *Communications of the ACM* (43:12), 34-40.

Friedman, Milton. (1970). "The Social Responsibility of Business is to Increase Its Profits." *The New York Times Magazine,* September 13.

Fritzsche, D.J. (2000). "Ethical Climates and Ethical Dimensions of Decision Making." *Journal of Business Ethics* (24:2), 125-140.

FTC. (1998). Accessed Feb.14, 2003 http://www.ftc.gov/reports/privacy3/priv-23a.pdf

FTC. (2000). Accessed Feb.14, 2003 http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Galaskiewicz, J. and S. Wasserman. (1989). "Mimetic Process Within an Interorganizational Field: An Empirical Test." *Administrative Science Quarterly* (34).

Galliers, R.D. (1993). "Research Issues in Onformation Systems." *Journal of Information Technology* (8), 92-98.

Gattiker, U.E. and H. Kelley. (1999). "Morality and Computers: Attitudes and Differences in Moral Judgments." *Information Systems Research* (10:3), 223-254.

Geist, M. (2002). *Internet Law in Canada (3rd ed.).* Concord, ON: Captus Press.

Geist, M. and G. Van Loon. (2000). "Canadian E-Commerce and Privacy Study 2000: A Failure to Communicate." Obtained from the first author.

George, J. (1996). "Computer-Based Monitoring: Common Perceptions and Empirical Results." *Management Information Systems Quarterly* (20), 459-480.

Gioia, D.A. and J.B. Thomas. (1996). "Institutional Identity, Image and Issue Interpretation: Sensemaking During Strategic Change in Academia," *Administrative Science Quarterly* (41:3), 370-403.

Goldstein, R.C. and R.L. Nolan. (1975). "Personal Privacy Versus the Corporate Computer." *Harvard Business Review* (53:2), 62-70.

Goodstein, J. (1994). "Institutional Pressures and Strategic Responsiveness: Employer Involvement in Work/Family Issues." *Academy of Management Journal* (37), 350-382.

Granovetter, Mark S. (1985). "Economic Action and Social Structure: The Problem of Social Embeddedness." *America Journal of Sociology* (31), 481-510.

Grant, R.M. (1991). "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation." *California Management Review* (33:3), 114-135.

Graphic, Visualization, and Usability Centre. (1998). *9th WWW User Survey*, http://www.gvu.gatech.edu/user_surveys downloaded 03/15/2002.

Greenaway, K.E. (2002). "A Lost Opportunity? MIS Privacy Research in Three Journals, 1995-2000." Conference presentation to *2002 Academy of Management Conference*, Denver, Colorado, August 2002.

Greenaway, K.E., P. Cunningham, and Y.E. Chan. (2002). "Privacy Orientation: A Competing Values Explanation of Why Organizations Vary in Their Treatment of Customer Information." Conference presentation to *2002 AMA Marketing and Public Policy Conference*, Atlanta, Georgia, May 2002.

Greenberg, J. (1987). "A Taxonomy of Organizational Justice Theories." *Academy of Management Review* (12:1), 9-22.

Greenman, C. (1999). "On the Net, Curiosity Has a Price: Registration." *New York Times*, (Dec. 23), E8.

Guba, E.G. and Y.S. Lincoln. (1994). "Competing Paradigms in Qualitative Research." In *Handbook of Qualitative Research* , N.K. Denzin and Y.S. Lincoln (Eds.). Thousand Oaks: Sage, 105-117.

Gulati, R, N. Nohria, and A. Zaheer. (2000). "Strategic Networks." *Strategic Management Journal* (21), 203-215.

Hambrick, D.C. (1989). "Guest Editor's Introduction: Putting Top Managers Back in the Strategy Picture." *Strategic Management Journal* (10: Special Issue), 5-15.

Hambrick, Donald C. and Phyllis A. Mason. (1984). "Upper Echelons: The Organization as a Reflection of Its Top Managers." *Academy of Management Review* (9:2), 193-206.

Hamel G. and C.K. Prahalad. (1994). *Competing for the Future.* Cambridge, MA: Harvard Business School Press.

Handelman, J.M. and S.J. Arnold. (1999). "The Role of Marketing Actions with a Social Dimension: Appeals to the Institutional Environment." *Journal of Marketing* (63:January), 33-48.

Hann, I., K. Hui, T.S. Lee, and I.P.L. Png. (2002). "Online Information Privacy: Measuring the Cost-Benefit Trade-Off." *2002 Twenty-Third International Conference on Information Systems*, Barcelona, Span, 1 -10.

Hannan, M.T. and J. Freeman. (1977). "The Population Ecology of Organizations." *American Journal of Sociology* (82), 929-964.

Haunschild, P.R. (1993). "Interorganizational Imitation: The Impact of Interlocks on Corporate Accounting Activity." *Administrative Science Quarterly* (38:4).

Haveman, H.A. (1993). "Organizational Size and Change: Diversification in the Savings and Loan Industry after Deregulation." *Administrative Science Quarterly* (38:4).

Heart and Stroke Foundation. (2003). "Case Study: A Roadmap to Privacy Compliance." *Privacy Conference*, Canadian Marketing Association, Toronto, ON, September 18, 2003.

Hine, C. and J. Eve. (1998). "Privacy on the Marketplace." *The Information Society* (14:4), 253-262.

Hitt, M.A., M.T. Dacin, E. Levitas, J.L. Arregele, and A. Borza. (2000). "Partner Selection in Emerging and Developed Market Contexts: Resource-Based and Organizational Learning Pespectives." *Academy of Management Journal* (43:3), 449-467.

Hoffman, Donna L., Thomas P. Novak, and Marcos Peralta. (1999). "Building Consumer Trust Online." *Communications of the ACM* (42:4), 80-85.

Hofstede, Geert. (1984). *Culture's Consequences: International Differences in Work Related Values*. Beverly Hills, CA: Sage Publications.

Hofstede,G., B. Neuijen, D.D. Ohayv, and G. Sanders. (1990). "Measuring Organizational Cultures: A Qualitative and Quantitative Study Across Twenty Cases." *Administrative Science Quarterly* (35:2), 286-317.

Homburg, C., J.P. Workman and Harley Krohmer. (1999). "Marketing's Influence Within the Firm." *Journal of Marketing* (63:April), 1-17.

Horovitz, J. (1998). "Using Information to Bond with Customers." In *Competing with Information: A Manager's Guide to Creating Business Value with Information Content,* D. Marchand (Ed.). London: Wiley.

Hunt, S.D. and R.M. Morgan. (1996). "The Resource-Advantage Theory of Competition:

Dynamics, Path Dependencies, and Evolutionary Dimensions." *Journal of Marketing* (60:4), 107-114.

Itami, Hiroyuki (with Thomas W. Roehl). (1987). *Mobilizing Invisible Assets*. Cambridge, MA: Harvard University Press.

Ives, B. and S. Jarvenpaa. (1991). "Applications of Global Information Technology: Key Issues for Management." *Management Information Systems Quarterly* (15:1), 33-49.

Jarvenpaa, S.L. and D.E. Leidner. (1998). "An Information Company in Mexico: Extending the Resource-Based View of the Firm to a Developing Country Context." *Information Systems Research* (9:4), 342-361.

Jick, T. D. (1979). "Mixing Qualitative and Quantitative Methods: Triangulation in Action." *Administrative Science Quarterly* (24:4), 602-611.

Kaplan, R.S. and D.P. Norton. (1996). *The Balanced Scorecard: Translating Strategy into Action*. Cambridge, MA: Harvard Business Press.

Keen P. (1980). "MIS Research: Reference Disciplines and A Cumulative Tradition." In *Proceedings of the First International Conference on Information* Systems, E.R. McLean (Ed.), 9-18.

Keen, P. and R. Macintosh. (2001). *The Freedom Economy: Gaining the M-Commerce Edge in the Era of the Wireless Internet*. Berkeley: Osborne/McGraw-Hill.

Keeney, R.L. (1994). "Creativity in Decision Making with Value focused Thinking." *Sloan Management Review* (Summer), 33-41.

Kilmann, R. (with M.J. Saxton). (1985). *Gaining Control of the Corporate Culture*. San Francisco: Jossey-Bass.

Kohli, A.K. and B.J. Jaworski. (1990). "Market Orientation: The Construct, Research Propositions, and Managerial Implications." *Journal of Marketing* (54:April), 1-18.

Kotler, P. (1994). *Marketing Management: Analysis, Planning, Implementation and Control.* Englewood Cliffs NJ: Prentice-Hall.

Kumar, K., R. Subramanian, and C. Yauger. (1998). "Explaining the Market Orientation-Performance Relationship: A Context-Specific Study." *Journal of Management* (24:2), 201-233.

Lacity, M.C. and M.A. Janson. (1994). "Understanding Qualitative Data: A Framework of Text Analysis Methods." *Journal of Management Information Systems* (11:2), 137.

Lacity, M.C. and R. Hirschheim. (1993). *Information Systems Outsourcing: Myths, Metaphors and Realities*. Chichester, U.K.: Wiley.

Langley, A. (1989). "In Search of Rationality: The Purpose Behind the Use of Formal Analysis." *Administrative Science Quarterly* (34:2).

Laudon, K.C. (1996). "Markets and Privacy." *Communications of the ACM* (39:9), 92-104.

Lee, A. (1999). "Rigor and Relevance in MIS Research: Beyond the Approach of Positivism Alone." *Management Information Systems Quarterly* (23:1), 29-34.

Leedy, P.D. (1997). *Practical Research Planning and Design (6th ed)*. Upper Saddle River, NJ: Prentice Hall.

Leizerov, S. (2001). "The Institutionalization of Conflicts in Cyberspace: A Study of the Conflict Over Online Privacy." Unpublished Dissertation. George Mason University.

Leonard-Barton, D. (1992). "Core Capabilities and Core Rigidities: A Paradox in Managing New Product Development." *Strategic Management Journal* (13), 111-125.

Lewicki, R.J., D.J. McAllister and R.J. Bies. (1998). "Trust and Distrust: New Relationships and Realities." *Academy of Management Review* (23:3), 438-458.

Lincoln, Y.S. and E.G. Guba. (1985). *Naturalistic Inquiry*. Beverly Hills: Sage.

Lind, E.A. and T.R. Tyler. (1988). *The Social Psychology of Procedural Justice*. New York:

Plenum.

Livingston, S.N. (2002). "The Protection of Personal Identifying Information Through Posted Internet Privacy Policies." Unpublished dissertation. Capella University.

March, J.G. (1991). "Exploration and Exploitation in Organizational Learning." *Organization. Science* (2), 71-87.

March, J.G. and H.A. Simon. (1958). *Organizations*. New York: Wiley.

Marchand, D. (1998). "Creating Business Value with Information." In *Competing with Information: A Manager's Guide to Creating Business Value with Information Content*, D. Marchand (Ed.). London: Wiley.

Markus, M.L. and A.S. Lee. (1999). "Special Issue on Intensive Research in Information Systems: Using Qualitative, Interpretive and Case Methods to Study Information Technology Foreward [sic]." *Management Information Systems Quarterly* (23:1), 35-38.

Marx, G. (1999). "Ethics for the New Surveillance." In *Visions of Privacy* , C.J. Bennett and R. Grant (Eds.). Toronto: University of Toronto Press, 39-67.

Mason, R.O. (1986). "Four Ethical Issues of the Information Age." *Management Information Systems Quarterly* (10:1), 4-12.

Mason, R.O. and I.I. Mitroff. (1981). *Challenging Strategic Planning Assumptions*. New York: Wiley.

Mason, R.O., M.J. Culnan, S., Ang, and F. Mason. (2000). "Privacy in the Age of the Internet." In *Information Technology and the Future Enterprise*, G.W. Dickson, and G. DeSanctis (Eds.). Upper Saddle River, NJ: Prentice Hall, 208-238.

Mata, F.J., W.L. Fuerst, and J.B. Barney. (1995). "Information Technology and Sustained Competitive Advantage." *Management Information Systems Quarterly* (December), 487-505.

Mayer, R., J. Davis, and F. Schoorman. (1995). "An Integrative Model of Organizational Trust." *Academy of Management Review* (20:3), 709-734.

McDonald, Gael. (2000). "Business Ethics: Practical Proposals for Organizations." *Journal of Business Ethics* (25), 169-184.

McGahan, A.M. and M.E. Porter. (1998). "How Much Does Industry Matter Really?" *Strategic Management Journal* (18:51), 15-30.

Meyer, J.W. and B. Rowan. (1977). "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony." *American Journal of Sociology* (83:2) 340-363.

Middlemiss, J. (2001). "RBC Pilots Online Privacy Tools Program." *Bank Systems and Technology Online*, December 7, 2001, downloaded from http://www.banktech.com/story/BNK20011207S0004, accessed January 2003.

Milberg, S.J., H.J. Smith, and S.J. Burke. (2000). "Information Privacy: Corporate Management and National Regulation." *Organization Science* (11:1), 35-57.

Miles, R.E. and C.C. Snow. (1978). *Organizational Strategy, Structure, and Process*. New York: McGraw-Hill Publishing.

Miller, D., R. Eisenstat, and N. Foote. (2002). "Strategy from the Inside Out." *California Management Review* (44: Spring), 37-54.

Miller, D. and J. Shamsie. (1996). "The Resource-Based View of the Firming Two Environments: The Hollywood Film Studios from 1936-1965." *Academy of Management Journal* (39:3), 519-543.

Milne, G. (2000). "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue." *Journal of Public Policy and Marketing* (19:1), 1-6.

Milne, G. and M. Boza. (1999). "Trust and Concern in Consumers' Perceptions of Marketing

Information Management Practices." *Journal of Interactive Marketing* (13:1), 5-24.

Milne, G. and M.J. Culnan. (2002). "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Sweeps." *The Information Society* (18:5), 345-360.

Milne, G. and M.J. Culnan. (2004). "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* (18:2), 15-29.

Mintzberg, H. (1998), *Strategy Safari*. New York: the Free Press.

Miyazaki, A.D. and A. Fernandez. (2000). "Internet Privacy and Security: An Examination of Online Retailer Disclosures." *Journal of Public Policy and Marketing* (19:1), 54-61.

Mizruchi, M.S. (1989). "Similarity of Political Behavior Among Large American Corporations." *American Journal of Sociology* (95:2).

Morse, J.M. (1994). "Designing Funded Qualitative Research." In *Handbook of Qualitative Research,* N.K. Denzin and Y.S. Guba (Eds.). Thousand Oaks: Sage, 220- 235.

Nahapiet, J. and S. Ghoshal. (1998). "Social Capital, Intellectual Capital, and the Organizational Advantage." *Academy of Management Review* (23:2), 242-266.

Nakra, P. (2001). "Consumer Privacy Rights: CPR and the Age of the Internet." *Management Decision* (39:4), 272-278.

Narver, J. C. and Stanley F. Slater. (1990). "The Effect of Market Orientation on Business Profitability." *Journal of Marketing* (54:October), 20-35.

Nohria, N. and R. Gulati. (1996). "Is Slack Good or Bad for Innovation." *Academy of Management Journal* (39:5), 1245-1264.

Oliver, C. (1991). "Strategic Responses to Institutional Processes." *Academy of Management Review* (16), 145-179.

Oliver, C. (1997). "Sustainable Competitive Advantage: Combining Institutional and Resource-Based Views." *Strategic Management Journal* (18:9), 697-713.

Orlikowski, W.J. and S.R.. Barley. (2001). "Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn From Each Other?" *Management Information Systems Quarterly* (25:2), 145-165.

Orlikowski, W.J. and J.J. Baroudi. (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." *Information Systems Research* (2:1), 1-28.

Ouchi, W.G. (1980). "Markets, Bureaucracies, and Clans." *Administrative Science Quarterly* (25), 129-141.

Patton, M.Q. (1990). *Qualitative Evaluation and Research Methods* (2nd ed.). Newbury Park, CA.: Sage.

Penrose, E.T. (1959). *The Theory of the Growth of the Firm*. New York: Wiley.

Perrin, S., H.H. Black, D.H. Flaherty, and T.M.Rankin. (2001). *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*. Toronto: Irwin Law, Inc.

Perrow, C. (1985). "Review Essay: Overboard with Myth and Symbols." *American Journal of Sociology* (91), 151-155.

Pettigrew, A.M. (1987). "Context and Action in the Transformation of the Firm." *Journal of Managerial Studies* (24:6), 649-670.

Pfeffer, J. (1992). *Managing with Power: Politics and Influence in Organizations*. Boston, MA: Harvard Business School Press.

Pfeffer, J. (1997). *New Directions for Organization Theory*. New York: Oxford University Press.

Phelps, J., G. Nowak and El. Ferrell. (2000). "Privacy Concerns and Consumer Willingness to Provide Personal Information." *Journal of Public Policy and Marketing* (19:1), 27-41.

Pheysey, D.C. (1993). *Organizational Culture: Types and Transformations*, London: Routledge.

Porter, M.E. (1980). *Competitive Strategy: Techniques for Analyzing Industries and Competitors.* New York: Free Press.

Porter, M.E. (1985). *Competitive Advantage.* New York: Free Press.

Prahalad, C.K. and G. Hamel. (1990). "The Core Competence of the Corporation." *Harvard Business Review* (68:3), 79-91.

Prakash, A. (2000). "Responsible Care: An Assessment." *Business and Society* (39:2), 183-209.

Quinn, R.E. and J. Rohrbaugh. (1983). "A Spatial Model of Effectiveness Criteria: Toward a Competing Values Approach to Organizational Analysis." *Management Science* (29), 363-377.

Ranganathan,C. and S. Ganapathy. (2002). "Key Dimensions of Business-to-Consumer Websites." *Information & Management* (39), 457-465.

Rao, H. (1994). "The Social Construction of Reputation: Certification Contest, Legitimation, and the Survival of Organizations in the American Automobile Industry: 1895-1912." *Strategic Management Journal* (15), 29-44.

Robey, D. and M. Boudreau. (1999). "Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications." *Information Systems Research* (10:2), 167-185.

Robinson, S.L. (1996). "Trust and Breach of the Psychological Contract." *Administrative Science Quarterly* (41:December), 574-590.

Rouse, M.J. and U.S. Daellanbach. (1999). "Rethinking Research Methods for the Resource-Based Perspective: Isolating Sources of Sustainable Competitive Advantage." *Strategic Management Journal* (20), 487-494.

Ruef, M. and W.R. Scott. (1998). "A Multidimensional Model of Organizational Legitimacy: Hospital Survival in Changing Institutional Environments." *Administrative Science*

Quarterly (43), 877-904.

Rugman, A. and A. Verbeke. (1998). "Corporate Strategies and Environmental Regulations: An Organizing Framework." *Strategic Management Journal* (19:4), 363-375.

Rule, J. and Hunter, L.(1999). "Property Rights in Personal Data." In *Visions of Privacy,* C.J. Bennett and R. Grant (Eds.). Toronto: University of Toronto Press, 168-181.

Ryker, R., E. Lafleur, B. McManis, and K.C. Cox. (2002). "Online Privacy Policies: An Assessment of the Fortune E-50." *Journal of Computer Information Systems* (Summer) 15-20.

Sabherwal, R. and Y. Chan. (2001). "Alignment Between Business and IS Strategies: A Study of Prospectors, Analyzers, and Defenders." *Information Systems Research* (12:1), 11-33.

Salant, P. and D.A. Dillman. (1994). *How to Conduct Your Own Survey*. New York: Wiley.

Scott, W.R. (1987). "The Adolescence of Institutional Theory." *Administrative Science Quarterly* (32:4), 493-511.

Scott, W. R. (2001). *Institutions and Organizations* (2nd ed.). Thousand Oaks, CA: Sage.

Sheehan, K.B. and M.G.Hoy. (2000). "Dimensions of Privacy Concern Among Online Consumers." *Journal of Public Policy and Marketing* (19:1), 62-73.

Slater, S.F. and J.C. Narver. (2000). "Intelligence Generation and Superior Customer Value." *Journal of the Academy of Marketing Science* (28:1), 120-127.

Smith, H.J. (1990). "Managing Information: A Study of Personal Information Privacy." Unpublished dissertation, Harvard Business School.

Smith, H.J. (1993). "Privacy Policies and Practices: Inside the Organizational Maze." *Communications of the ACM* (36:12), 105-122.

Smith, H.J. and J. Hasnas. (1999). "Ethics and Information Systems: The Corporate Domain."

Management Information Systems Quarterly (23:1),109-127.

Smith, H.J., S.J. Milberg, and S.J. Burke. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *Management Information Systems Quarterly* (20:2),167-196.

Smith, N.C. (1995). "Marketing Strategies for the Ethics Era." *Sloan Management Review* (36:4), 85-97.

Srivastava, R.K., T. Shervani, and L. Fahey. (1998). "Market-Based Assets and Shareholder Value: A Framework for Analysis." *Journal of Marketing* (62:1), 2-18.

Srivastava, R.K., L. Fahey and H.K. Christensen. (2001). "The Resource-Based View and Marketing: The Role of Market-Based Assets in Gaining Competitive Advantage." *Journal of Management* (27), 777-802.

Srivastava, R.P. and T.J. Mock. (2000). "Evidential Reasoning for WebTrust Assurance Services." *Journal of Management Information Systems* (16:3), 11-32.

Stewart , K.A. and A.H. Segars. (2002). "An Empirical Examination of the Concern for Privacy Instrument." *Information Systems Research* (13:1), 36-49.

Stewart, S. and D. Akin (2004). "Damage Control Time at CIBC." *Globe & Mail* downloaded from www.globeandmail.com accessed November 29, 2004.

Stone, E.F., D.G. Gardner, H.G. Gueutal, and S. McClure. (1983). "A Field Experiment Comparing Information-Privacy Values, Beliefs and Attitudes Across Several Types of Organizations." *Journal of Applied Psychology* (68:3), 459-468.

Stone, E.F. and D.L. Stone. (1990). "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms." In *Research in Personnel and Human Resource Management,* G.R. Ferris (Ed.), 8, 349-411.Greenwich, CT: JAI Press.

Straub, D. and R.W. Collins. (1990). "Key Information Liability Issues Facing Managers: Software and Proprietary Databases, and Individual Rights to Privacy." *Management Information Systems Quarterly* (22:4), 441-470.

Suchman, M.C. (1995). "Managing Legitimacy: Strategies and Institutional Approaches." *Academy of Management Review* (20), 571-610.

Sveiby, K.E. (1997). *The New Organizational Wealth.* San Francisco, CA: Berrett-Koehler.

Tam, E., K. Hui and B.C.Y. Tan. (2002). "What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses." *Twenty Third International Conference on Information Systems*, Barcelona Spain, 11-21.

Tedeschi, B. (2002). "Everybody Talks About Online Privacy, But Few Do Anything About It." *New York Times* (June 3, 2002). Accessed Jan.23, 2003.

Teece, D.J. and G. Pisano. (1998). "The Dynamic Capabilities of Firms: An Introduction." In *Technology, Organization and Competitiveness,* G. Dosi, D.J. Teece and J. Chytry (Eds.). Oxford: Oxford University Press, 193-212.

Teece, D.J., G. Pisano, and A. Shuen. (1997). "Dynamic Capabilities and Strategic Management." *Strategic Management Journal* (18:7), 509-533.

Thomas, D.M. and R.T. Watson. (2002). "Q-Sorting and MIS Research: A Primer." *Communications of the AIS* (8), 141-156.

Tolbert, P.S. and L.G. Zucker. (1996). "The Institutionalization of Institutional Theory." In *Handbook of Organizational Studies*, Stewart R. Clegg, Cynthia Hardy and Walter R. Nord (Eds.). Thousand Oaks, CA: Sage, 175-190.

Trice, H.M. and J.M. Beyer. (1993). *The Cultures of Work Organizations*. Englewood Cliffs, NJ: Prentice Hall.

Victor, B. and J.B. Cullen. (1987). "A Theory of the Measure of Ethical Climate in

Organizations." In *Research in Corporate Social Performance and Policy*, W.C. Frederick and L.E. Preston (Eds.). Greenwich, CT: JAI Press, 51-71.

Walczuch, R.M. and L. Steeghs. (2001). "Implications of the New EU Directive on Data Protection for Multinational Corporations." *Information Technology & People* (14:2), 142-162.

Weaver, G.R., L.K. Trevino and P. Cochran. (1999). "Integrated and Decoupled Corporate Social Performance: Management Commitments, External Pressures, and Corporate Ethics Practices." *Academy of Management Journal* (42:5), 539-552.

Webster, J. (1998). "Desktop Videoconferencing: Experiences of Complete Users, Wary Users and Non-Users." *Management Information Systems Quarterly* (22:3), 257-286.

Webster, J. and Deborah Compeau. (1996). "Computer-Assisted Versus Paper-and-Pencil Administration of Questionnaires." *Behavior Research Methods, Instruments & Computers* (28:4), 567-576.

Webster, J. and R.T. Watson. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *Management Information Systems Quarterly* (26:2), iii-xiii.

Weick, K. (1984)."Theoretical Assumptions and Research Methodology Selection." In *The Information Systems Research Challenge,* F. Warren McFarlan (Ed.). Boston: Harvard Business School Press, 115.

Wernerfelt, B. (1992). "A Resource-Based View of the Firm." *Management Journal* (5:2), 171-180.

Westin, A. (1967). *Privacy and Freedom*. New York: Athenaeum.

Winbush, J.C., J.M. Shapard, and S.E. Markham. (1997). "An Empirical Examination of the Multi-dimensionality of Ethical Climate in Organizations." *Journal of Business Ethics* (16), 67-77.

Wright, J. (2003). "Creating Privacy Practices That Work in the Real World." *Privacy Conference*, Canadian Marketing Association, Toronto, ON, September 18, 2003.

Yin, Robert K. (1994). *Case Study Research Design and Methods (2nd edition)*. Thousand Oaks: Sage Publications.

Zucker, Lyn G. (1986). "Production of Trust: Institutional Sources of Economic Structure, 1840-1920." In R*esearch in Organizational Behavior (8)*, Barry M. Staw and L.L. Cummings (Eds.). Greenwich, CT: JAI Press, 53-111.

INFORMATION PRIVACY ORIENTATION

by

KATHLEEN ERIN GREENAWAY

Volume 2

A thesis submitted to the Department of Management

in conformity with the requirements for the degree

of Doctor of Philosophy

Queen's University

Kingston, Ontario, Canada

December, 2004

TABLE OF CONTENTS

VOLUME II

Appendix A: Consumer Level Studies Summary 373
Appendix B: Organizational Level Studies Summary 381
Appendix C: Sectoral/National Studies Summary 385
Appendix D: Background to Information Privacy Principles 391
Appendix E: Differences Between Chartered Banks and Credit Unions 393
Appendix F: Canadian Domestic Banks 395
Appendix G: Top 20 Canadian Credit Unions 397
Appendix H: Research Methods – Validating and Adapting Instruments 400
Appendix H-1: Data Collection Strategy: Interviews (Initial Version) 401
Appendix H-2: Data Collection Strategy (Revised) – Basic Interview for All Participants 405
Appendix H-3: Summary of IPO Guide and IPO Survey Instrument Validation Pre-Test Participants 410
Appendix H-4: IPO Interview Guides: General Content Improvements from Pre-Test 412
Appendix H-5: IPO Interview Guides: Specific Guide Content Improvements from Pre-Test 414
Appendix H-6: IPO Interview Guide: Construction Issues from Pre-Test 417
Appendix H-7: Questionnaire Revisions and Improvements During and After Research Visit (Based on Case A Experience) 418
Appendix H-8: IPO Interview Guides (Examples of Questions) 421
Appendix H-8.1 Basic 421
Appendix H-8.2 Privacy Professionals 425
Appendix H-8.3 IT/Information Management/Information Security Functions 427
Appendix H-9: Draft Initial IPO Survey Instrument for Information Privacy Orientation 428
Appendix H-10: IPO Survey Instrument Construction – Card Sort Description and Results 433
Appendix H-11: Questionnaire Item Sorting Instructions 446
Appendix H-12: IPO Survey Instrument – Content Improvements from Pre-Test 452
Appendix H-13: Final Version of IPO Survey – Procedure (Paper-and-Pencil Survey) 453
Appendix H-14: Final Version of IPO Survey Instrument 454
Appendix H-15: IPO Survey Instrument – Web-Based Version 467
Appendix I: Research Sites Recruitment 475
Appendix I-1: Request for Participation 476
Appendix I-2: Invitation Letter 479
Appendix I-3: Research Project Summary 480
Appendix I-4: Research Site Requirements 482
Appendix I-5: Confidentiality & Non-Disclosure Agreement 484
Appendix J: Phase One Privacy Policy Evaluation Study – Detailed Findings 491
Appendix J-1: Phase One Privacy Policies Evaluation Study - Evaluation Form 492
Appendix J-1.1 Firm 1 501
Appendix J-1.2 Firm 2 505
Appendix J-1.3 Firm 3 509

Appendix J-1.4 Firm 4 513
Appendix J-1.5 Firm 5 517
Appendix J-1.6 Firm 6 522
Appendix J-1.7 Firm 7 526
Appendix J-1.8 Firm 8 530
Appendix J-1.9 Firm 9 534
Appendix J-1.10 Firm 10 538
Appendix K: Case A (Pilot Study) - Supplementary Information from Case Study Database 542
Appendix K-1: Case A - Research Setting and Site Visit 543
Appendix K-2: Case A – Case A - Interviews 544
Appendix K-3: Case A - Distribution of Completed Surveys 544
Appendix K-4: Case A - Survey Respondent Characteristics 545
Appendix K-5: Case A - Desirable Privacy Documents 546
Appendix K-6: Case A - Frequencies and Means from IPO Survey 547
Appendix L: Case B - Supplementary Information from Case Study Database 551
Appendix L-1: Case B - Research Setting and Site Visit 552
Appendix L-2: Case B - Interviews 556
Appendix L-3: Case B - Distribution of Completed Surveys 556
Appendix L-4: Case B - Survey Respondent Characteristics 557
Appendix L-5: Case B - Privacy Documents 558
Appendix L-6: Case B - Frequencies and Means from IPO Survey 560
Appendix M: Case C - Supplementary Information from Case Study Database 564
Appendix M-1: Case C - Research Setting and Site Visit 565
Appendix M-2: Case C - Interviews 568
Appendix M-3: Case C - Documents 569
Appendix N: Case D - Supplementary Information from Case Study Database 573
Appendix N-1: Case D - Research Setting and Site Visit 574
Appendix N-2: Case D - Interviews 577
Appendix N-3: Case D - Survey Respondent Characteristics 578
Appendix N-4: Case D - Privacy Documents 579
Appendix N-5: Case D - Frequencies and Means from IPO Survey 580

Appendix A: Consumer Level Studies Summary
(By order of appearance in Chapter Two)

Study	Type, purpose, sample	Theory & Variables	Results/Conclusions
Culnan (1993)	Empirical, quantitative, exploratory survey using undergraduate students (n=126) to distinguish between those who object to secondary data use and those who don't in direct mail circumstance	• **Categorization Theory** (Dutton & Jackson 1987): gain-loss, positive-negative, controllable-uncontrollable • **Concern for privacy** (IV): addresses shoppers' general concern for privacy, their perceptions of loss of control over personal information and specifically their perceptions of whether firms should use data for secondary use • **Attitudes to direct mail marketing** (IV): that measured overall perceptions of direct mail, whether catalogue shopping was perceived positively or negatively, and the perceived ability of the shopper to control direct mail marketing. • **Demographics** (control): whether the shopper had had a previous negative experience (i.e., a privacy invasion) • **Attitudes to 2ndary info** use (DV): Measured sensitivity to use (positive or negative)	• **CONTROL** as a core dimension underlying attitudes toward privacy; i.e., know how to get name off a list (perceptions of control correlate with lower privacy concerns) • Respondents with a greater concern for privacy, with a more negative attitude towards direct mail marketing, and who had previous negative privacy experiences were more likely to have negative attitude (be more sensitive to) to secondary information use
Culnan & Armstrong (1999)	Empirical, quantitative, theory building Secondary data analysis of 1994 public opinion survey (respondents were prospective subscribers to interactive home information services)	• Organization justice → procedural justice → procedural fairness • "Procedural fairness" creates a *privacy leverage point* that organizations can exploit (creating a willingness in individuals to disclose personal info by disclosing its information policies thereby creating trust)– *privacy calculus* is an assessment that their personal information will subsequently be used fairly and they will not suffer negative consequences	• "Procedural fairness can be used to address privacy concerns, and when FIP are observed, customers will be more willing to continue in a relationship with a firm, allowing the firm to benefit from the collection and use of data that results from the relationship" • Notice and consent provisions of FIP support procedural fairness (as consumer control points)

Appendix A cont'd

Culnan & Armstrong (1999) Cont'd		Dependent Variables: • Willingness to be profiled if FIP used • Willingness to be profiled if no FIP used Independent Variables: • Direct Marketing Experience • Concern for Privacy	• When advised that FIP would be used, only prior experience distinguished those willing to be profiled from those who were unwilling • When not advised specifically that FIP would be used, both privacy and prior experience distinguished those willing to be profiled from those who were unwilling
Smith, Milberg & Burke (1996)	Quantitative, development of a 15 item instrument that measures the primary dimensions of individuals' concerns about the privacy practices of organizations	The different dimensions were developed based on the 1972 Code of Fair Information Practices developed by the U.S. Department of Health, Education and Welfare (which underpin the FTC's F.I.P.) and an extensive literature review.	• Developed "Concern for Information Privacy" (CFIP) Instrument • Found four factors that made up individual concern 1. **COLLECTION**: concern that extensive amounts of personally identifiable data are being collected and stored in databases 2. **ERRORS:** Concern that protections against deliberate and accidental errors in personal data are inadequate 3. **UNAUTHORIZED SECONDARY USE**: concern that information is collected from individuals for one purpose but is used for another, secondary purpose either internally within an organization or after disclosure to an external party without authorization from individuals 4. **IMPROPER ACCESS**: Concern that data about individuals are readily available to people not properly authorized to view or work with this data

Appendix A cont'd

Stewart & Segars (2002)	Empirical, quantitative, validation and reconsideration of Smith et al. (1996) concern for information privacy instrument (CFIP); 355 usable surveys of consumers in mall intercept study at four sites in U.S.	Reconceptualized theory using (Hoffman et al. 1999): • **Environmental Control** – consumer's ability to control the actions of other people in the environment during a market exchange (p.38) • **Secondary Use of Information Control** - consumer's ability to control dissemination of information related to or provided during transaction (p.38)	• Confirmed initial item measures from Smith et al. • Determined that CFIP is a second order factor madel • CFIP can be defined as more than four distinct factors – consists of the four factors as well as the structure of interrelationships among the factors (p.39) • Consumers are concerned about all four of these dimensions simultaneously, and not individually as Smith et al.'s first order model suggested.
Sheehan & Hoy (2000)	Empirical, quantitative, 889 usable email surveys to assess influences on consumer online privacy	Independent Variables: Influences on consumer privacy • **Awareness of Information Collection** – consumer's extent of awareness that information is being collected about them (p.63) • **Information Usage** – consumer's understanding of the use being made of their information (p.63) • **Information Sensitivity** – "the level of privacy concern an individual feels for a type of data in a given specific situation" (p.64) • **Familiarity with Entity** – the degree to which consumer's trust the organization collecting the data based on knowing about the organization (p.64) • **Compensation** – the nature of the benefit being offered in exchange for information (p.64) Dependent Variables: **Privacy concern** – low, medium high	Found 3 factors: 1. **Control over collection and usage of information** – (32.8% of variance) – it is important to consumers to maintain control (consistent with previous research) But , users do not consider all information equal 2. **Short term transactional relationship** – (27.3% of variance) – willing to give out unimportant (i.e. email address) in exchange for a benefit (i.e. gift, entry into a contest) 3. **Established long term relationship** - (14.2% of variance) – consumer less likely to view messages from firms as privacy intrusive if they have an established relationship with the firm or have provided consent via giving email address

Appendix A cont'd

Dinev & Hart (2003)	Empirical, quantitative, U.S.-based survey (3 studies) to develop and test a model of tradeoff factors to predict Internet use based on privacy factors	Based on Culnan and Armstrong (1999) "consumer privacy calculus" Theorize a "Model of Internet Use" (p.13) Antecedents • **Perceptions of vulnerability** – Internet users' concern for the risks associated with the misuse of their personal information (p.6) • **Ability to control** - consumer's ability to limit the amount if information disclosed and the uses to which the information is put by the collecting organizations (p.7) Leading to: • **Privacy Concerns** – the collection of customer anxieties about how their personal information is collected, used and reused with or without their consent in order to obtain products, services and information (p.8) • **Trust** – belief that another party will act in an anticipated way (p.9) • **Interest** – customer's personal interest in receiving the benefits of the products, services and information sufficient to provide personal information (p.12) Culminating in DV: • **Internet Use** – the likelihood of engaging in Internet commerce (p. 13) Demographic variables for control: Race, age, education, income, occupation, employment	Confirmatory factor analysis: • Positive relationship between users' perceptions of Vulnerability and Privacy Concerns • Negative relationship between users' perceptions of Vulnerability and Trust in Internet vendor • Negative relationship between users' perceptions of Vulnerability and Internet Use • Positive relationship between users' perceptions of Control and Privacy Concerns • Positive relationship between users' perceptions of Control and Internet Use • Positive relationship between users' perceptions of Control and Trust • Positive relationship between Trust and Internet Use • Positive relationship between Level of Interest and Trust and Internet Use • Positive relationship between Level of and Internet Use

Appendix A cont'd

Dhillon, Bardacino & Hackney (2002)	Empirical, quantitative, exploratory interviews with 92 individuals with Internet shopping experience in U.S. and U.K.; assessed individual concerns for privacy based on their values for privacy when online shoopping	• Based study on **Value-focused** thinking approach (Keeney 1999)	Distinguish between two types of objectives as articulation of values – Means objectives and Fundamental objectives. Fundamental objective: Overall, maximize privacy when purchasing online (p.708) through 8 fundamental objectives including: 1. Maximize discreteness of transactions 2. Increase fraud prevention 3. Maximize reputation of firm 4. Decrease spam 5. Maximize security of personal information 6. Maximize shoppers' ability to control personal data 7. Maximize expectation of shopping privately 8. Maximize privacy relative to ease of online shopping
Tam, Hui, & Tan (2002)	Quantitative, development of a 32 item instrument to measure the motivation to disclose personal information; 371 undergraduate students	**Expectancy Theory** (p.12) – individuals pursue outcomes that maximize positive valences (such as positive benefits) and minimize negative valences (such as privacy invasions) (Stone and Stone 1990) **Economic Utility Theory** (p.12) – individuals maximize their total utility in making choices based on criteria such as time or money savings (Stigler 1950) **Motivation Theory:** Extrinsic Motivation – people seek benefits that are functionally instrumental to achieving other goals (p.12); operationalized as MONETARY SAVINGS; TIME SAVINGS, SELF-ENHANCEMENT, SOCIAL ADJUSTMENT	Consumers are motivated by: MONETARY SAVINGS; TIME SAVINGS (extrinsic motivators) PLEASURE (intrinsic motivator)

Appendix A cont'd

Tam, Hui, & Tan (2002) cont'd		Intrinsic Motivation – people seek to consume as its own end (p.12); operationalized as PLEASURE, NOVELTY, ALTRUISM	
Hann, Hui, Lee & Png (2002)	Empirical, quantitative, experiment about tradeoffs consumers are prepared to make with privacy disclosure	Economic theory	
Phelps, Nowak & Ferrell (2000)	Empirical, quantitative, 556 usable U.S.-based mail surveys about direct marketing and privacy issues (pre Internet)	Social Contract Theory (p.29): marketers should view consumers' exchange of personal information as an implied social contract (Culnan 1995; Milne 1997; Milne & Gordon 1993) Conceptual model for consumer privacy concerns: Input factors: • Type of personal information requested (demographic, lifestyle, purchase related, personal identifiers, financial) • Amount of information control offered • Potential consequences and benefits • Consumer characteristics Outcomes: • Beliefs regarding marketer's information practices • Overall concern level regarding the way companies use personal information Future outcomes: • Behavioral and attitudinal responses	Six factors are important correlates of PRIVACY CONCERN (p.38): 1. Type pf personal information requested 2. Consumers' ability and desire to control subsequent dissemination of personal information 3. Consumers' perceptions regarding marketers' knowledge about them and their interests 4. Consumers' attitudes toward direct mail 5. Consumers' preferences with respect to catalog and advertising mail volume 6. Previous name removal behavior • Consumers have privacy preferences involving control. • Consumers are willing to provide certain kinds of information (basic demographic info) but less willing top provide other (financial information and personal identifiers). • Consumers will make tradeoffs between privacy and convenience. • Education is the only demographic variable of significance: the greater the level of education, the greater the level of concern for privacy.

Appendix A cont'd

Ranganathan & Ganapathy (2002)	Empirical, quantitative survey using convenience sample of Illinois online shoppers who had made at least one online purchase in the previous 6 months (n=214) to determine the key characteristics of B to C web sites that matter to consumers	• **Information content**: what kinds of services, products, information or features on a website • **Design**: manner of presentation of the content • **Security**: technology features for assuring the security of financial transactions • **Privacy**: type and amount of personal information gathered as well as the privacy policies articulated	• Security was the best predictor of online purchase intent (particularly alternate payment option) (Discriminant loading = .65) • Privacy was the second best predictor discriminating between high and low purchase intentions (Discriminant loading = .58) • Design was the third • Information content was the fourth
Hine & Eve (1998)	Empirical, qualitative, 26 semistructured interviews with shoppers in the U.K.; discourse analytic approach (Wetherell & Potter 1992) to identifying emerging themes	• Privacy and privacy infringement are socially constructed, "Situated" phenomena. • **Privacy infringement**: made up of how "representations of the self, representations of the data-using organization, and the technology" are combined. • Perceptions of Privacy infringement depend on the social relations between customers and the firms that collect data from them and the customers understanding of the technology and use of the information.	Five factors contributed to the construction of an account about information collection: 1. **Visibility of Mediating Technology**: shopping loyalty cards were seen as benign but Internet was seen to be technologically threatening (loss of control over one's information). Explained as a function of customer knowledge of the technology. Familiar technology was less threatening and data collection capacities were rendered invisible. 2. **Legitimacy of Motives for Information Requests**: customers attributed motives for information gathering, largely expressed in terms of benefits received. The better able to articulate a direct personal benefit, the more likely not to characterize data collection as intrusive or illegitimate. 3. **Intrusion/disruption of legitimate activity**: Respondents characterized certain data collection activities (i.e. direct mail) as less intrusive because they perceived they had

Appendix A cont'd

Hine & Eve (1998) cont'd			control while other forms (telemarketing) were deemed illegitimate because they had less control. Firms were seen to be making "unreasonable assumptions" about how people want to spend their time (engaged in own activities versus answering unsolicited marketing phone calls). 4. **Imbalances of power and control**: involved both technology (the extent to which the respondent felt in control of or controlled by the technology) as well as the respondents feelings of being up to the task of taking control. 5. **Social Context**: Respondents constructed a social environment in which certain groups were seen to be more or less vulnerable (i.e. elderly) or more or less dangerous (i.e. burglars) as well as they reflected on their own capacities to manage within a privacy infringing context. *Perceptions of privacy* had to do with control and trust (of technology, of business). *Perceptions about the use of information* were based on conceptions of technology and the role of computers in society. Four repertoires were drawn on to construct an account of privacy infringement: **Benefit, Risk, Trust, Control**.

Appendix B: Organizational Level Studies Summary

(By order of appearance in Chapter Two)

Study	Type, purpose, sample	Theory & Variables	Results/Conclusions
Goldstein & Nolan (1975)	Opinion piece with managerial focus on dealing with information privacy as a result of early 1990 actions by US government	N/A	• Warned that privacy would be a big issue for companies and governments • Drew parallel with environmental protection activities • Narrow view of privacy • Four steps for organizations to deal with "personal privacy" (p.69) 1. Prepare a "privacy impact statement" 2. Construct a comprehensive privacy plan 3. Train employees who handle personal information 4. Make privacy a part of social responsibility programs
Ives & Jarvenpaa (1991)	Empirical, qualitative examination of global IT issues; 25 interviews with U.S. based senior managers	Key issues for global IT management (p.34): 1. linking global IT to global business strategy 2. IT platforms 3. **International data-sharing** 4. Cultural environments	Four types of international data sharing (p.37) (after Lerner 1984): 1. operations data 2. **personally identifiable data** 3. electronic transfers of money 4. technical and scientific data Identified "legal requirements" as a key business driver (p.40) using example of "information requirements mandated by laws .. necessitate corporate-wide information requirements "International data sharing" key issues include (p.44): Understand your responsibilities, limitations, and exposures vis-à-vis TDF and privacy laws.

Appendix B cont'd

Straub & Collins (1990)	Discussion piece examining legal aspects of computing	Key legal aspects of computing (p.144): 1. Intellectual property and software piracy 2. IP and downloading, 3. **Individual privacy rights**: how to collect and disseminate information on individuals while respecting individual rights to privacy	• Three main sources of managers' INFORMATION LIABILITY including "how to collect and disseminate information on individuals while respecting individual rights to privacy" (p.144) • Sources for privacy violation include security breaches, inaccurate data collection, inappropriate disclosure • Remedies/action by managers include security (both technical – access controls, cryptography; and policy including training, policies to encourage trust and honesty with employees); stewardship (lifecycle of information approach) and informed consent by data subjects. • Argues for the need for ethical perspective on privacy (as in ethics is the "right thing to do") but no specific ethical theory invoked
Bordoloi, Mykytyn & Mykytyn (1996)	Discussion piece examining legal aspects of computing	Key legal issue involves torts: • Torts of negligence (fault-based liability) • Strict product liability (no fault based liability)	• Companies can be held liable for incorrect information being used to make decisions or to generate other information (i.e., maps or reports) that other parties would use. • Reinforces the need for firms to follow strict practices to ensure that information is entered correctly into databases and to verify information before it is acted upon. (similar to FIP: verification)
Srivatava & Mock (2000)	Theoretical article provides framework for audit firms to use to provide independent third party assurance		• Four "categories of assertion" important for web assurance: 1. Soundness of business practices, 2. Ensuring transaction integrity, 3. Offering information protection, 4. Compliance with legal requirements.

Appendix B cont'd

Srivatava & Mock (2000) cont'd			• The information protection category generally follows fair information practice concerns including reference to ensuring that there is no unauthorized access to customer data and no improper use.
Cadogan (2001)	Evaluative, qualitative multiple case study, dissertation research; U.S. based websites (n=3) Amazon.com, Dell Computers, Online Privacy Alliance Readability of privacy policies is an "ethical" issue.	FTC F.I.P.: • Notice • Choice • Access • Security Readability indices: length, average length of sentences, Flesch-Kincaid grade level, Harris-Trottier readability Index, negative words, immediacy, vague and qualification	• Different organizations have different privacy approaches that are better or worse at addressing both the letter and spirit of F.I.P. • Different privacy approaches reveal differences in corporate privacy philosophy and organizational intentions. • Different privacy polices are more or less readable/understandable by consumers.
Smith (1993)	Empirical, qualitative, exploratory; 7 case study of U.S. based financial institutions (i.e., banks, credit cards, insurance); 105 semi-structured interviews Based on dissertation about how organizations handle sensitive personal information.	Research questions: 1. How are policies and practices regarding the use of personal information developed within the corporation? 2. How well are current corporate policies and practices meeting societal expectations with respect to uses of personal information?	Re: Research Question 1: Privacy Policy cycle (p.107) • Drift – "policy by least steps" • Threat – perception of threat of negative publicity or legislation • Reaction – policy with executive approval "Emotional dissonance" (p. 112) experienced by employees (especially IS staff) between personal values about privacy and organizational actions "Personal rationalization" (p.112) to compensate for emotional dissonance

Appendix B cont'd

Smith (1993) cont'd			Re: Research Question 2: Existence of policies – many non-existent or major gaps in content covering (p. 115) 1. Collection 2. New Use (same as secondary use) 3. Sharing (internal and "third party) 4. Deliberate Errors 5. Accidental Errors 6. Improper Access – computerized 7. Improper Access – hardcopy and oral 8. Reduced judgment Also, significant mismatch between official policies and actual practices/operations (p.118)

Appendix C: Sectoral/National Studies Summary

(By order of appearance in Chapter Two)

Study	Type & purpose	Timing	Sample	Variables	Results
FTC 1998	Evaluative, quantitative. Compliance with FTC's FIP	Mar. 1998	n=1,402 consumer websites 674 comprehensive sample 137 health, 142 retail, 125 financial, 212 children's, 111 most popular	Compliance with • Notice • Choice • Access • Security	• 97% of websites collected some personally identifiable information • 14% of websites posted privacy information (policies or statements)
GIPP 1999 (Culnan 1999a)	Evaluative, quantitative. Compliance with expanded FIP	Jan. 1999	Top consumer websites n=7500	Compliance with • Notice • Choice • Access • Security • Contact Information	• 92.8 % of websites collected some personally identifiable information • 34% of websites had no posted privacy policy • 14% had all five FIP elements
OPA 1999 (Culnan 1999b)	Evaluative, quantitative. Compliance with expanded O.P.A. industry guidelines (similar to GIPP)	Mar. 1999	Top consumer websites (32000 unduplicated visits per month) n=100 (taken from GIPP sample frame)	Compliance with OPA (1998) Industry Guidelines • Notice • Choice • Access • Security • Contact Information	• 99 % of websites collected some personally identifiable information • 93% of websites had posted privacy statements • 81% of websites had posted privacy policies • 22% had all four FTC FIP elements
FTC 2000	Evaluative, quantitative. Compliance with FTC's FIP	Jan. 2000	"Most popular" U.S. consumer websites (39000 unduplicated visits per month) n=100; Randomly selected U.S. consumer websites n=335	Compliance with • Notice • Choice • Access • Security	"Most Popular" sites • 45% addressed all four FIP • 45% displayed a webseal "Randomly selected" sites • 20% of addressed all four FIP • 8% displayed a webseal

Appendix C cont'd

Ryker et al. (2002)	Evaluative, quantitative. Compliance with FTC's FIP	Sept. 2000	Fortune magazine "e-50" B to C (n=35) B to B (n=15)	Full, partial and non-compliance with • Notice • Choice • Access • Security	B to C sites • 2% were fully compliant with all four FIP • 62.8% were partially compliant • 31.4% did not comply with even one of the four FIP • NOTICE was best practice (85.5% fully compliant) • CHOICE (42.8 %) • ACCESS was weakest practice (17.1%) • SECURITY (54.2%) B to B sites • 20% had a posted privacy statement • No statement was fully compliant
Miyazaki & Fernandez (2000)	Evaluative, quantitative. Whether and how privacy and security statements address consumer privacy concerns	Jan. & Feb. 1999	Consumer websites that took credit cards organized by 17 shopping categories (n=293) Randomly selected from 3 shopping portals (excite.com, yahoo.com, netscape.com)	Privacy concerns: • Identification • Unsolicited contacts • Information dissemination Company responses: • Technology for security • Guarantees against fraud • Alternate payment options	Privacy Statements • 49.8% of sites overall Of these: • 28% addressed identification • 40.3% addressed unsolicited contacts • 34.8% addressed information dissemination Security Statements • 78.5% of sites overall Of these: • 65.5% had secured transaction systems • 7.5% guaranteed reimbursement • 54.9% had alternate payment

Appendix C cont'd

Earp et al (2002)	Qualitative case study of healthcare sites using Goals-Based Requirements to identify organizational privacy goals	Not given	U.S. healthcare sites (n=23) B to C and B to B Pharmaceutical = 6 Health insurance = 7 Online Pharmacy = 10	• Privacy policies, • Privacy protection goals • Privacy obstacles representing organizational perspectives: • Legal • Technical • Business • Contractual Social	• 131 goal statements identified that appeared 403 times within the 23 policies Statements supported perspective: • 46% social • 23% technical • 20% contractual • 9% business • 3% legal • Legal statements dealt with vulnerability (obstacles) and not protection • Technical statements were evenly split between protection and obstacles
Alexander (2001)	Evaluative, quantitative dissertation research. What personal characteristics drive concerns? How can firms use privacy policies to address privacy concerns? Is there a difference in privacy statements between traditional and non-traditional firms? Developed a Privacy Consciousness Matrix.	2000	High traffic consumer websites used in previous FTC, GIPP studies (n=335) Survey questionnaire (n=100) Analyzed by: • Industry category • Industry type	FTC FIP: • Notice • Choice • Access • Security Dependent Variables – (CFIP) • Collection • Unauthorized use • Improper access • Errors Independent variables - Gender, Negative personal experience, trust, previous personal activity, Computer use, computer experience, computer skill, active internet user, corporate culture, age	• Negative personal experience correlated to all four concerns (individually and overall) • Age of consumer correlated with secondary use and improper access concerns • Weekly internet use correlated with collection concerns • 70% of "traditional firms" (online and physical firms) posted privacy policies • 56% of "cyber" firms (online only) posted privacy policies • Traditional firms were better at addressing • Most privacy policies are concerned with NOTICE and CHOICE which address only "Collection" concern Traditional firms dealt better with NOTICE and CHOICE

Appendix C cont'd

Livingston (2002)	Evaluative, qualitative dissertation research. Compliance with OECD principles. How readable or confusing are privacy policies?	Not given	U.S. based websites (n=41)	OECD principles: • Collection • Data quality • Purpose specification • Use limitation • Security safeguards • Openness • Individual Participation • Accountability Clarity of policy • States • Did not state • Appeared ambiguous	• A great diversity of privacy practices among the sites • Great variance in the comprehensiveness and clarity of the policies • None of the sites clearly (unambiguously) met all the OECD requirements
Leizerov (2001)	Evaluative, holistic case study. Examined extent to which the conflict of interest between firms and consumers over internet privacy has been institutionalized.	Not given	U.S. based websites randomly selected from within the "most popular" FTC sample and augmented to ensure • A minimum of 19 sites for each of 7 industry categories • Representation of 2 webseal programs (Truste, BBBonline) (n = 145)	FTC FIP: • Notice • Choice • Access • Security Commercial categories: • Industry • Commercial type • Ownership • Organization • Gender targeting • Affiliation Conflict Institutionalization: • Compliance and Attitude of compliance with regulations	COMPLIANCE to F.I.P: • Significant differences by industry. ATTITUDE to compliance: • Mixed results. • No industry difference except with permission to third parties to place cookies on users computers. • Commercial sites less likely to permit 3rd party cookies than "free information" sites. • Publicly held sites less likely to permit 3rd party cookies than "free information" sites.

Appendix C cont'd

Leizerov (2001) cont'd				Building of Social bonds: • Intrusiveness of data collection • Integrity • Trust building through responsible privacy practices • Transparency and competition for customers	BUILDING OF SOCIAL BONDS: • Industry differences for all four aspects. • Travel and retail sites least intrusive. • Travel and computer had highest integrity. • Retailers had greatest number of responsible privacy practices. • Retailers had greatest degree of transparency and competitive privacy behaviours. WEBSEAL members: • Significant differences between performance of members of different programs. • BBBonline members displayed greater compliance with FIP, had greater attitude to compliance, and made larger efforts at building social bonds than did Truste members. • Many non-members had greater compliance and displayed greater effort at building social bonds than did Truste members. • High correlation between adhering to rules and efforts to build trust.

Appendix C cont'd

Milberg, Burke, Smith and Kallman (1995)	Quantitative, cross-cultural Theorized that cultural values influence and are influenced by privacy regulatory scheme	1993	N=595 Members of Information Systems Audit and Control Assoc. Countries represented: Australia, Canada, Denmark, France Japan, New Zealand, Thailand, United Kingdom, United States	Used Smith et al. (1996) CFIP instrument and assessed differences in responses based on • National Cultural Values (Hofstede 1980) • Regulatory Approaches (Bennett 1992) • Managers' Regulatory Preferences	• Overall level of concern for privacy varied across nationalities • BUT no difference in relative significance of different concerns across nationalities • No significant relationship between privacy concern and Hofstede's three value dimensions (power distance, uncertainty avoidance, individuality) • Differences in level of concern based on existing regulatory regime – no regulation or strictest regulation related to lower concern; moderate regulation related to increased concern
Milberg, Smith & Burke (2000)	Quantitative	1993	N=595 Members of Information Systems Audit and Control Assoc. Countries represented: Australia, Canada, Denmark, France Japan, New Zealand, Thailand, United Kingdom, United States	• Corporate privacy management environment • Information privacy problems within corporate environment • Preferences for regulation of information privacy • Personal information privacy concerns • Information privacy regulatory approaches	• Country's cultural values are associated strongly with population's privacy concerns and somewhat with regulatory approach • Privacy concerns influence regulatory approaches and higher concerns for privacy are linked to higher preferences for strong laws over corporate management • Regulatory approach has some influence on corporate privacy environment and regulatory preferences • Corporate privacy management environment affects privacy-related problems (strong policies, fewer problems) and affects regulatory preferences (strong policies preferred for self management)

Appendix D: Background to Information Privacy Principles

Business researchers have generally equated privacy behaviors with fair information practices (FIP) (Bennett & Grant, 1999; Culnan & Bies, 1999; Marx, 1999; Mason et al, 2000; Rule & Hunter, 1999). FIP form the core of regulation in jurisdictions such as the European Community and Canada as well as acting as guiding principles in self-regulating jurisdictions such as the United States. These practices are defined as *notice* that information is being gathered, *choice* with regard to information tracking and use, *access* to personal information records, and *security* for these records (Culnan 1993; Milne 2000).

Canada has had an approach to information privacy that has been significantly different from the U.S. experience. Throughout the 1990's, there has been an increase in public concern for information privacy. Part of the industry's response was pre-emptive action to stave off a threat of legislation that was emanating from both Ottawa and several provincial governments. The Canadian Standards Association established a technical committee to develop a standard for data protection. This standard was based on the OECD (1980) guidelines. The draft standard was unanimously adopted by CSA (1995). In 1996, the model code was adopted as a national standard (CAN/CSA-Q830-96) by the Standards Council of Canada. This standard is at the heart of the federal legislation the Protection of Information Privacy and Electronic Documents Act (PIPEDA) which came into force in 2001. The initial implementation of the Act affected all federally regulated firms (i.e., banks, telecommunications, interprovincial transportation). The second wave of the Act applied to the personal health information collected and used by the organizations included in the first stage of compliance. The final stage required compliance by all other private sector establishments by January 2004 (unless a substantively similar provincial statute is passed prior to the date.) This legislation has been accepted by the European Commission as meeting the requirements of the 1998 European Data Protection Directive (Canada 2002).

The CSA Standard was incorporated into PIPEDA as Schedule 1. Note that the 10 Principles of PIPEDA "are interrelated principles that should not be read in isolation from each other" (Perrin et al. 2001: 14).

1. Accountability – An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. Identifying purposes – The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. Consent – The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. Limiting Collection – The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure, and Retention – Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6. Accuracy – Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. Openness – An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Individual Access – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance – An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Appendix E: Differences Between Chartered Banks and Credit Unions[1]

	Chartered Banks	Credit Unions
Regulation	• Regulated by the federal government under the Bank Act. • Supervised by Office of Supervisor of Financial Institutions.	• Regulated by respective provincial governments according to specified credit union statutes. • Supervised by respective provincial superintendents.
Privacy regime	• Regulated under the federal PIPEDA since 2001.	• Come under federal PIPEDA in 2004 unless provincial government passes substantively similar legislation.
Governance	• Operated on a shareholder model. • Operated by managers responsible to a Board of Directors that shareholders elect.	• Operated on a "democratic" model. • Operated by managers responsible to a Board of Directors that members elect.
Capitalization	• Majority are listed on public exchanges. • Widely held.	• Some of the larger credit unions are traded publicly. • Most of the larger credit unions raise equity through private (member only) share offerings.
Size	• Asset range is $3.8 B to $380 B. • Branch network size range is 0 (brokerage system or virtual bank) to 1,300+.	• Asset range is $ .6 B to $6.9 B (within Top 20) • Branch network size range is 1 to 44 (within Top 20).
Trade Association	• Most are members of the Canadian Bankers Association (CBA). • Primarily a lobbying and public affairs association.	• Most are members of a provincially designated "Central Credit Union." • Services range from banking activities (liquidity, loan securitization, joint marketing, processing) to lobbying and public affairs.

[1] Source: Binhammer, H.H. and P. Sephton (2001). *Money, Banking and the Canadian Financial System* (8th ed.) Scarborough, ON: Nelson Canada.

Appendix E cont'd

	Chartered Banks	Credit Unions
Market Coverage	• Most operate across the country. • A minority operate as regional entitities. • Some have international operations.	• By definition, operate in local or regional markets (within provincial boundaries). • Most through their centrals, are affiliated with networks that provide national coverage.
Service offerings	• Most offer branch, telephone, ATM and internet channels. • A few are "virtual" only. • Consumer (retail customer) products and services include accounts (savings, chequing), loans (mortgage, line of credit), investments (RRSP, REF, mutual finds, money market). Insurance services are offered through subsidiaries.	• Most offer branch, telephone, ATM and internet channels. • Consumer (retail customer) products and services include accounts (savings, chequing), loans (mortgage, line of credit) and investments (RRSP, REF, mutual finds, money market). • Depending on the jurisdiction, insurance services may or may not be offered directly or through subsidiary arrangements.
Customers	• Refer to their customers as "customers." • Distinguish between customers and shareholders.	• Refer to customers as "members," "owners" or "member-owners" because a condition of being a customer is owning a share in the credit union. "Ownership" shares are not tradable. • Therefore, no distinction made between customers and shareholders as non exists.

Appendix F: Canadian Domestic Banks[1]
(alphabetical order)

Financial Institution[2] & Head Office	Assets ($000's)	Customers	Employees	Locations	Notes	CBA mbr[3]	Reason for exclusion
1. Amicus Bank Toronto, ON	Electronic banking operating arm of CIBC. Does not report separately except as a CIBC profit/loss centre.				Operates President's Choice Financial		× No customers of its own
2. Bank of Montreal Toronto, ON	252,864	8 million	17,000	1,100 +		✓	
3. Bank of Nova Scotia Toronto, ON	296,380	10 million (global)	49,000 (global)	1,000		✓	
4. Bank West High River, AB					Owned by Western Financial Group; operates through brokerage system		× Could not distinguish policies
5. Canadian Imperial Bank of Commerce Toronto, ON	273,293	9 million	37,000 (global)	1,139		✓	
6. Canadian Tire Bank Toronto, ON					Owned by Canadian Tire Financial Services		× Banking not primary purpose
7. Canadian Western Bank Edmonton, AB	3,828	unavailable	583 (FTE)	27	Regional Bank operating in (BC,AB,SK,MB); combined network and brokerage		× Could not distinguish policies

[1] Listing of Domestic banks obtained from the website of the Office of Superintendent of Financial Institutions (OSFI).
[2] Details about bank operations obtained from individual websites and email correspondence with the institutions.
[3] CBA mbr – refers to whether or not the institution is a member of the Canadian Bankers Association (trade association purposes). Listing of CBA members obtained from CBA website.

Appendix F cont'd

8. Citizens Bank of Canada Vancouver, BC	Does not appear to be reported separately from VanCity. Email has been sent requesting further information.				Owned by VanCity Credit Union; "virtual" only	✓	
9. CS Alterna Bank Ottawa, ON	Does not appear to be reported separately from CS Co-op. Email has been sent requesting further information.				Owned by CS Co-op	✓	
10. First Nations Bank Saskatoon, SK				3	Operating in an affiliate arrangement with TD Bank		✗ Could not distinguish policies
11. Laurentian Bank Montreal, PQ	18,595		3,730	214	Sold Western Canada and Ontario branches to focus on Quebec only	✓	✗Difficult to separate federal from provincial policy influences
12. Manulife Bank Waterloo, ON	Does not appear to be reported separately from main Manulife operations. Email has been sent requesting further information.				Owned by Manulife Financial; "virtual" only		
13. National Bank of Canada Montreal, PQ	78,400	2.5 million	17,214	546		✓	
14. Pacific & Western Bank of Canada London, ON					Subsidiary of Pacific and Western Credit Corp; no branch network – operates through broker system		✗ Could not distinguish policies
15. President's Choice Bank Toronto, ON	7,000	1.05 million	Operations within the Amicus/CIBC structure.		Owned by Loblaws Companies Limited (a division of George Weston)		
16. Royal Bank of Canada Toronto, ON	376,956	4.7 million	59,549	1,311		✓	
17. Toronto-Dominion Bank Toronto, ON	302,000	10 million (global, incl. Green Line?)	51,000	1,154		✓	

Appendix G: Top 20 Canadian Credit Unions
(As of Q4 2002)[1]

Financial Institution[2]	Head Office	Assets ($000's)	Members[3]	Employees	Locations	Notes	CUC mbr[4]
1. Vancouver City Savings	Vancouver, BC	6, 956,486	286,365	1,600	41	Owns Citizen's Bank	✓
2. Coast Capital Savings	Surrey, BC	6,065,507	295,921	2,000	44		✓
3. Envision	Langley, BC	1,793,565	104,412	700	19		✓
4. Capital City Savings	Edmonton, AB	1,659,461	118,490	Info requested	25		✓
5. Community Savings	Red Deer, AB	1,374,390	90,642	440	24		✓
6. Niagara	St. Catharines, ON	1,353,264	87,324	400	16		✓
7. Steinbach	Steinbach, MB	1,219,628	49,273	info requested	1		✓
8. Civil Service Co-op *	Ottawa, ON	1,211,008	148,676	400	20	Owns CS Alterna Bank	✗
9. First Calgary Savings	Calgary, AB	1,149,640	83,875	info requested	12		✓
10. Hepcoe	Toronto, ON	1,135,317	78,517	Info requested	26		✓

[1] Listing of Top 20 Credit Unions (excludes Quebec based Caisses Populaires) obtained from Credit Union Central of Ontario.
[2] Details of credit union operations obtained from Credit Union Central of Ontario, individual credit union websites, and email correspondence with the institutions.
[3] Credit Unions refer to their customers as "members," "owners" or "member-owners" because a condition of being a customer is owning a share in the credit union. Note that "ownership" shares are not tradable. "Ownership" shares confer voting privileges for inter alia Directors. Many credit unions issue equity shares to raise capital. These shares may have voting restrictions. Some credit unions' equity shares are publicly listed while others are open to purchase by members only.
[4] CUC (Credit Union Central) mbr – refers to whether or not the credit union is affiliated with a provincial "Central" for banking operations (liquidity, risk management and processing) and trade association purposes. Status of CUC membership obtained from Credit Union Central of Ontario.

Appendix G cont'd

11. Prospera	Abbotsford, BC	1,093,263	42,154	492	14		✓
12. Westminster Savings	New Westminster, BC	1,020,459	63,902	320	11		✓
13. Interior (Thompson)	Kelowna, BC	1,010,347	77,904	info requested	20		✓
14. North Shore	North Vancouver, BC	915,429	35,984	info requested	11		✓
15. Conexus (Sherwood)	Regina, SK	865,853	62,579	466	15		✓
16. FirstOntario	Hamilton, ON	752,448	62,704	info requested	18		✓
17. Cambrian	Winnipeg, MB	720,986	43,200	225	13		✓
18. St Willibrord Community	London, ON	708,631	42,098	200+	11		✓
19. Valley First	Penticton, BC	675,802	40,557	330	14		✓
20. Assiniboine	Winnipeg, MB	622,781	50,846	info requested	11		✓

Appendix H: Research Methods – Validating and Adapting Instruments

Interview Guides

H-1 Data Collection Strategy: Interviews (Initial Version)
H-2 Data Collection Strategy (Revised) – Basic Interview for All Participants
H-3 Summary of IPO Guide and IPO Survey Instrument Validation Pre-Test Participants
H-4 IPO Interview Guides – General Content Improvements from Pre-Test
H-5 IPO Interview Guides – Specific Guide Content Improvements from Pre-Test
H-6 IPO Interview Guide – Construction Issues from Pre-Test
H-7 Questionnaire Revisions and Improvements During and After Research Visit (Based on Case A Experience)
H-8 IPO Interview Guides (Examples of Questions):
- H-8.1 Basic
- H-8.2 Privacy Professionals
- H-8.3 IT/CII/Security/Tech Solns Function

IPO Survey

H-9 Draft Initial IPO Survey Instrument for Information Privacy Orientation
H-10 IPO Survey Instrument Construction – Card Sort Description and Results
H-11 Questionnaire Item Sorting Instructions
H-12 IPO Survey Instrument – Content Improvements from Pre-Test
H-13 Final Version of IPO Survey – Procedure (Paper-and-Pencil Survey)
H-14 Final Version IPO Survey Instrument
H-15 IPO Survey Instrument – Web-Based Version

Appendix H: Research Methods - Validating and Adapting the Instruments

The process of validation involved two phases. First, I mapped the draft interview questions and follow-ups/probes against the overarching research questions and the anticipated interviewee (i.e., Chief Privacy Officer, Legal Counsel, Marketing VP, etc.). This was collected in a table called Data Collection Strategy: Interviews and was circulated to my supervisor, two committee members and another faculty member with some knowledge of the research. All four returned useful suggestions for improvement. For example, one committee member asked for questions to be added that more specifically addressed the two competing theories. To accommodate additional questions, I dropped two questions that dealt specifically with responses to the imposition of the privacy legislation (as this issue was also addressed in the IPO Survey and through the document review). To address the competing theories, I added four questions that addressed *inter alia* the importance of being seen to be the same as or different from peers in terms of both the use of customer information and the deployment of customer information privacy. Appendices H-1 and H-2 contain the Initial and Revised Interview Data Collection Strategies.[1]

[1] Note that the draft Interview Guides received the approval of the Queen's University General Research Ethics Board in February 2004. The final IPO Guides do not deviate significantly from the drafts.

Appendix H-1: Data Collection Strategy: Interviews (Initial Version)[2]

Research Question	Interview Question	Follow-ups/Probes	Interviewee					
			Prv	Mkt	IT	Leg	Reg	Br
1. Do firms have an Information Privacy Orientation?	1.1 What would you say are your organization's goals with respect to your information privacy program?	1.1.1 How well do you think these are being met? 1.1.2 What do you think accounts for any gap between what you want to achieve and what actually is happening?	✓	✓	✓	✓	✓	✓
	1.2 What lessons would you say your firm has learned about information privacy as a result of implementing your privacy program?	1.2.1 Looking back over your experiences, would you do anything differently? What specifically? Why?	✓	✓	✓	✓	✓	✓
2. Is Information Privacy Orientation constructed as I have theorized?	2.1 How would you describe your firm's customer information strategy?	2.1.1 How is the customer information strategy set in your firm? 2.1.2 What impact has implementing a privacy program had on your customer information strategy?	✓	✓	✓			

[2] Note that this does not reflect the order that the questions will be asked nor does it include all the potential interviewees.

	2.2 How would you describe your firm's relationship with your customers?	2.2.1 What three words would your customers use to describe your firm? Why? 2.2.2 What three words would you like them to use to describe you? Why? 2.2.3. What role, if any, might your privacy program play in changing your customers description of your firm? (Positive? Negative?)	✓	✓	✓			
3. To what extent does the Institutional Approach help us to explain homogeneity in information privacy orientation across firms in the same industry?	3.1 To what extent was your firm involved with the development of the CSA model code?	3.1.1. Can you give me the reasons why your firm engaged in this activity? What was the extent of your firm's involvement (at the table, through trade association, comment on drafts?)	✓			✓		
	3.2 Once the code was finalized, to what extent did your firm adopt it (in advance of federal legislation being passed)?	3.2.1 Can you give me the reasons why your firm chose to adopt the Code voluntarily? How difficult was the Code to implement in your firm?	✓			✓		
	3.3 Could you tell me about a firm, that you believe does a particularly effective job with consumer privacy?	3.3.1 What is it about their privacy actions that impresses you? 3.3.2 Would your firm consider emulating that firm? Why or why not?	✓	✓	✓	✓		
4. To what extent does the Resource-Based View help us to explain heterogeneity in information privacy orientation across firms in the same industry?	4.1 To what extent does your firm believe that its information privacy approach is different from your competitors' approach(es)?	4.1.1 Is this difference deliberate? (Did you design your privacy program to be different or did it evolve that way)?	✓	✓	✓	✓	✓	✓

	4.2 Can you provide examples of the differences?	4.2.1 To what extent do you think this difference is noticeable to your customers? 4.2.2 To what extent do you think this difference is important to your customers? 4.2.3 To what extent do you think this difference is noticeable to your competitors? 4.2.4 To what extent do you think this difference is important to your customers?	✓	✓	✓		✓	✓
5. What is the effect of the firm's overall context (external and internal environment) on its Information Privacy Orientation?	5.1. What was your firm's position with respect to the federal government's decision to legislate information privacy in your industry?	5.1.1 What do you believe were the reasons the government took this action? 5.1.2 What action did your firm take to make your position known to the federal government (letter(s) to politicians/bureaucrats; comments to trade association, statement to Committees, etc?)	✓			✓		
	5.2 How easy has it been for your firm to meet the requirements of the law?	5.2.1. Could you give me examples of activities that you had to engage in?	✓	✓	✓	✓	✓	✓

	5.3 What would you say were the biggest challenges your firm had to overcome to implement your privacy program?	5.1.3 Which, if any of your firm's policies have had to be adapted, changed or stopped?	✓	✓	✓	✓	✓	✓
6. What is the effect of IPO on firm performance?	6.1 What research has your firm undertaken to measure the effect that your information privacy activities have had on your company?	6.1.1 What has been the effect on your customers? 6.1.2Your employees? 6.1.3 Your information systems? 6.1.4 Your overall business performance? 6.1.5 Can you estimate how much PIPEDA implementation has cost your firm?	✓	✓	✓	✓		
	6.2 What do you think would be important measures to consider in future?		✓	✓	✓		✓	
	6.3 If you could change one aspect of how your firm conducts its customer information privacy program (and assuming all things are legal), what change would you make?	6.3.1 Why? What result would you be trying to achieve?	✓	✓	✓	✓	✓	✓

Key:
Prv = Privacy personnel
Mkt = Marketing personnel
IT = Information Technology/Systems personnel
Leg = Legal personnel
Reg = Regional Office personnel
Br = Branch office Personnel

Appendix H-2 - Data Collection Strategy (Revised) – Basic Interview for All Participants

Research Question	Interview Question	Follow-ups/Probes
1. Do firms have an Information Privacy Orientation? (R1)	1.3 What would you say are your organization's goals with respect to your information privacy program? (also IA or RBV)	1.1.3 How well do you think these are being met? 1.1.4 What do you think accounts for any gap between what you want to achieve and what actually is happening?
	1.4 What lessons has your firm learned about information privacy as a result of implementing your privacy program?	1.4.1 What stage is your company at in developing and implementing your privacy policies? 1.4.2 How easy has it been to incorporate privacy in to your operations? What have been the challenges?
	1.5 How important is providing customer information privacy to the success of your company? (also IA or RBV)	
	1.4 If you could change one aspect of how your firm conducts its customer information privacy program (and assuming all things are legal), what change would you make? (also IA or RBV) Alternate: What actions do you foresee your company taking to address challenges?	1.4.1 Why? What result would you be trying to achieve? (also IA or RBV)
	1.5 What is or has been your role with respect to the development and implementation of your company's customer information privacy policies?	

	1.6 What does success mean to you in your privacy role?	
2. Is Information Privacy Orientation constructed as I have theorized? (R2)	2.1 What kinds of information, beyond transaction data, does your firm gather from and about your customers? (also RBV)	2.2.1 What does having this kind of information about your customers let you do? (also RBV)
	2.2 What are your business's primary objectives for gathering and using customer information? (also RBV)	2.2.2 How would you describe or characterize the value to your company of the customer information that you gather and use? (also RBV)
	2.3 In terms of the use of customer information, would you say your company is: ☐ more sophisticated than its competitors? ☐ equivalent to your competitors? ☐ pursuing a different path from your competitors?	
	2.4 Could you tell me about your customers. In broad terms, who does your firm serve?	2.4.1 What three words would your customers use to describe your firm? Why? 2.4.2 What three words would you like them to use to describe you? Why? 2.4.3 To what extent might your privacy approach help to address any gap?
3. To what extent does the Institutional Approach or the Resource-Based View help us to explain heterogeneity in information privacy orientation across firms in the same	3.1 To what extent does your firm believe that its information privacy approach is different from your competitors' approach(es)?	3.1.1 Is this difference deliberate? What you wanted to achieve?

industry? (R3 and R4)	3.2 How important is it for your company to be seen to be: ☐ Behaving the same as other financial institutions with respect to dealing with customer information privacy? (IA) ☐ Behaving differently from other financial institutions with respect to dealing with customer information privacy? (RBV)	3.2.1 Why is this important?
	3.3 In terms of your customer information privacy program, would you say your company is: ☐ more sophisticated than its competitors? ☐ equivalent to your competitors? ☐ pursuing a different path from your competitors?	3.3.1 On what do you base this assessment? 3.3.2 Is this where you want to be?
	3.4 Is there any company in your industry that stands apart in how they deal with customer information privacy? Can you tell me about this firm?	3.4.1 Can you tell me how they stand apart? 3.4.2 What is your opinion of why they do this?
4. What is the effect of the firm's overall context (external and internal environment) on its Information Privacy Orientation? (R5)	4.1 Who (people) or what (organizations) are key external influences on how your company "does privacy"? (also IA)	
	4.2 Within your company, who would you say are the key privacy influencers (roles, functions, departments)? (also RBV)	

5. What is the effect of IPO on firm performance? (R6)	5.1What steps has your firm taken to measure the effect that your information privacy activities have had on your company? If response is NONE: How do you think your company should go about assessing the impact of your privacy policies?	5.1.1 Customers?
		5.1.2 Employees?
		5.1.3 Business/work processes?
		5.1.4 Decision making?
		5.1.5 Financial performance?
		5.1.6 Firm reputation? (also IA)
		5.1.7 Competitive positioning?)(also RBV)
	5.2 What do you think would be important performance measures to consider in future?	
6. 6. General Questions	6.1 Is there anything else that you would like to tell me about your company's customer information privacy program?	6.1.1 What important question did I neglect to ask you?

I drafted the comprehensive Interview Guides (preamble, questions and probes, transitions, and conclusion) and determined the final set to be pre-tested – Privacy Officer, Marketing, Information Technology, and Legal (which could also be used as a "high level" or "general" guide).

The second validation round for the IPOG took place simultaneously with the pre-testing of the IPOS. Through personal contacts, I secured the cooperation of eight individuals with a wide variety of privacy expertise (such as privacy consultant or privacy manager) and functional experience (such as marketing or IT), to pre-test one of the IPO Interview Guides as well as the IPOS. (Information about the validation of the survey instrument is provided below). See Appendix H-3 for a summary of participants. All participants were emailed a letter explaining the research project, a copy of the IPO survey instrument, and a copy of the most relevant IPO Interview guide (based on my understanding of their privacy and functional expertise). Each participant either met with me personally or provided a telephone interview over a two week period in May 2004. I hand-recorded their comments directly onto the interview guide being discussed.

Appendix H-3: Summary of IPO Guide and IPO Survey Instrument Validation Pre-Test Participants

Title/Role	Organization	Expertise	Review Format	Interview Guide
President & CEO	Canadian business association	• Privacy law • Privacy as a central marketing concern	In-person	Marketing
Principal Consultant	Privacy consultancy	• Privacy law • Privacy as a central IT concern	Telephone	CIO/IT and CPO
Director, Public Affairs	Financial Institution	• Privacy as a reputational risk concern	In-person	Legal/General
Privacy Compliance Manager	Financial Institution	• Privacy law • Implementation of PIPEDA in financial institutions	In-person	CPO
Director, Organizational Excellence	Canadian business association	• Privacy as a competitive challenge • CPO role	Telephone	CPO
	Canadian business Association	• Privacy as an implementation challenge • CPO role	Telephone	CPO
Lawyer	Private practice	• Privacy law • Privacy as a legal compliance issue in financial institutions	In-person	Legal/High level
Business owner/operator	On-line company	• Privacy as both a marketing and IT challenge	Telephone	Marketing and IT

IPO Interview Guides - Content

The interview guides were generally well received. The expert reviewers indicated that the questions were interesting, would engage participants and were unlikely to provoke non-responses. In all cases, the subject matter experts requested briefings about the research findings as they were uniformly interested in the results. All pre-test participants suggested improvements. The suggestions included content issues applicable generally across the set of interview guides as well as specific improvements required for individual types. The issues identified and action taken are summarized in Appendix H-4 (General Content Improvements) and Appendix H-5 (Specific Guide Content Improvements).

Appendix H-4: IPO Interview Guides: General Content Improvements from Pre-Test

Issue/Suggestion	Action
Warm-up questions: 1. Good way to ease interviewees into discussion 2. But focus more on specific privacy responsibilities.	Reworded opening questions and probe. • How long have you been with [name of organization]? When did you become the [use relevant title] for [name of organization]? • What is your role with respect to the development and implementation of your company's customer information privacy policies? • PROBE: How much time as a %age do you spend on privacy related activities? • What does success mean to you in your privacy related role?
Customer questions: 1. Cautioned that some respondents may experience difficulty answering as their orientation is more internal than external. 2. Agreed that from a privacy perspective there should be some knowledge of who is a "typical" customer. 3. Difficulty with "relationship" wording.	Reworded question. Could you tell me about your customers? In broad terms, who does <NAME OF COMPANY> serve? Prompt: Broad segments.
Information strategy questions: 1. Cautioned that this may be a problem section for all but privacy specialists and marketers. 2. Agreed the questions were useful. 3. May have to dig for responses. 4. May get a "stock response" to the question of why gather information (i.e., so we can market). 5. Problem with the term "information strategy". This may not be a familiar term to any/everyone. 6. Add industry comparison within the topic.	Reworded questions and noted the need to emphasize non-transaction data. • What are your business's primary objectives for gathering and using customer information? • What does having this kind of information about your customers let you do? • How would you describe or characterize the value to your company of the customer information that you gather and use? In terms of the use of customer information, would you say your company is: ☐ more sophisticated than its competitors? ☐ equivalent to your competitors? ☐ pursuing a different path from your competitors?
Information Privacy questions: 1. Agreement that these were good spurs to conversation.	Added new question (altered for Legal and Privacy specific) • What actions do you foresee your company taking to address these challenges?

<table>
<tr><td>2. Issue that questions were very "present" oriented.</td><td colspan="2"></td></tr>
<tr><td>Need for specific questions for within and across case comparisons.</td><td colspan="2">Added choice questions:
In terms of the
• use of customer information,
• of customer information privacy
would you say your company is:
☐ more sophisticated than your competitors?
☐ equivalent to your competitors?
☐ pursuing a different path from your competitors?

How important is providing customer information privacy to the success of your company?
PROBE:
If "compliance response": What are the consequences to the firm of non-compliance?
If "competitive response": What are the benefits to the firm of providing customer information privacy?</td></tr>
<tr><td>Need for theory (Institutional and RBV) specific questions.</td><td>Institutional Theory:
• In your privacy role, who (people, organizations) do you look to for advice/guidance/best practices?
• Who (people) or what (organizations) are key external influences on how your company "does privacy"??
• Is there any company in your industry that stands apart in how they deal with customer information privacy ? How? Why?
• How important is it for your company to be seen to be behaving the same as other financial institutions with respect to dealing with customer information privacy? Why?
• How do you think your company should go about assessing the impact of your privacy policies? On firm reputation?</td><td>RBV:
• What are your business's primary objectives for gathering and using customer information?
• What does having this kind of information about your customers let you do?
• How would you describe or characterize the value to your company of the customer information that you gather and use?
• How important is it for your company to be seen to be behaving differently from other financial institutions with respect to dealing with customer information privacy? Why?
• How do you think your company should go about assessing the impact of your privacy policies? On competitive positioning?</td></tr>
</table>

Appendix H-5: IPO Interview Guides: Specific Guide Content Improvements from Pre-Test

Questionnaire Type	Issue/Suggestion	Action
Privacy	1. Privacy work may not be only responsibility. 2. Need to address lessons learned. 3. Need to address future plans.	Revised question (Privacy I) • Please describe your role as <Privacy Title>. • What is the scope of your role? • What are the activities of your role? • Is this a full time position? • How much time do you spend on privacy activities? Additional Questions (Privacy II) • Your company has gained a lot of experience with managing customer information privacy. Looking back, what would you say really worked in your approach/process? • What would you like to be able to go back and redo/undo? • Looking ahead, what role do you believe you company's approach to customer information privacy will have on how you do business? • What will be the impact? • Do you anticipate any significant changes to how you "do" privacy ? What might the changes be?
IT	1. Need to examine the extent to which IT has embraced privacy specifically beyond "policy boilerplate".	New question: • Does your company have a formal plan or methodology for incorporating privacy into your development projects? Can you tell me how this works? Ex: Capability Maturity Model?
IT and Marketing	1. Specifically need to probe about the uses of information beyond "policy boilerplate". 2. Need to ask specifically about customer information systems.	Revised question: • Do you try to leverage this information for new business purposes? • What secondary purposes do you use customer information for? Ex: Customer analytics/data profiling/data mining; Lifecycle Value of Customer • Do these activities confer competitive advantage? In what way? Additional question: • Does your company use CRM or a similar enterprise-wide system? What are the main features of the system?

		• PROBE: Does the system provide a single view of the customer?
Marketing	1. Need to address source of information issues.	Added new question: • From what other sources do you obtain information about your customers?
Legal	1. Be as specific as possible about legal issues. Lawyers do not like uncertainty.	Not interested in engaging in a detailed legal examination. <more interested in organizational issues. However, made a few revisions: • What privacy statute does your company comply with? • If you operate in more than one jurisdiction, how do you decide which law your company will follow? • How easy has it been to incorporate <name of specific law> into your operations?

IPO Interview Guides - Construction

Again, the guides were generally well received in terms of the flow of questions. However, a few issues required consideration. These issues and the action taken are summarized in Appendix H-6.

Appendix H-6: IPO Interview Guides: Construction Issues from Pre-Test

Issue/Suggestion	Action
Example: Confidentiality and Anonymity. It was emphasized by several experts that I needed to better underscore the confidentiality and anonymity of the interviews in the introduction. As well, this needed to be restated before asking especially sensitive questions such as how the company in question compares with industry peers.	I revised the guides as suggested.
Example: Jumping between the topics Customer Information and Customer Information Privacy. It was pointed out that this could be confusing to interviewees and lead them to want to hurry up and finish. We discussed alternative ordering.	I reviewed the flow of these sections with other experts. I decided to consolidate the Customer Information and Customer Information Privacy questions into discrete question blocks.
Example: Transition wording from discussing information management strategy to privacy programs. I was cautioned that the preamble was too long, the examples of duties likely to get people into narrow ways of thinking, and the "lecture" about PIPEDA principles unnecessary.	I reviewed all transitions to reduce the amount of time required to say them and to focus very specifically on the discussion and not "lecturing." I amended the specific examples raised by the expert reviewers.
Example: Connecting the research to something that is meaningful to the participants. Several experts offered that I needed to better hook the interviewees by appealing to their expertise.	I amended certain of the transition wording to emphasize that the interviewees were the experts and that I was there to learn from their experiences.
Example: Attempting to cover too much in a single Chief Privacy Officer interview.	I discussed this observation with another expert and determined that the best way to handle this was to split the interview guide into two parts and ask for the additional time. IPOG Privacy was divided into two guides. Privacy I covers general issues such as customers, information and privacy in a broad company and industry context. Privacy II examines the specific approaches taken by the company.

Appendix H-7: Questionnaire Revisions and Improvements During and After Research Visit (Based on Case A Experience)

In Process: Some questions were revised during the course of the three-day exercise as they were immediately problematic. An example of a change during the process is:

Original Question	**Revised Question**
What three words would <u>your customers</u> use to describe your firm? Why?	You have been appointed the director of your company's first reality TV program. You take your microphone out to <major street in city> and identify your customers. You ask them "What three words or phrases come to mind when you hear <name of company> and why?" What is the reply?
What three words <u>would you like them to use</u> to describe your firm? Why?	Congratulations! Your reality TV program was so successful that you were appointed CEO! As you gaze down from your corner office with the big windows, what are the three words that you would like your customers to use to describe your company?

When I used the original version, I discerned that interviewees were struggling to respond, mainly because head office personnel tend not to deal directly with the company's customers. I found that asking the customer-related questions in a "game show style" made it easier for respondents to situate their responses, helped them relax, and provided a good laugh. I don't think that the immediate effect of the change in wording produced necessarily "better" answers for that specific question. However, I think that the change helped to vary the style of question (thus reducing the potential for boredom), lightened the tone of the remainder of the interview, and reduced some of the anxiety to give the "right answer" (despite my repeated assurances that there was no right or wrong answer).

After the process: I also made changes as a consequence of reviewing the interview notes. For example,

Original Question	Revised Question
How easy is it/has it been to incorporate legislated privacy requirements into your operations?	One a scale of 1 to 10, where 1 means really, really easy and 10 means extremely difficult, how easy is it/has it been to incorporate legislated privacy requirements into your operations? (If necessary, PROBE) How did you arrive at the conclusion that it was [depending on the number] easy, moderately difficult, extremely difficult?
What do you think are the challenges to meet these goals?	Depending on the richness of the answer to above revised question, may be able to dispense with a specific question about challenges.

The revised approach was "suggested" by one interviewee's response. I had posed the originally worded question and she had responded by providing her own scale - "On a scale of 1 to 10 where 10 is difficult and 1 is easy, I'd say 5 or 6." She then elaborated on her response without prompting. Her approach may have been suggested because she is a marketer and has training in market research techniques. However, I liked the technique. It provided a change of pace in the format of the questions, gave participants something that seemed tangible to attach their responses to, and afforded some basis for comparison across respondents. For these reasons, I decided to use the revised question in future interviews.

A final example involves adding a new question to the interview guides. Throughout the pilot test interviews, it was apparent to me that many interviewees used the words privacy and confidentiality interchangeably. In addition, some equated privacy simply with physical security. In a couple of cases, I asked the interviewees to specifically comment on their usage. I asked "Do privacy and confidentiality mean the same thing to you?" I received mixed responses ranging from a simple "Yes" [branch personnel] to "That's a good question. I think they are different but I can't say how" [project manager] to "I think it's [privacy] a much broader concept than many people appreciate ... I think that people in banks and financial institutions ... tend to assume that customer confidentiality and privacy are the same" [legal staff]. This lack of clarity might be explained by the "developmental" stage of the pilot site's privacy program. The interviewees

might not have received training or communications that explained the difference. It may also be that terminological precision is not that important in the workplace and that I was betraying an academic's concern for language. However, I believe my concern is justified. For example, when asked the importance of customer information privacy to the company's success, one interviewee responded,

> "If you substitute 'confidentiality' for privacy, then it's very important. It's very critical. If customers don't trust that their financial institution will look after their money, won't lose their money, you won't stay in business. It's all part of concern for reputational risk." [marketing staff]

My interpretation of this response is that the interviewee equated confidentiality (not privacy) with trust, but gave an example of what could be termed a risk management or security issue ("won't lose their money"). There is a difference among the three terms (recall the distinctions introduced in Chapter One). The relative emphasis placed by companies on one term (as representing a set of organizational activities) over the others may suggest preferences and priorities that support differences in information privacy orientation. As a result, I asked interviewees in the three case sites to distinguish among these terms as indicated:

Potential New Question
Often we use terms interchangeably even when they really mean different things. For example, people often interchange the terms privacy, security and confidentiality. Just to be certain that I understand how you use these words .... Can you tell me what these words mean to you and what makes them different from each other? I don't need a dictionary definition! You can give an example of each if that makes more sense for you.

Asking this question would help me to understand the extent to which the employees had been educated around the differences among the three terms. It would also assist me in interpreting their responses to other questions. Lastly, it would be useful in understanding the relative importance placed by different groups on the different activities associated with each term. Additional information about revisions to the questionnaires can be found in the relevant sections of the individual case chapters.

Appendix H-8: IPO Interview Guides (Examples of Questions)

Appendix H-8.1 - Basic

Interviewer: Thank you for taking the time to meet with me. As you know, I am conducting research into how firms develop and implement their information privacy programs and policies. All the information you provide today will be used to build a picture of the processes carried out in your firm, the decisions that were made or are in the process of being made, and the reasons for the direction your firm took. Please be assured that your specific responses will not be identified in anyway but will be used to build an aggregate portrait. Neither will anything that you tell me be reported to anyone else in the firm. In order to ensure that my coding of your responses is accurate, I would prefer to tape the interview. Do you consent to having this interview audio recorded?

Note: If no (objection is raised) proceed with handwriting. If yes (permission to record is granted), ensure the Audio recording consent form is signed before proceeding. Reiterate the confidentiality of the interview and that respondent can refuse to answer any questions.

Interviewer: As we discussed previously, this interview will take about one hour. It is covers four themes. One section concerns you and your role in your company. Another is about customers and information. A third section is about your company's privacy program. The last section concerns customer information privacy within the context of your industry.

At the end of our discussion, there will be an opportunity for you to provide any additional information you believe is necessary for me to gain a better understanding of how your company deals with customer information privacy.

Before we proceed, do you have any questions about this interview?

[Note: Layout not as used in interviews. Compressed format]

Perhaps we could begin with you telling me a bit about yourself.

- How long have you been with [name of organization]? When did you become the [use relevant title] for [name of organization]?
- What is or has been your role with respect to the development and implementation of your company's customer information privacy policies?

  PROBE: How much time as a %age do you spend on privacy related activities?
- What does success mean to you in your privacy related role?

Thank you. This information is very helpful. Now let's spend some time talking a bit more about <NAME OF ORGANIZATION>. This will help me get a better picture of the firm. (PAUSE)

Let's talk about customers.

- Could you tell me about your customers? In broad terms, who does <NAME OF COMPANY> serve? Prompt: Broad segments.

PROBE:
What three words would your customers use to describe your firm? Why?
I

II

III

What three words would you like them to use to describe your firm? Why?
I

II

III

NOTE: If a significant discrepancy between these lists of words:

- The words your customers use to describe your firm (LIST THE WORDS) are quite different from the ones you'd like them to use (LIST THE WORDS) aren't they? Why do you think that is?

- To what extent might your company's privacy approach help to address this gap?

One important aspect of customer relations concerns the information you gather and use about customers. Let's talk about how information is used in your firm.

- What kinds of information, beyond transaction data, does your firm gather from and about your customers?

PROBE:
- What are your business's primary objectives for gathering and using customer information?
- What does having this kind of information about your customers let you do?

- How would you describe or characterize the value to your company of the customer information that you gather and use?

- In terms of the use of customer information, would you say your company is:

☐ more sophisticated than its competitors?
☐ equivalent to your competitors?
☐ pursuing a different path from your competitors?

Up to this point we've talked about your role in the business and we've discussed two aspects of your organization – your customers and your information strategy. Now I'd like us to talk about information privacy and your organization.

- From your perspective, what would you say are or ought to be your firm's goals for its privacy policies/program?

PROBE: What stage is your company at in developing and implementing your privacy policies?

- How easy is it to incorporate <jurisdiction X's> requirements into your operations?

- What do you think are the challenges to meet these goals?

- What action is or do you foresee your company taking to address these challenges?

- How important is providing customer information privacy to the success of your company?

PROBE:
If "compliance response": What are the consequences to the firm of non-compliance?
If "competitive response": what are the benefits to the firm of providing customer information privacy?

- In terms of customer information privacy, would you say your company is:

☐ more sophisticated than its competitors?
☐ equivalent to your competitors?
☐ pursuing a different path from your competitors?

Thanks! This is really interesting and helpful information. (PAUSE) Now I'd like us to focus on information privacy within the larger context of your industry. Now, let's talk about these issues again this time thinking about customer information <u>privacy</u>.

- In your privacy role, who (people, organizations) do you look to for advice/guidance/best practices?

- Who (people) or what (organizations) are key external influences on how your company "does privacy"??

- Within your company, who would you say are the key privacy influencers (roles, functions, departments)?

- Is there any company in your industry that stands apart in how they deal with customer information privacy ?

- Can you tell me how they stand apart?

- What is your opinion of why they do this?

- How important is it for your company to be seen to be:

☐ behaving the same as other financial institutions with respect to dealing with customer information privacy?
☐ Behaving differently from other financial institutions with respect to dealing with customer information privacy?

- WHY?

- How do you think your company should go about assessing the impact of your privacy policies?

PROBE: Affect on
- Employees
- Business/work processes
- Decision-making
- Financial performance
- Firm reputation
- Competitive positioning

Thanks! Your insights into how your company handles the important issue of customer information privacy have been very helpful. Before we conclude this discussion,

- **is there anything else you would like to add about customer information privacy that you think is important for me to understand?**

- **Are there any questions you have for me about this research?**

- **Thanks again for your assistance. It is very much appreciated.**

Appendix H-8.2 - Privacy Professionals

1. Can you give me an overview of the history of the privacy program in your company?

PROBE: When did you first have a privacy code?

PROBE: What was the impetus/circumstances for implementing a privacy program?\

2. Can you describe for me how your company went about implementing your privacy program in response to PIPEDA?
3. How easy was it for your firm to meet the law's requirements?

PROBE: What were the biggest challenges?

PROBE: Were there policies or activities that had to be changed? Stopped? Can you give me examples?

PROBE: Did your organization have to engage in new activities? Functions? Can you give me examples?

4. You've indicated that there were several challenges <LIST A COUPLE OF CHALLENGES>. Were there any "pleasant surprises" that resulted from implementing your privacy program? Can you give me examples?
5. How have you structured the privacy program in your company? Can you tell me the reasons for the particular choices that were made?

PROBE: Centralized versus decentralized?

PROBE: Overall sponsor versus champions within individual units?

6. How did you roll out the privacy program across the retail banking side of the business?

PROBE: Communications strategies.

PROBE: Training/help desk

7. What steps has your company taken to assess how your privacy program has affected how you do business? Are there specific goals and metrics?

PROBE:

What do you think the effect of your privacy program has been on your:

a) Customers? {Example: Appreciate? Disinterested? A Hassle?}
b) Employees? {Example: Appreciate? Disinterested? A Hassle?}
c) Financial performance? {Example: Your ability to increase revenue per customer?}
d) Firm reputation? {Example: Ability to win new customers? Be perceived as a caring company?}
e) Business/Work processes? (Example:
f) Competitive positioning? {Example: Share of certain markets?}
g) Decision-making ability? {Example: Speed/ confidence of decision-making}

8. Throughout the process of developing and implementing customer information privacy policies in your company:

   a) What/who were the key external influences on your process?

   PROBE: trade groups (CBA, CIPS, CMA); competitors, government, others

   b) What/who were the key internal influences on your process?

   PROBE: Senior Mgmt team, functional groups, lawyers?

9. Your company has gained a lot of experience with managing customer information privacy. Looking back:

   a) What would you say really worked in your approach/process?

b) What would you like to be able to go back and redo/undo?

10. Looking ahead,
    a) Do you anticipate any significant changes to how you "do" privacy ? What might the changes be? From your perspective, why would these changes be necessary?
    b) What role do you believe you company's approach to customer information privacy will have on how you do business over the next few years?

Appendix H-8.3 - IT/ Information Management/ Information Security Functions

1. How are the activities of your group (i.e., IT support, SysDev, Enterprise Computing) affected by your company's customer information privacy policies?
2. What are your business's primary objectives for gathering and using customer information?
3. What does having this kind of information about your customers let you do?

PROBE: Customer Profiling; Data Analytics; Lifetime Value of Customer?

4. Does your company have a formal information strategy concerning the collection and use of customer information? What are the key aspects of this plan? What input do you/does your IT group have to this plan?
5. Can you tell me about any dedicated customer systems you have in place.
6. Does your company use CRM or a similar enterprise-wide system? What are the main features of the system?
   PROBE: Does the system provide a single view of the customer?
7. What would you say are your firm's goals for its privacy program?

PROBE: If response is "compliance" ask if there are secondary goals.
EXAMPLES: Accuracy of data, Usefulness of Data, Completeness of Customer Information, Competitive Differentiation? Customer Trust?
PROBE: How well are your company's privacy goals being met do you think?

8. What role did you and/or your IT group play in developing your company's privacy policies?

PROBE: From the perspective of the IT group, how easy was it for your firm to meet the law's requirements?
PROBE: From the perspective of the IT group, what were the biggest challenges?
PROBE: What has been the impact of information privacy policies on your ability to get the best results from your enterprise system?

9. Did the IT group have to change any policies or activities as a result of implementing the company's privacy policies? Can you give me examples?
10. Did the IT group have to engage in <u>new activities</u>? Functions? Can you give me examples?

Thanks again for your assistance. It is very much appreciated.

Appendix H-9: Draft Initial IPO Survey Instrument for Information Privacy Orientation

Section 1

Respondents will be asked to rate the strength of their agreement with the following statements using a 7 point Likert-type scale where 1=strongly disagree and 7=strongly agree.

[Customer Relationship Stance:
The firm's perspective on the obligations they owe their customers.]

In my firm, we believe that:

#	Item	
1.	Customers exist to be sources of profit for firms.	Buyer exploitation
2.	It is our obligation to make as much money from our customers as possible.	Buyer exploitation
3.	We should ask for as much information as possible from every customer.	Buyer exploitation
4.	Customers are responsible for looking out for their own interests.	Buyer self-protection
5.	We are obliged to look after our own interests first and our customers interests second.	Buyer self-protection
6.	If customers want more information about our business practices, it is up to them to ask for it.	Buyer self-protection
7.	Customers and firms exist for mutual benefit.	Shared Responsibility
8.	We should try to anticipate customer questions about our business practices and provide information to help them make good decisions.	Shared Responsibility
9.	We should work with our customers to maximize customer benefits and firm profits.	Shared Responsibility
10.	We are obliged to help customers make the best decisions in their interests.	Consumer well-being
11.	We should ensure that customers have the best information possible about our business practices for them to make the best decisions.	Consumer well-being
12.	Customers exist to be served by the firm even if that means we sometimes "leave money on the table"	Consumer well-being

[Information Management Strategy
The organization's predominant strategy with respect to its objectives for gathering and using information.]

#	Item	
1.	Information is primarily useful as a tool to reduce costs.	Reduce costs
2.	Our customers expect us to gather personal information in order to keep our prices low.	Reduce costs
3.	It is more important to achieve our cost targets than our customer satisfaction targets.	Reduce costs
4.	Information is primarily useful as a tool to minimize risks.	Minimize risks
5.	Our customers expect us to gather personal information in order to properly manage risks such as maintaining security.	Minimize risks
6.	It is more important that we identify and manage risks than we achieve customer satisfaction targets.	Minimize risks
7.	Information is primarily useful as a means to develop value added products/services.	Add value
8.	Our customers expect us to gather personal information in order to tailor existing products/services to their needs.	Add value
9.	It is more important that we use customer information to improve existing products than to innovate new ones.	Add value
10.	Information is primarily useful as a means to create new competitive realities.	Create new realities
11.	Our customers expect us to gather personal information in order to develop new products and services.	Create new realities
12.	Our overriding target is to use customer information to create new opportunities.	Create new realities

[Privacy Philosophy:
The firm's view about the need to and rationale for engaging in privacy activities.]

In our firm, we believe that:

#	Item	
1.	We have no obligation to protect customer privacy.	Privacy to be ignored
2.	Privacy laws are not something that applies to our business.	Privacy to be ignored
3.	We can gather and use whatever information we can get from our customers.	Privacy to be ignored
4.	Customers who think their information has been used improperly can move their business to another company.	Privacy as Constraint
5.	Privacy laws make it difficult for customers to get the best deal from our firm.	Privacy as Constraint
6.	Privacy laws make it very difficult to operate our business.	Privacy as Constraint
7.	Customers trade their personal information for better service and benefits.	Privacy as Exchange
8.	Privacy legislation has helped us to secure better information from our customers.	Privacy as Exchange
9.	We are better able to provide goods and services to our customers because d the detailed information we obtain from them.	Privacy as Exchange
10.	Privacy legislation has helped our firm become better at how we gather and use customer information.	Privacy as Differentiator
11.	We are able to make our firm more attractive to potential customers by emphasizing our privacy policy.	Privacy as Differentiator
12.	We are better positioned to serve our customers as a result of our privacy policies than are our competitors.	Privacy as Differentiator

[Privacy Behaviors:
What privacy actions are taken by the firm.]

In our firm, we believe that

#	Item	
1.	Our customers have no expectation of privacy in dealing with us.	Non-compliant
2.	Privacy laws don't affect our firm and our ability to gather and use customer information.	Non-compliant
3.	Any information we gather is ours to use as we choose.	Non-compliant
4.	As long as we follow the letter of the law, we needn't be too concerned with what we do with customer information.	Minimally compliant
5.	If a customer really is concerned, we'll talk to them about how our policies comply with the law.	Minimally compliant
6.	The information we gather is ours to use as we see fit.	Minimally compliant
7.	In comparison with our most important competitors, we offer our customers just as good privacy protection.	Moderately compliant
8.	Our customers share their information with us and we use it to make better offers for them.	Moderately compliant
9.	We provide good information to customers who are concerned about how their information is used.	Moderately compliant
10.	In comparison with our most important competitors, we offer our customers better privacy protection.	Significantly enhanced privacy protection
11.	Our customers own their information and lend it to us. We aim to assist them to keep it private.	Significantly enhanced privacy protection
12.	Our company goes out of its way to assist customers to understand the benefits of sharing their information and the steps that are in place to protect their privacy.	Significantly enhanced privacy protection

Section 2:

Respondents will be asked to select the paragraph that most closely describes the current situation in their organization.

Which of the following descriptions most closely fits your organization compared to other firms in the industry? (Please consider your company as a whole and note that none of the types listed below is inherently "good" or "bad"). (Wording taken from Snow and Hrebiniak,1980)

_____	Type 1	This organization believes that customers are responsible for their own welfare. This organization primarily exists to make a profit for its shareholders. The focus is primarily on reducing costs which is the focus of our information strategy. As a result, we believe that we have no obligation to address customer privacy issues.
_____	Type 2	This organization believes that customers are responsible for their own welfare. This organization primarily exists to make a profit for its shareholders. The focus is primarily on minimizing risks which is the focus of our information strategy. As a result, we believe that we have no obligation to address customer privacy issues.
_____	Type 3	This organization believes that we and our customers share in the responsibility to protect their privacy. This organization tries to balance its obligations to its shareholders and its customers. Our information strategy emphasizes how to use information to add value to our products and services. Our customers provide us with information in order to obtain better products and services. Our privacy policies are consistent with industry standards.
_____	Type 4	This organization believes that we are responsible for our customers wellbeing. This organization primarily exists to serve our customers. The focus is primarily on minimizing risks which is the focus of our information strategy. Our customers As a result, we believe that addressing customer privacy issues is fundamental to our competitive position. This organization believes that we are responsible for our customers privacy.

Appendix H-10: IPO Survey Instrument Construction – Card Sort Description and Results

The IPO survey instrument was tested in four rounds of card sorts in April 2004. For the first two rounds of the card sort, the following procedure was followed. First, I prepared a set of 64 (4 constructs X 4 strengths X 4 items per strength category) index cards on each of which was printed one individual item. I also prepared four index cards on each of which was printed a construct name and its definition. Second, I prepared an instruction sheet to be read by each card sort participant. See Appendix H-11 for the text of the instruction sheets for each round of the card sort. Third, I prepared a master list of the items and assigned random numbers to each item. The index cards were then organized into a single pile according to the randomized list. I pencilled a number on the back of each card (not visible to participants). This numbering system was used to record the actual card ordering and to reassemble the card deck after each process. This latter step ensured that the participants in all rounds were presented with the cards in exactly the same order, thus minimizing potential bias from the ordering. Fourth, I solicited participation from three categories of individual – faculty, graduate students, and business professionals. Table H-10.1 lists the participants in each card sort round. Details and results from the four rounds of card sorts are addressed below.

Card Sort Round One

For this card sort exercise, each participant (in separate sessions) was seated at a large desk. Across the top of the desk were placed the four construct and definition cards. The construct names and definitions were highlighted in yellow to distinguish them from the item cards. Each participant was provided with the instruction sheet and given a few minutes to read it. Each was asked if s/he had any questions and if s/he understood the task they were to perform. Any questions were answered. The participants were handed the stack of 64 index cards and asked to place the cards in piles according to how well the card reflected the definition of the construct. Note that participants were not prompted to sort the cards into equally numbered piles, merely

into four piles. Once the participants had completed the initial sort, they proceeded to do a construct by construct review and to shift the cards until they were satisfied with their efforts. I was present throughout these processes except for brief absences to obtain refreshments for the participants. I did not interact with the participants about the card sort exercise until they had declared that they were finished.

Table H-10.1: Card Sort Participants

Sort	Type of sort	Participant	Details
1.1	Four constructs specified; original instrument (v1.1)	Faculty member	PhD (Marketing) ethics expertise
1.2	Four constructs specified; original instrument (v1.1)	Graduate Student	PhD student (Management Information Systems) interest in privacy
1.3	Four constructs specified; original instrument (v1.1)	Business professional	MBA, extensive executive background in major Canadian financial institution
2.1	Four constructs specified; instrument (v.1.2)	Faculty member	MBA,MPA Extensive managerial experience; expertise at firm level of analysis
2.2	Four constructs specified; instrument (V.1.2)	Graduate student	PhD student (Organization Behaviour)
3.1	Number and definition of constructs unspecified; instrument (V.2)	Business Professional	MBA, extensive executive background in major global firms
3.2	Number and definition of constructs unspecified; instrument (V.2)	Faculty member	PhD (Information Systems) Experience with senior executives in global firms
4.1A	Constructs unspecified; forced to 4 equal piles; instrument (V.2.3)	Faculty member	PhD (Information Systems) Significant non-academic work experience
4.2A	Constructs unspecified; forced to 4 equal piles; instrument V.(2.3)	Faculty member	PhD (Information Systems); experienced with employee surveillance studies
4.3A	Constructs unspecified; forced to 4 equal piles; instrument (V.2.3)	Graduate Student	PhD student (Marketing); interest in privacy and surveillance
4.1B	Constructs specified; forced to 4 equal piles; instrument (V.2.3)	Graduate student	PhD student (Organization Behaviour)
4.2B	Constructs specified; forced to 4 equal piles; instrument (V.2.3)	Graduate student	PhD student (Information Systems); interest in privacy and surveillance

Once the participants had concluded their sorting exercises, I immediately manually recorded the sort results. Then the raters and I discussed their experiences (i.e., how difficult was it for you to make decisions about where to sort the cards?) and the items themselves (i.e., were the words clear?). Each participant provided useful comments about the experience which I audio

recorded and used for subsequent refinement of the IPO survey instrument. The comments were audio-recorded and are available on request.

After we had concluded our debriefing sessions, I recorded the results of each sort into two spreadsheets. The first spreadsheet recorded what cards had been sorted into which of the four categories (in effect a "raw score" of the actual sort). I used the random number assigned to each card to identify the items against each of the four constructs. This information was useful in the process of reviewing each item and determining the need for revisions. The revision process is discussed further on. In the second spreadsheet I recorded the three different card sorts against the distribution of items in the original instrument. I prepared summary charts for each participant as follows. I also transcribed the audiotape of the participants' specific comments into a Word document. These comments helped to shed light on the reasons for the decisions and specifically identified difficulties that the participants had experienced with the exercise. In addition, I computed the inter-reliability (Cronbach alpha) for this round. The alpha was .916 which is a very good result. However, a an item by item review of results by participant revealed difficulties with the draft instrument as described below.

Round One Results

Participant 1.1 (faculty member) took 36 minutes to sort the cards into 4 uneven piles.

Construct	# of items in original instrument	# of items sorted per construct	Items in agreement with original instrument
CRS	16	18	10/16 = .625
IMS	16	22	13/16 = .8125
PHIL	16	22	8/16 = .5
BHV	16	2	2/16 = .125

Participant 1.2 (graduate student) took 47 minutes to sort the cards into 4 uneven piles. This participant also sorted into items into sub-categories (unrequested/unprompted). This is shown as an additive function in the third column.

Construct	# of items in original instrument	# of items sorted per construct	Items in agreement with original instrument
CRS	16	15	12/16 = .75
IMS	16	11 + 6 = 17	12/16 = .75
PHIL	16	4 + 4 + 6 + 7 = 21	13/16 = .8125
BHV	16	2 + 3 + 6 = 11	7/16 = .4375

Participant .33 (business professional) took 54 minutes to sort the cards into 4 uneven piles.

Construct	# of items in original instrument	# of items sorted per construct	Items in agreement with original instrument
CRS	16	24	7/16 = .4375
IMS	16	8	8/16 = .5
PHIL	16	19	6/16 = .375
BHV	16	13	4/16 = .25

This data review showed three important results of this initial card sort. First, the items did not sort neatly into the four constructs. The agreement achieved across the constructs (in order of strength of agreement) was IMS, CRS, PHIL and BHV. Second, the sorting was very uneven, that is, there was no consistency across the choices made by the different participants. This suggested that there was no consistency in how the participants were interpreting either the definitions or the items. Third, the debriefings indicated that the participants found overlaps among the constructs and, as a result, had experienced difficulty in making sorting choices.

I then constructed a table to visually assess the results of Round One. This data showed me where there was agreement or disagreement in two ways. First, it showed the extent to which the sort was consistent with the original instrument. Second, it showed the specific items that were selected or not by the participants. I have summarized this information in Table H-10.2.

Table H-10.2: Summary of Round 1 Card Sort Against Original Instrument

Construct/ # of agreements	Items															
BHV (2)	1	2	3	4	5	6	7	8	9	10	11	**12**	13	14	**15**	16
PHIL (10)	**1**	**2**	3	**4**	5	6	**7**	**8**	9	**10**	11	**12**	**13**	14	**15**	16
IMS (12)	**1**	**2**	3	4	**5**	**6**	**7**	8	**9**	**10**	11	**12**	**13**	**14**	**15**	**16**
CRS (11)	**1**	**2**	3	**4**	**5**	**6**	7	**8**	**9**	**10**	11	**12**	**13**	**14**	15	16

Table H-10.2 is organized as follows. The left most column indicates the construct name abbreviation and the number of items which received at least two agreements. By agreements, I mean that the participants placed that specific item in the same construct as I had prepared the original instrument. The sequence of numbers 1-16 running from left to right indicate the number of the actual item in the original instrument. The numbers that are bolded indicate an item upon which two or more participants agreed. The shaded and unshaded blocks are provided both to reflect the four strength categories of the IPO continuum and to improve readability. Examples of how to read the table follow.

For the construct called Customer Information Management Strategy (IMS), two or more participants sorted 12 items similar to the original instrument. Specifically, items IMS 1,2,5,6,7,9,10,12,13,14,15,16 were selected. In contrast, for the construct called Customer Information Privacy Behaviours (BHV), only 2 items were in agreement (BHV 12, 15). For all other BHV items, either only a single participant sorted the item or no participant sorted the item according to the original instrument. A vertical inspection of the results shows the extent of consistency across participants. For example, no participant "correctly" sorted items 3 and 11.

This table overstates the strength of agreement between the participants and the original instrument. Recall that in this round, participants were not asked to force their sort. That is, they were not told that there was a uniform number of items per construct. As a result, while the number of agreements for IMS, for example, seems high (12 agreements), this tally does not reflect the number of "incorrect" sorts that were made. While the original instrument contained 16 items for the IMS construct, participants assigned 22, 17 and 8 items to this construct.

Subsequently, my supervisor and I conducted an item by item review. We paid particular attention to the alternative placements made by the participants and reviewed what language may have triggered participants to sort "incorrectly." As a result of this review, I reworked the instrument. I redefined the constructs to more tightly reflect the underlying ideas and to place the respondents' organizations at the centre of the definitions. Table H-10.3 shows the original and revised definitions that were used for Round Two. Next, I reworded the items to more tightly reflect the constructs, to eliminate ambiguity and to be more specific.

Table H-10.3: Revised Construct Definitions from Card Sort Round One

Construct	Original Definition	Revised Definition
Customer Relationship Stance	The firm's perspective on the obligations it owes its customers.	How your firm describes its obligations to its customers.
Customer Information Management Strategy	The organization's predominant strategy with respect to its objectives for gathering and using information.	Your firm's predominant purpose for collecting and using customers' personal information.
Customer Information Privacy Philosophy	The firm's view about the need to and rationale for engaging in privacy activities.	Your firm's view of the effect privacy laws have on your ability to carry on business.
Customer Information Privacy Behaviours	What privacy actions are taken by the firm.	The privacy policies that guide behaviour and the privacy actions that are taken by your firm.

Card Sort Round Two

The second card sort round followed the method previously described except that only two raters were used, a graduate student and a faculty member. Participants were provided with the construct definitions but were not asked to force the sorting to a specific number of items per construct. The Cronbach alpha computed for the inter-rater reliability of this round was 1.00 which while very good was not substantiated in the review of the debriefings.

Round Two Results

Participant 2.1 (graduate student) took 37 minutes to sort the cards into 4 even piles.

Construct	# of items in original instrument	# of items sorted per construct	Items in agreement with original instrument
CRS	16	16	16/16 = 1.00
IMS	16	16	16/16 = 1.00
PHIL	16	16	16/16 = 1.00
BHV	16	16	16/16 = 1.00

Participant 2.2 (faculty) took 50 minutes to sort the cards into 4 uneven piles. This participant also sorted some items into sub-categories (in the course of the debriefing). This is shown as an additive function in the third column.

Construct	# of items in original instrument	# of items sorted per construct	Items in agreement with original instrument
CRS	16	6 + 9 = 15	15/16 = .9375
IMS	16	16	16/16 = 1.00
PHIL	16	14	14/16 = .875
BHV	16	19	16/16 = 1.00

The results of the second round are summarized in Table H-10.4. This table is similar to the one presented for the results of Round 1 with one exception. The numbers in bold type represent the three items for which there was only one rater in agreement with the revised instrument. Both participants were in agreement with the revised instrument on 61 of 64 items.

Table H-10.4: Summary of Round 2 Card Sort Against Revised Instrument

Construct/ Number of agreements	Items															
BHV (16)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
PHIL (14)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
IMS (16)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CRS (15)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

The items for which there was not an agreement were:

CRS4	We do not owe our customers any explanation for how we do business.	Buyer exploitation

This item was sorted as BHV.

PHIL1	Our firm is not required by law to protect customer privacy.	Privacy to be ignored

This item was sorted as BHV.

PHIL3	We can gather and use whatever personal data we can get from our customers or any other source without any concern for privacy legislation.	Privacy to be ignored

This item was sorted as BHV.

In consultation with my supervisor, I decided to do another round of card sorts. Our concern, based on a review of the debriefing documents, was that we were still not tapping the constructs in an understandable and consistent manner that reflected what I was trying to accomplish with the instrument. Despite having achieved an apparently high level of inter-rater reliability, we were concerned with the explanations provided for the sorting decisions. For example, both participants expressed difficulty with distinguishing between PHIL and BHV. My supervisor and I conducted another item by item review and made many minor revisions to the

instrument. We also rewrote the definition for Privacy Behaviours. The revised definition was short and to the point: "Your firm's privacy policies that guide your privacy actions."

Card Sort Round Three

For this round of validation, there were three deviations from the previously described card sort methodology. First, the instruction sheet did not provide the construct names and definitions. (See Appendix H-11 for the revised Instruction sheet.) Second, the participants were not provided with the construct names and definitions on cards to guide their sorting. Third, participants were not provided any written or verbal instruction indicating the number of constructs. Participants were simply instructed to sort cards into however many piles they chose. Once the participants had concluded the initial sorting, each was asked to provide a statement and/or definition for each pile or category they had created.

This round proved to be problematic. The absence of specific information (i.e., construct names and definitions, number of constructs) seemed to overwhelm the raters. Faced with 64 cards, the participants appeared to find it easier to cope with many small piles of cards. The results for Round Three appear below.

Round Three Results

Participant 3.1(business professional) took 37 minutes to sort the cards into 6 uneven piles.

Category Name/Definition	# of items in category
1. Industry related statements	CRS = 4
2. Law related statements	PHIL = 13
3. Big picture statements	CRS = 7; IMS = 2; BHV = 2; PHIL = 1
4. External market activities statements	IMS = 6; CRS = 1; PHIL = 1
5. Internal operations statements	IMS = 8; BHV = 2
6. Business Policy statements	BHV = 12; CRS = 4; PHIL = 1

Participant 3.2(faculty member) took 76 minutes to sort the cards into 9 uneven piles.

Category Name /Definition	# of items in category	Category Name /Definition	# of items in category
1. Proactive and Positive statements	18 IMS = 8; BHV = 6; PHIL = 4	6. Compliance statements	5 BHV = 5
2. Costs statements	4 IMS = 4	7. Negative statements	10 PHIL = 5; BHV = 4; CRS = 1
3. Risks statements	4 IMS = 4	8. Buyer beware statements	7 CRS = 5; PHIL = 1; BHV = 1
4. Customer first statements	5 CRS = 5	9. Customer-business relationship statements	5 CRS = 5
5. Customer tradeoff statements	5 PHIL = 5	Not sorted	1 PHIL = 1

I again transposed this information into a visual display. Each group of cards was plotted onto a grid and then reviewed. My supervisor and I reviewed the results of this third round. We concluded that despite the number of groups identified there were some good results coming from the sort. First, the IMS construct was holding together well in both sorts. Second, the BHV construct was generally holding together although in need of some tweaking. However, the CRS and PHIL constructs were still problematic. Once again we reviewed the items and edited statements according to the debriefing transcripts and the experience we were steadily gaining with the instrument. We decided to run another card sort to determine if we had improved the instrument with our tweaking processes.

Card Sort Round Four

Round Four was held April 27 and April 30 at Queen's School of Business. There were five judges used for this final card sort – two MIS faculty members and three graduate students (MIS, Marketing and Organization Behaviour). Each rater was instructed to "force the sort" – that is, to sort the cards evenly into four piles of 16 cards. Three of the judges (both faculty raters and one graduate student) sorted the 64 cards using only the IPO definition for guidance. The instructions for this round (4A) appear in Appendix H-11. Round 4a proved difficult for raters because of the large number of cards and the single construct definition for guidance.

The two judges for Round 4B were provided with the IPO definition and the four construct definitions (without labels). The instructions for Round (4B) appear in Appendix H-11. The raters for 4B experienced greater success with the card sort given the additional information they were provided.

The results of the five sorts are described below.

Round Four 4A Results

Participant 4.1A MIS Faculty member took 42 minutes to sort the cards.

Category Name/Definition	# of items in category
1. Action Statements	BHV = 13/16; IMS = 3/16
2. Policy/strategy statements	IMS = 13/16; BHV = 2/16; PHIL 1/16
3. Values statements	CRS = 15/16; BHV = 1/16
4. Beliefs statements	PHIL = 15/16; CRS = 1/16

Participant 4.2 MIS Faculty member took 47 minutes to sort the cards.

Category Name/Definition	# of items in category
1. Privacy for competitive advantage statements	BHV = 5; CRS = 4; IMS = 4; PHIL = 3
2. Privacy to match competitors/meet customer needs statements	IMS = 8; PHIL = 4; BHV = 3; CRS = 1
3. Letter of law/ efficiency and risk statements	CRS = 7; IMS = 4; BHV = 4; PHIL = 1
4. Privacy laws are bad statements	PHIL = 8; CRS = 4; BHV = 4

Participant 4.3 Marketing PhD Student took 55 minutes to sort the cards.

Category Name/Definition	# of items in category
1. Positive customer orientation statements	CRS = 8; PHIL = 5; BHV = 2; IMS = 1
2. Negative customer orientation statements	BHV = 8; PHIL = 6; CRS = 1; IMS = 1
3. Firm oriented statements	IMS = 14; BHV = 2
4. Competition oriented & misc. statements	CRS = 7; PHIL = 5; BHV = 4

I then compared the three blind sorts to each other to ascertain where there was agreement among the sorters. The heuristic I employed was to determine for each rater the construct with the greatest representation in the different groups of cards. I mapped these onto the construct grid and

then prepared a comparison for agreements between two or more raters (represented by the bolded items). The results are reported in Table H-10.5.

Table H-10.5: Sort Round 4A: Agreements

Construct/ # of agreements	Items															
BHV	1	2	3	4	**5**	**6**	**7**	**8**	**9**	**10**	11	**12**	**13**	**14**	**15**	**16**
PHIL	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	9	10	11	**12**	13	14	15	16
IMS	**1**	**2**	**3**	4	**5**	**6**	7	**8**	**9**	**10**	11	**12**	**13**	14	**15**	**16**
CRS	1	2	3	4	5	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**

On the basis of this comparison, the agreements among the three raters were:

Construct	# of items in instrument	# of items sorted per construct (forced sort)	Items for which there was agreement between 2 or more raters:
CRS	16	16	11/16 = .6875
IMS	16	16	12/16 = .75
PHIL	16	16	8/16 = .5
BHV	16	16	10/16 = .625

These were still low levels of agreement, which indicated some level of unreliability when raters were not provided with the construct definitions. However, the results were very positive when the definitions were provided. In Round 4B, two raters were asked to force their sort against the definitions (not including construct labels) so that they ended up with 4 groups of 16 cards. The results were:

Participant 4.1B Organization Behaviour PhD Student took 40 minutes to sort the cards.

Category Name/Definition	# of items in category	Agreement with instrument
1. Customer Relationship Management	CRS = 16	CRS 16/16 = 1.00
2. Information Management Strategy	IMS = 16	IMS 16/16 = 1.00
3. Privacy Philosophy	PHIL = 16	PHIL 16/16 = 1.00

4. Privacy Behavior	BHV = 16	BHV16/16 = 1.00

Participant 4:5: MIS PhD Student took 35 minutes to sort the cards.

Category Name/Definition	# of items in category	Agreement with instrument
1. Customer Relationship Management	CRS = 16	CRS 16/16 = 1.00
2. Information Management Strategy	IMS = 16	IMS 16/16 = 1.00
3. Privacy Philosophy	PHIL = 15; BHV = 1	PHIL 15/16 = .9375
4. Privacy Behaviour	BHV = 15; PHIL = 1	BHV15/16 = .9375

I then computed the reliability for the entire round (waves a and b) and determined that the alpha = .953. A review of the debriefing transcripts suggested that the instrument was ready to be field tested.

Appendix H-11: Questionnaire Item Sorting Instructions

Four Category Sort: Round 1

Card Sorting Instructions for Information Privacy Orientation Package

Information Privacy Orientation is defined as *the principles, values, decisions rules, policies and desired objectives that organizations adopt to guide them in the collection and use of their customers' personal information.*

You have been given a set of 64 cards. On each card is written a single statement about some aspect of an organization's information privacy orientation. Each statement is intended to reflect one particular aspect:

- *Customer Relationship Stance:* The firm's perspective on the obligations it owes its customers.
- *Information Management Strategy*: The firm's predominant strategy with respect to its objectives for gathering and using information.
- *Privacy Philosophy:* The firm's view about the need to engage, and rationale for engaging, in privacy activities.
- *Privacy Behaviours:* What privacy actions are taken by the firm.

Please sort the cards into the four categories. There are an equal number of statements for each category. The statements in each category should be related to each other as much as they reflect the category definition. Many of the statements will seem to be similar. Try to determine the *underlying* category that the statements reflect.

Do not hesitate to change the grouping of cards as you proceed with the sorting exercise. It is normal to change your mind about how you think the different statements relate to each category. Take your time. Once you have completed sorting the cards, please go through each pile for one last time to be certain that the cards are placed in the most appropriate categories and that you are satisfied to leave them that way. Do not hesitate to resort the cards until you are satisfied with your efforts.

This is not a test! The purpose of this sorting exercise is to determine if the statements are related to the four categories as originally determined when the questionnaire was first drafted.

Thanks very much for helping me with my research.

Sub-Category Sort: Round 1

Card Sorting Instructions for Information Privacy Orientation Package

You have been given a set of 64 cards, divided into 4 groups. On each card is written a single statement about some aspect of an organization's information privacy orientation. Each statement is intended to reflect one particular aspect or category. The four categories are:

- *Customer Relationship Stance:* The firm's perspective on the obligations it owes its customers.
- *Information Management Strategy*: The firm's predominant strategy with respect to its objectives for gathering and using information.
- *Privacy Philosophy:* The firm's view about the need to engage, and rationale for engaging, in privacy activities.
- *Privacy Behaviours:* What privacy actions are taken by the firm.

For each of the four groups of cards:

Please sort the 16 cards into the four categories. There are an equal number of statements for each category. The statements in each category should be related to each other as much as they reflect the category definition. Many of the statements will seem to be similar. Try to determine the *underlying* category that the statements reflect. For each group of four cards, please tell me what you think is the theme for that particular group of the cards.

Take your time. Once you have completed sorting the cards, please go through each pile for one last time to be certain that the cards are placed in the most appropriate categories and that you are satisfied to leave them that way. Do not hesitate to resort the cards until you are satisfied with your efforts.

This is not a test! The purpose of this sorting exercise is to determine if the statements are related to the four categories as originally determined when the questionnaire was first drafted and that there are themes that are evident for each group of cards.

Thanks very much for helping me with my research.

Overall Sort: Round 2

Card Sorting Instructions for Information Privacy Orientation Package

Information Privacy Orientation is defined as *the principles, values, decisions rules, policies and desired objectives that organizations adopt to guide them in the collection and use of their customers' personal information.*

You have been given a set of 64 cards. On each card is written a single statement about some aspect of an organization's information privacy orientation. Each statement is intended to reflect one particular aspect or category.

Please sort the cards into as many categories as you see fit. The statements in each category should be related to each other. Many of the statements will seem to be similar. Try to determine the *underlying* category that the statements reflect.

Do not hesitate to change the grouping of cards as you proceed with the sorting exercise. It is normal to change your mind about how you think the different statements relate to each other. Take your time. Once you have completed sorting the cards, please go through each pile for one last time to be certain that the cards are placed in the most appropriate categories and that you are satisfied to leave them that way. Do not hesitate to resort the cards until you are satisfied with your efforts.

Once you are satisfied with the how you have sorted the cards, please try to give a name or make a statement that describes each of the different categories you have created with the cards.

This is not a test! The purpose of this sorting exercise is to determine if the statements are related to in the manner originally determined when the questionnaire was first drafted.

Thanks very much for helping me with my research.

Overall Sort: Round 3

Card Sorting Instructions for Information Privacy Orientation

Information Privacy Orientation is defined as *the principles, values, decision rules, policies and desired objectives that organisations adopt to guide them in the collection and use of their customers' personal information.*

You have been given a set of 64 cards. On each card is written a single statement about some aspect of an organization's information privacy orientation. Each statement is intended to reflect a particular aspect of information privacy orientation.

Please sort the cards into as many categories as you see fit. The statements in each category should be related to each other. Many of the statements will seem to be similar. Try to determine the *underlying* category that the statements reflect.

Do not hesitate to change the grouping of cards as you proceed with the sorting exercise. It is normal to change your mind about how you think the different statements relate to each other. Take your time. Once you have completed sorting the cards, please go through each pile for one last time to be certain that the cards are placed in the most appropriate categories and that you are satisfied to leave them that way. Do not hesitate to resort the cards until you are satisfied with your efforts.

Please advise me when you are finished. I would like to discuss with you:

a) your reasons for sorting the cards in a particular manner;
b) any "decision rules" you may have evolved for sorting the cards; and
c) the description you assigned to the various categories you constructed.

For convenience sake, and with your consent, I will audiotape the discussion. Please let me know if you do not want the discussion to be taped.

This is not a test! The purpose of this sorting exercise is to assess if the statements are related in the manner originally determined when the questionnaire was first drafted.

Thanks very much for helping me with my research.

Four Category Sort: Round 4a

Card Sorting Instructions for Information Privacy Orientation Package

Information Privacy Orientation is defined as *the principles, values, decision rules, policies and desired objectives that organisations adopt to guide them in the collection and use of their customers' personal information.*

You have been given a set of 64 cards. On each card is written a single statement about some aspect of an organization's information privacy orientation. Each statement is intended to reflect a particular aspect of information privacy orientation.

Please sort the cards into four categories. There should be 16 cards placed in each category. The statements in each category should be related to each other as much as they reflect the category definition. Many of the statements will seem to be similar. Try to determine the *underlying* category that the statements reflect.

Do not hesitate to change the grouping of cards as you proceed with the sorting exercise. It is normal to change your mind about how you think the different statements relate to each category. Take your time. Once you have completed sorting the cards, please go through each pile for one last time to be certain that the cards are placed in the most appropriate categories and that you are satisfied to leave them that way. Do not hesitate to resort the cards until you are satisfied with your efforts. Once you are satisfied with the final sort, please think of a word or phrase that you would use to describe the theme for each of the four piles of cards.

Please advise me when you are finished. I would like to discuss with you:
d) your reasons for sorting the cards in a particular manner;
e) any "decision rules" you may have evolved for sorting the cards; and
f) the theme/description you assigned to the four categories you constructed.
For convenience sake, and with your consent, I will audiotape the discussion. Please let me know if you do not want the discussion to be taped.

This is not a test! The purpose of this sorting exercise is to determine if the statements are related to the four categories as originally determined when the questionnaire was first drafted.

Thanks very much for helping me with my research.

Four Category Sort: Round 4b

Card Sorting Instructions for Information Privacy Orientation Package

Information Privacy Orientation is defined as *the principles, values, decision rules, policies and desired objectives that organisations adopt to guide them in the collection and use of their customers' personal information.*

You have been given a set of 64 cards. On each card is written a single statement about some aspect of an organization's information privacy orientation. Each statement is intended to reflect a particular aspect of information privacy orientation:

- *How your firm describes its obligations to its customers.*
- *Your firm's predominant purpose for collecting and using customers' personal information.*
- *Your firm's view of the effect privacy laws have on your ability to carry on business.*
- *Your firm's privacy policies that guide your privacy actions.*

Please sort the cards into the four categories. There should be 16 cards placed in each category. The statements in each category should be related to each other as much as they reflect the category definition. Many of the statements will seem to be similar. Try to determine the *underlying* category that the statements reflect.

Do not hesitate to change the grouping of cards as you proceed with the sorting exercise. It is normal to change your mind about how you think the different statements relate to each category. Take your time. Once you have completed sorting the cards, please go through each pile for one last time to be certain that the cards are placed in the most appropriate categories and that you are satisfied to leave them that way. Do not hesitate to resort the cards until you are satisfied with your efforts. Once you are satisfied with the final sort, please think of a word or phrase that you would use to describe the theme for each of the four piles of cards.

Please advise me when you are finished. I would like to discuss with you:
g) your reasons for sorting the cards in a particular manner;
h) any "decision rules" you may have evolved for sorting the cards; and
i) the theme/description you assigned to the four categories you constructed.
For convenience sake, and with your consent, I will audiotape the discussion. Please let me know if you do not want the discussion to be taped.

This is not a test! The purpose of this sorting exercise is to determine if the statements are related to the four categories as originally determined when the questionnaire was first drafted.

Thanks very much for helping me with my research.

TABLE H-12: IPO Survey Instrument - Content Improvements From Pre-Test

Issue/Suggestion	Action
Example CRS 1: It was argued that in the absence of a delimitation of the item, an "ethical marketer" could claim CRS1 as a "very strong agree" because it is ethical to maximize shareholder value.	CRS 1: The wording was changed as suggested to: *We are obliged to maximize profits by whatever means possible.*
Example: IMS 12-16 It was suggested that most Financial Institutions will gravitate to these items thus this may not produce a significant variance.	I reviewed these with items against the research on which they are based (Marchand 1998) and concluded that there was no basis at this time to reword the items.
Example: PHIL 1-4 It was suggested that respondents in financial institutions might be insulted and provoke a response of "How stupid does she think we are?" This could possibly cause respondents to not deal seriously with the survey or abandon it. I explained that the instrument would eventually be used with other industries and in other jurisdictions.	I asked for input about this concern with several participants once it had been raised. Once they were clear about the research objectives and the reasons for including these kinds of items, it was suggested that the cover letter/instruction sheet address the issue directly and specifically. Wording was added to the cover letter: *Some of the questions or statements might seem extreme or silly to you. I understand that not all statements apply to your company. Please try to give as complete a picture of your company as possible.*
Example: BHV There were no suggestions for improvements to this part of the IPOS.	None required.

Appendix H-13: Final Version of IPO Survey - Procedure (Paper-and-Pencil Survey)

1. I prepared a cover letter (see Appendix H-14). The incentive for completion of the survey was a donation to a charitable foundation supported by the financial institution.
2. I photocopied the different sections of the survey onto different coloured paper. I used this approach as a tactic to make the survey look less intimidating, and to provide me with an easy way to identify the different parts at data entry.
3. I provided a self-addressed postage prepaid envelope. Respondents were instructed to complete the survey and return it in the provided envelope (which ensured return directly to the Queen's School of Business).
4. I arranged with the Queen's School of Business PhD Program Office to receive the surveys and indicate the date of receipt in order to track early and late respondents.

Appendix H-14: Final Version of IPO Survey Instrument

Queen's School of Business Letterhead

Customer Information Privacy Survey

<BANK NAME> has kindly agreed to support my doctoral dissertation research into customer information privacy. Part of this support includes agreeing to having a survey conducted of employees who are knowledgeable about the company's customer information privacy activities. Your name was provided for inclusion in this survey.

This survey concerns your opinions about your company's approach to handling customer information privacy. The survey should take about 15 minutes to complete. Please be assured that **your responses are confidential and anonymous**. No specific comments will be reported back to your company. The results of the survey will be reported in aggregate only.

If you would like to expand on any answers or have a comment to make about any question or statement, please feel free to use the margins or to attach an additional page. I promise to read all your comments and take them into account. Some of the questions or statements might seem extreme or irrelevant to you. I understand that not all statements apply to your company. Please try to give as complete a picture of your company as possible. I really appreciate your efforts.

I understand that your time is valuable. As a small token of appreciation for taking the time to complete the survey, **I pledge to donate $100.00 to the <NAME OF CHARITY> if I receive at least a 75% response rate.** In order for your survey to count towards this pledge, it must be received at Queen's University by **<DATE>.**

Thanks very much. Your assistance is greatly appreciated.

Instructions for completing the survey:
Unless otherwise instructed, please indicate the extent to which you believe that a statement reflects what happens in your company. Circle the response that most appropriately reflects your company where …
1= Strongly Disagree
2= Disagree
3= Somewhat Disagree
4= Neither agree nor disagree
5= Somewhat agree
6= Agree
7= Strongly agree
DK = No opinion/Don't know

First, I would like you to tell me about how *your company* <u>thinks about customers</u>.

		Strongly Disagree			Neither Disagree nor Agree			Strongly Agree	No Opinion / Don't Know
1.	We are obliged to maximise profits by whatever means possible.	1	2	3	4	5	6	7	X
2.	My firm is obliged to look after our own interests first but we recognize that our customers have interests that they will want to protect.	1	2	3	4	5	6	7	X
3.	We should work with our customers to maximize customer benefits and firm profits.	1	2	3	4	5	6	7	X
4.	We are obliged to help our customers make the best decisions to further their interests.	1	2	3	4	5	6	7	X
5.	My company exists to make profits from customers in every way that we can.	1	2	3	4	5	6	7	X
6.	Companies exist to make profits from customers while customers exist to satisfy their own wants and needs.	1	2	3	4	5	6	7	X
7.	Customers and firms exist for mutual benefit.	1	2	3	4	5	6	7	X
8.	Customers exist to be served by the firm even if that means we sometimes do not engage in profitable activities.	1	2	3	4	5	6	7	X
9.	My firm's business interests are more important than the interests of our customers.	1	2	3	4	5	6	7	X
10.	We expect our customers to look after their own interests when they do business with us.	1	2	3	4	5	6	7	X

11.	It is important that firms and customers understand their respective responsibilities within the commercial relationship.	1	2	3	4	5	6	7	X
12.	Our firm places the interests of our customers ahead of our own.	1	2	3	4	5	6	7	X
13.	We do not owe our customers any explanation for how we do business.	1	2	3	4	5	6	7	X
14.	Customers should take responsibility to inform themselves about our firm's business practices.	1	2	3	4	5	6	7	X
15.	Our customers deserve to be given an explanation of our business practices if they request such explanations.	1	2	3	4	5	6	7	X
16.	Our customers deserve to be proactively advised about our business practices.	1	2	3	4	5	6	7	X

This next section asks you to comment on how *your company* <u>uses customer information</u>.

		Strongly Disagree			Neither Disagree nor Agree			Strongly Agree	No Opinion / Don't Know
1.	The primary purpose of our information management strategy is to help manage operational costs.	1	2	3	4	5	6	7	X
2.	The primary purpose of our information management strategy is to help manage various risks to the business.	1	2	3	4	5	6	7	X
3.	The primary purpose of our information management strategy is to add value to our current goods and services.	1	2	3	4	5	6	7	X
4.	The primary purpose of our information management strategy is to position the firm for the future.	1	2	3	4	5	6	7	X
5.	Customer information is primarily useful as a tool to reduce costs.	1	2	3	4	5	6	7	X
6.	Customer information is primarily useful as a tool to minimize market, security and similar risks to our business.	1	2	3	4	5	6	7	X
7.	Customer information is primarily useful to add value to our goods and services.	1	2	3	4	5	6	7	X
8.	Customer information is primarily useful as a means to create new competitive realities for our company.	1	2	3	4	5	6	7	X
9.	It is most important to my firm to use customer information to achieve our cost targets.	1	2	3	4	5	6	7	X
10.	It is most important to my company to use customer information to identify and manage risks.	1	2	3	4	5	6	7	X

11.	At my firm, it is most important to use customer information to add value to our goods and services.	1	2	3	4	5	6	7	X
12.	It is most important to my firm to use customer information for innovation.	1	2	3	4	5	6	7	X
13.	In order to achieve our cost efficiency targets, we collect as much information about our customers as we need	1	2	3	4	5	6	7	X
14.	In order to properly manage risks, we gather personal information.	1	2	3	4	5	6	7	X
15.	In order to tailor our products to customers' preferences, we collect personal information.	1	2	3	4	5	6	7	X
16.	Our overriding information management priority is to apply customer information to the creation of new opportunities.	1	2	3	4	5	6	7	X

Now I would like you to reflect on *your company's* view of the <u>impact of privacy legislation</u> on how you do business.

		Strongly Disagree			Neither Disagree nor Agree			Strongly Agree	No Opinion / Don't Know
1.	In our view, the law does not require that we protect our customers' privacy.	1	2	3	4	5	6	7	X
2.	Privacy laws make it difficult for customers to get the best deal from our firm.	1	2	3	4	5	6	7	X
3.	Privacy laws allow customers to trade their personal data for better service and benefits.	1	2	3	4	5	6	7	X
4.	The privacy approach we have adopted as a consequence of the privacy legislation helps us to retain and attract customers.	1	2	3	4	5	6	7	X
5.	We believe that we can gather whatever personal data we can get about our customers without concern for privacy legislation.	1	2	3	4	5	6	7	X
6.	Privacy laws mean that we can no longer collect all the personal data that we want about our customers.	1	2	3	4	5	6	7	X
7.	Because of privacy legislation, customers are more willing to provide accurate personal data to our firm.	1	2	3	4	5	6	7	X
8.	Privacy legislation has improved our firm's decision-making regarding what personal data to gather and how best to use that data.	1	2	3	4	5	6	7	X
9.	We believe that our customers don't care about privacy legislation.	1	2	3	4	5	6	7	X
10.	We believe that customers care more about efficient	1	2	3	4	5	6	7	X

	service than about legal privacy protections.								
11.	Privacy laws permit us to give customers fair value in exchange for providing their personal data.	1	2	3	4	5	6	7	X
12.	We are better positioned than are our competitors to serve our customers as a result of having to respond to the privacy laws.	1	2	3	4	5	6	7	X
13.	Privacy laws do not really apply to our industry.	1	2	3	4	5	6	7	X
14.	Privacy legislation has removed an important source of competitive advantage for our firm.	1	2	3	4	5	6	7	X
15.	Privacy laws allow us to collect detailed personal data on customers and provide them with better goods and services.	1	2	3	4	5	6	7	X
16.	We believe that the privacy laws have provided our firm the opportunity for industry leadership.	1	2	3	4	5	6	7	X

In this section, I would like you to tell me about *your company's* privacy actions.

		Strongly Disagree			Neither Disagree nor Agree			Strongly Agree	No Opinion / Don't Know
1.	Our firm has not implemented a privacy policy.	1	2	3	4	5	6	7	X
2.	Our firm has implemented a basic privacy policy.	1	2	3	4	5	6	7	X
3.	Our firm has implemented a privacy policy that is at least as good as our competitors'.	1	2	3	4	5	6	7	X
4.	Our firm has implemented a privacy policy that is regarded by others as leading in our industry.	1	2	3	4	5	6	7	X
5.	We make business plans without taking customer privacy considerations into account.	1	2	3	4	5	6	7	X
6.	We think about the privacy implications of our business plans when we have to.	1	2	3	4	5	6	7	X
7.	We try to incorporate privacy considerations when developing business initiatives.	1	2	3	4	5	6	7	X
8.	We give priority to privacy considerations when developing business initiatives.	1	2	3	4	5	6	7	X
9.	We collect the personal data we need on customers without advising them on how we use the data.	1	2	3	4	5	6	7	X
10.	We provide our customers with the minimum required privacy protection.	1	2	3	4	5	6	7	X
11.	We offer our customers a good level of privacy protection so that they will continue to do business with us.	1	2	3	4	5	6	7	X

12.	Our company goes out of its way to provide our customers with specific privacy protections that are beyond what is offered by our competitors.	1	2	3	4	5	6	7	X
13.	Privacy is not an issue for our industry.	1	2	3	4	5	6	7	X
14.	Our privacy policy merely reflects our industry's consensus about how to meet our privacy requirements.	1	2	3	4	5	6	7	X
15.	Our privacy practices are comparable to those adopted by most firms in our industry.	1	2	3	4	5	6	7	X
16.	We provide the best privacy practices we have been able to find in our industry.	1	2	3	4	5	6	7	X

Thanks! You are almost at the end of the questionnaire.

Please rank the following five statements in order of importance, where 1= most important.

In my company, privacy of customer information is:

___ An information management issue.
___ A legal compliance issue.
___ An ethical issue.
___ A marketing issue.
___ A risk management issue.

Please read through the four descriptions below.

Select the <u>one</u> description that most accurately describes your company <u>in comparison with your competitors</u>. Circle the single Type (1, 2, 3 or 4) that corresponds to your selection. Please think about your organization overall (not your single unit or division) as you choose your response.

Please understand that there is no "right" or "wrong" or "good" or "bad" answer.

Circle one
↓

Type 1	This company exists to make a profit. Customers exist solely as a source of profit. Customer information is used primarily to achieve cost reductions. We believe that we have no obligation to address customer privacy issues.
Type 2	This company primarily exists to make a profit although we recognize that customers' needs are important, too. This company believes customers are responsible for their own welfare including protecting their information privacy. Our customer information strategy emphasizes using personal information primarily to minimize risks to the business. As a result, we have organizational policies that strictly address customer information privacy as a legal issue.
Type 3	This company exists to satisfy both its shareholders and its customers. This organization believes that we and our customers share in the responsibility to protect their privacy. Our information strategy emphasizes how to use information to add value to our current products and services. Our customers provide us with information in order to obtain better products and services. As a result, our privacy policies are consistent with industry standards.
Type 4	This company primarily exists to serve customers. This organization believes that it is responsible for ensuring its customers' privacy. It is very future oriented. Our customer information strategy primarily emphasizes using personal information to create new products and services. As a result, we believe that addressing customer privacy issues is fundamental to our competitive position.

In the previous question, you selected a particular description of your organization today. Which description (i.e., Type 1,2,3, or 4) best fits your organization for the following periods of time:

1-3 years ago Type _____ Can't say/Wasn't here _____

1-3 years from now Type _____ No opinion _____

Please tell me a little bit about you. This information is being collected for statistical purposes only.

1.	I have been with this company:	☐ Less than 1 year ☐ 1 to 5 years ☐ 6 to 10 years ☐ More than 10 years
2.	I work in (business unit/department):	
3.	My position is located in (check one):	☐ Head Office ☐ Regional Office ☐ Branch Office ☐ Call Centre
4.	I have received training on privacy laws.	☐ Yes ☐ No ☐ Don't remember
5.	I have received training on my company's privacy policies and practices.	☐ Yes ☐ No ☐ Don't remember
6.	Part of my personal performance evaluation depends on how well I implement the firm's privacy policies and practices.	☐ Yes ☐ No ☐ Don't know
7.	I am:	☐ Female ☐ Male
8.	My age is:	☐ Less than 30 ☐ 30 – 39 ☐ 40 – 49 ☐ 50 – 59 ☐ 60 and older
9.	My highest level of education is:	☐ High School ☐ Some College ☐ College Diploma ☐ Some University ☐ Bachelor degree ☐ Graduate/Professional degree

THANK YOU VERY MUCH FOR COMPLETING THIS SURVEY.

Thank you very much for completing this survey. I really appreciate your help. Please mail your survey using the stamped, self addressed envelope marked "Survey."

Don't forget that the deadline for your completed survey to count towards the <CHARITABLE ORGANISATION> donation is <DATE>.

If you would like to receive a copy of the summary of my research findings, please check off the appropriate box below.

If you have any questions or concerns related to this study please contact me by telephone <#> or by email kgreenaway@business.queensu.ca. You may also address any concerns to:

- Dr. Yolande Chan, dissertation supervisor, Queen's School of Business, <telephone>, <email address>;
- Dr. Stephen Salterio, Chair, Unit Ethics Review Committee, Queen's School of Business, <telephone>, <email address>; or
- Dr. Joan Stevenson, Chair, General Research Ethics Board, Queen's University, telephone>, <email address>.

Thank you for helping me with my dissertation research.

Kathleen Greenaway, PhD Program
Queen's School of Business
Goodes Hall
143 Union Street
Kingston, ON K7L 3N6

✂ ----------

DETACH this coupon and place in the envelope marked SURVEY. This coupon will be handled separately and your anonymity will be maintained.

☐ Yes, I would like to receive a summary of the research findings.

Name: _____

Email Address: _____

Appendix H-15: IPO Survey Instrument – Web-Based Version

Instructions for completing the survey:
Unless otherwise instructed, please indicate the extent to which you believe that a statement reflects what happens in your company. Select the response that most appropriately reflects your company.

First, I would like you to tell me about how your company thinks about customers.

We are obliged to maximise profits by whatever means possible.	
My firm is obliged to look after our own interests first but we recognize that our customers have interests that they will want to protect.	
We should work with our customers to maximise customer benefits and firm profits.	
We are obliged to help our customers make the best decisions to further their interests.	
My company exists to make profits from customers in every way that we can.	
Companies exist to make profits from customers while customers exist to satisfy their own wants and needs.	
Customers and firms exist for mutual benefit.	
Customers exist to be served by the firm even if that means we sometimes do not engage in profitable activities.	
My firm's business interests are more important than the interests of our customers.	
We expect our customers to look after their own interests when they do business with us.	

It is important that firms and customers understand their respective responsibilities within the commercial relationship.	
Our firm places the interests of our customers ahead of our own.	
We do not owe our customers any explanation for how we do business.	
Customers should take responsibility to inform themselves about our firm's business practices.	
Our customers deserve to be given an explanation of our business practices if they request such explanations.	
Our customers deserve to be proactively advised about our business practices	

This next section asks you to comment on how your company <u>uses customer information</u>.

The primary purpose of our information management strategy is to help manage operational costs.	
The primary purpose of our information management strategy is to help manage various risks to the business.	
The primary purpose of our information management strategy is to add value to our current goods and services.	
The primary purpose of our information management strategy is to position the firm for the future.	
Customer information is primarily useful as a tool to reduce costs.	
Customer information is primarily useful as a tool to minimise market, security and similar risks to our business.	

Customer information is primarily useful to add value to our goods and services.	
Customer information is primarily useful as a means to create new competitive realities for our company.	
It is most important to my firm to use customer information to achieve our cost targets.	
It is most important to my company to use customer information to identify and manage risks.	
At my firm, it is most important to use customer information to add value to our goods and services.	
It is most important to my firm to use customer information for innovation.	
In order to achieve our cost efficiency targets, we collect as much information about our customers as we need.	
In order to properly manage risks, we gather personal information.	
In order to tailor our products to customers' preferences, we collect personal information.	
Our overriding information management priority is to apply customer information to the creation of new opportunities.	

Now I would like you to reflect on your company's view of the impact of privacy legislation on how you do business.

In our view, the law does not require that we protect our customers' privacy.	
Privacy laws make it difficult for customers to get the best deal from our firm.	
Privacy laws allow customers to trade their personal data for better service and benefits.	

The privacy approach we have adopted as a consequence of the privacy legislation helps us to retain and attract customers.	
We believe that we can gather whatever personal data we can get about our customers without concern for privacy legislation.	
Privacy laws mean that we can no longer collect all the personal data that we want about our customers.	
Because of privacy legislation, customers are more willing to provide accurate personal data to our firm.	
Privacy legislation has improved our firm's decision-making regarding what personal data to gather and how best to use that data.	
We believe that our customers don't care about privacy legislation.	
We believe that customers care more about efficient service than about legal privacy protections.	
Privacy laws permit us to give customers fair value in exchange for providing their personal data.	
We are better positioned than are our competitors to serve our customers as a result of having to respond to the privacy laws.	
Privacy laws do not really apply to our industry.	
Privacy legislation has removed an important source of competitive advantage for our firm.	
Privacy laws allow us to collect detailed personal data on customers and provide them with better goods and services.	
We believe that the privacy laws have provided our firm the opportunity for industry leadership.	

In this section, I would like you to tell us about your company's privacy actions.

Our firm has not implemented a privacy policy.	
Our firm has implemented a basic privacy policy.	
Our firm has implemented a privacy policy that is at least as good as our competitors'.	
Our firm has implemented a privacy policy that is regarded by others as leading in our industry.	
We make business plans without taking customer privacy considerations into account.	
We think about the privacy implications of our business plans when we have to.	
We try to incorporate privacy considerations when developing business initiatives.	
We give priority to privacy considerations when developing business initiatives.	
We collect the personal data we need on customers without advising them on how we use the data.	
We provide our customers with the minimum required privacy protection.	
We offer our customers a good level of privacy protection so that they will continue to do business with us.	
Our company goes out of its way to provide our customers with specific privacy protections that are beyond what is offered by our competitors.	
Privacy is not an issue for our industry.	

Our privacy policy merely reflects our industry's consensus about how to meet our privacy requirements.	
Our privacy practices are comparable to those adopted by most firms in our industry.	
We provide the best privacy practices we have been able to find in our industry.	

Please rank the following five statements in order of importance, where 1 equals the most important. Each statement should receive a unique ranking - i.e. each rank (1 through 5) should be selected only once.

In my company, providing customer information privacy is primarily...

- An information management issue.
- A legal compliance issue.
- An ethical issue.
- A marketing issue.
- A risk management issue.

Please read through the four descriptions below.

Select the one description that most accurately describes your company in comparison with your competitors. Please think about your organization overall (not your single unit or division) as you choose your response.

Please understand that there is no "right" or "wrong" or "good" or "bad" answer.

Type 1	This company exists to make a profit. Customers exist solely as a source of profit. Customer information is used primarily to achieve cost reductions. We believe that we have no obligation to address customer privacy issues.

Type 2	This company primarily exists to make a profit although we recognize that customers' needs are important, too. This company believes customers are responsible for their own welfare including protecting their information privacy. Our customer information strategy emphasizes using personal information primarily to minimize risks to the business. As a result, we have organizational policies that strictly address customer information privacy as a legal issue.
Type 3	This company exists to satisfy both its shareholders and its customers. This organization believes that we and our customers share in the responsibility to protect their privacy. Our information strategy emphasizes how to use information to add value to our current products and services. Our customers provide us with information in order to obtain better products and services. As a result, our privacy policies are consistent with industry standards.
Type 4	This company primarily exists to serve customers. This organization believes that it is responsible for ensuring its customers' privacy. It is very future oriented. Our customer information strategy primarily emphasizes using personal information to create new products and services. As a result, we believe that addressing customer privacy issues is fundamental to our competitive position.

In the previous question, you selected a particular description of your organization today. Which description (i.e., Type 1,2,3, or 4) best fits your organization for the following periods of time:

1-3 years ago:

1-3 years from now:

Please tell me a little bit about you. This information is being collected for statistical purposes only.

I have been with this company:	
I work in (business unit/department):	
I work at (work location):	

I have received training on privacy laws.	
I have received training on my company's privacy policies and practices.	
Part of my personal performance evaluation depends on how well I implement the firm's privacy policies and practices.	
I am:	
My age is:	
My highest level of education is:	

Please include any other relevant comments here:

Thank you very much for completing this survey.

Submit

Appendix I: Research Sites Recruitment

This appendix contains the documents I used to recruit the research sites.

Item Number	Title
I-1	Request for Participation (initial email)
I-2	Invitation Letter (formal request sent by courier)
I-3	Research Project Summary (included in formal request)
I-4	Research Site Requirements (emailed when requested)
I-5	Confidentiality & Non-Disclosure Agreement (includes Schedule A: Consent Form)

Appendix I-1: Request for Participation

Information Privacy Orientation:
Dissertation Research Request for Participation as a Research Site

---

Background

This case study research will investigate the manner in which four Canadian financial institutions have developed and implemented their information privacy regimes. The research will specifically examine the organisational phenomenon called "Information Privacy Orientation" that is defined as "the principles, values, decision rules, policies and desired objectives that organisations adopt to guide them in the collection and use of their customers' personal information."

Information privacy is a key ethical, legal, information management and strategic issue for firms that arises largely, although not exclusively, as a result of the deployment of information technologies such as CRM systems. Research has demonstrated that consumers are concerned about how organisations collect, use, reuse and retain personally identifiable information, especially their sensitive financial and medical information. These concerns are exacerbated by the growth of the "internet economy" characterised by its interconnected databases. However, there has been limited empirical work examining how organisations manage the conflict between exploiting technological capabilities for profit maximization and addressing customer concerns for privacy.

Benefits to Participating Organisations

1. I will provide a confidential management report to each participating company and would be prepared to make a detailed presentation to the organisation, if requested.
2. Companies infrequently have the time to undertake a detailed "debriefing" of initiatives that affect significant aspects of your operations across the company. My report will provide you with a retrospective on the implementation of your privacy program as it relates to customer information privacy within the domestic retail banking business.
3. Without revealing names or other identifying information, your company will gain a sense of the alignment of your privacy positioning across a range of employees. This may assist you to diagnose and take actions to improve the alignment to achieve a desired privacy positioning.

Research Questions

In order to improve our understanding of how firms have organised their information privacy functions and programs, I address the following questions:

1. How were the Information Privacy functions and programs developed and implemented?
2. Where are these firms positioned on an Information Privacy Orientation continuum?
3. What have been the effects of their privacy programs on key firm activities (such as credit, risk management, IT, marketing, compliance/legal and front-line customer service)?
4. In what way and to what degree has implementing customer information privacy policies affected key firm performance measures?

Please note the scope for this dissertation research is limited to customer information privacy in retail banking settings in Canada.

Information Requirements

This research will examine privacy programs in four Canadian financial institutions. To accomplish the research objectives, I will require the following information.

Interviews: I would like to interview a cross section of privacy informed personnel.

1. I would like to interview a cross section of privacy informed personnel including executives, managers, and operational staff that occupy roles with some privacy responsibility. Depending on the company's organisational structure, these roles/positions would include personnel in CRM/databasemarketing, IT systems (development and security), Legal, Privacy/compliance, Credit, Risk Management, Help Desk as well as branch staff. I anticipate meeting with 8-12 individuals at the Head Office level to get a well rounded view of the company's customer information privacy practices. These interviews should last about one hour each.
2. It may be that during the course of the interviews, other staff are suggested. I may need to interview a limited number of additional personnel and would request some flexibility from the company in this regard.
3. While I prefer to conduct these interviews in person, I would be willing to conduct interviews by telephone if necessary. Furthermore, while my protocol is primarily set for one on one interviews, I am prepared to meet with 2 or 3 people at a time if that is more convenient. I would be amenable to undertaking a larger group interview (say 5 or 6 staff) over 1.5 hours if there is an intact group (such as a privacy task force) that would be important to interview. I am prepared to conduct these interviews at the convenience of the personnel including meeting with them outside of normal working hours (early morning or evening meetings).
4. All interviews would be anonymous and confidential. If requested, participants will be provided with a typed transcript of their interview in order to confirm that it accurately reflects our conversation and to provide additional or clarifying information.
5. For ease of administration and to minimize disruption to your operations, I would prefer to work with a knowledgeable contact at the company who would be able to advise me regarding who best to interview. Ideally, an administrative assistant would also help with the task of scheduling the interviews.

Survey: I have developed an Information Privacy Orientation survey that takes about 20 minutes to complete.

1. I will ask the people I interview to complete the questionnaire.
2. In addition, it would be helpful to have the survey completed by personnel who are presently or have been involved with the company's privacy implementation process (i.e., participated on privacy task forces, conducted training or information sessions).
3. To make this a statistically valid process, I would seek to distribute about 50 copies of the survey.
4. All survey data will be anonymous and confidential. Completed surveys will be returned directly to me. Statistical results will be reported in aggregate only.
5. For ease of administration and to minimize disruption to your operations, I would prefer to work with a knowledgeable contact at the company who could identify individuals within the company who are best positioned to respond to the privacy survey.

Documents: It would be helpful to review privacy-related documents.

1. This could include such items as privacy audits, training and policy manuals, privacy governance papers and privacy business cases prepared over time.
2. Background papers and committee minutes for implementation task forces are other types of information that would be valuable to review.
3. Wherever possible, I would prefer to obtain copies of the documents.

Timeline

This research project is a key aspect of my doctoral dissertation which is to be completed in the autumn of 2004. Data collection must be completed by the beginning of August. The deliverables for the participating organisations will be provided at a time and in a format as negotiated.

Confidentiality

The confidentiality of the information provided by your company and employees will be protected.

1. Only my dissertation supervisor and I will know the identity of participating research sites. We will both sign confidentiality and non-disclosure agreements if necessary.
2. Only my dissertation supervisor and I will see the draft interview transcripts and completed surveys.
3. The company identity and the names of participants will be concealed in all dissertation-related publications and presentations.
4. All information obtained (whether interview transcripts, completed surveys or documents) will be retained in a secure location for a period of three to five years (until thesis publications have been completed), at which time it will be disposed of in a secure manner.

Costs

There is no direct cost to the organisation for participation in this research or for receiving the management report.

Contacts

Further information can be obtained by contacting:

Kathleen Greenaway PhD Candidate Queen's School of Business Goodes Hall Queen's University Kingston, ON K7L 3N6 <Telephone> <Email Address>	or	Dr. Yolande Chan, Dissertation Supervisor Professor, Management of IT Queen's School of Business Goodes Hall Queen's University Kingston, ON K7L 3N6 <Telephone> <Email Address>

Appendix I-2 – Invitation Letter

<Date>

<CONTACT name>
<Inside Address>

Dear <Contact Name>:

Re: Canadian Banks and Information Privacy

Canada's banks are acknowledged leaders in customer service and technology innovations. While the introduction of federal privacy legislation in 2001 likely complicated the ability of these financial institutions to continue to provide this leadership, Canada's banks appeared to have persevered. However, the actions that banks have taken with respect to managing information privacy challenges have not been systematically researched in order that the lessons learned can be identified and shared.

I am currently completing a PhD in Management at Queen's University, conducting research into how firms organise their information privacy function. I hope to document the range of approaches that different firms have taken in deciding how to respond to the challenge of balancing their legal obligations and their business requirements with their customers' desire for privacy. This research will help to shed light on an area that is not well understood by many firms even as they attempt to develop and implement their privacy policies across their firms' range of businesses and activities.

My research objectives will be met by examining the information privacy policies and practices of banks, such as yours, with experience in developing and implementing privacy regimes in response to Canada's federal privacy legislation. I would like to interview a small number of key executives involved with your bank's privacy and related functions at the head office level as well as at the regional and branch levels of the organisation. In addition, I would like to administer a confidential survey to gauge the opinions of selected, knowledgeable personnel about aspects of the firm's privacy policies. Finally, I would like to review relevant privacy documents, such as privacy training manuals, in order to round out my view of how customer information privacy is managed in a large bank.

I would appreciate having the opportunity to include <Bank> in my study. In exchange for this access, I will prepare a confidential management report of my findings within your firm as well as provide your firm with the overall conclusions from the entire research project. I have attached a brief summary of the research project for your further information. In addition, I have enclosed two privacy related reports that I hope you will find interesting and informative.

The data collection phase of my research is scheduled to be concluded in July. I plan on studying and providing feedback to four organisations. I sincerely hope that <Bank> will be one of these firms.

I will contact you next week to discuss how we might involve <Bank> in this project. Please do not hesitate to contact me before then if you have any questions either at <telephone> or <email>.

Thank you for your consideration.

Yours truly,

Kathleen Greenaway, MBA, MPA
PhD Candidate
Queen's School of Business

ENCL:
1. Proposal Summary
2. Customer Knowledge Management Roundtable (not attached)
3. Information Privacy & M-Commerce Symposium (not attached)

Appendix I-3 – Research Project Summary

Research Project Summary
Information Privacy Orientation

Background

This case study research investigates the manner in which four Canadian financial institutions developed and implemented their information privacy regimes. The specific research examines the organisational phenomenon called "Information Privacy Orientation" that is defined as "the principles, values, decision rules, policies and desired objectives that organisations adopt to guide them in the collection and use of their customers' personal information."

Information privacy is a key ethical, legal, information management and strategic issue for firms. Research has demonstrated that consumers are concerned about how organisations collect, use, reuse and retain personally identifiable information, especially their sensitive financial and medical information. These concerns are exacerbated by the growth of the "internet economy" characterised by its interconnected databases. However, there has been limited empirical work examining how organisations manage the conflict between exploiting technological capabilities for profit maximization and addressing customer concerns for privacy.

Research Questions

In order to improve our understanding of how firms have organised their information privacy functions and programs, I address the following questions:

1. Where are these firms positioned on an Information Privacy Orientation continuum?
2. How were the Information Privacy functions and programs developed and implemented?
3. What have been the effects of the privacy programs on key firm activities?
4. How have the privacy programs affected key firm performance measures?

This research examines privacy programs in four Canadian firms. Data are collected in three ways. First, I interview senior managers in each of the selected organizations. Second, I administer Information Privacy Orientation questionnaires to the managers interviewed as well as other knowledgeable employees. Lastly, I review privacy–related documentation (such as training manuals and policy manuals).

Timeline

This research project is a key aspect of my doctoral dissertation which is to be completed in the autumn of 2004. As a result, the three data collection approaches outlined above must be completed in August. The deliverables for the participating organisations will be provided in the autumn at a time and in a format as negotiated.

Confidentiality

The confidentiality of the information provided by participating organisations will be protected. The company identity and the names of participants will be concealed in all dissertation-related publications and presentations. In addition, I will provide a confidential management report to each participating organisation.

Costs

There is no direct cost to the organisation for participation in this research or for receiving the management report.

Contacts

Further information can be obtained by contacting:

Kathleen Greenaway or PhD Candidate Queen's School of Business Goodes Hall Queen's University Kingston, ON K7L 3N6 <Telephone> <Email Address>	Dr. Yolande Chan, Dissertation Supervisor Professor, Management of IT Queen's School of Business Goodes Hall Queen's University Kingston, ON K7L 3N6 <Telephone> <Email Address>

Appendix I-4: Research Site Requirements

Re: Interviews

Here is what a site visit schedule might entail. This does not have to be done in a single week (although that is preferable from my perspective).

DAY 1: AM meet with Prime Contact[1], overview of privacy program, look at documents, provide mailing labels (see section on Surveys below), etc.
PM conduct 3 interviews

DAY 2: AM conduct 3 - 4 interviews
PM conduct 3 interviews & short debrief with Prime Contact (can be in-person, by phone or email as preferred)

DAY 3: AM conduct 3- 4 interviews
PM conduct 3 interviews & short debrief with Prime Contact (by phone if pref)

DAY 4: AM document review & meet with Prime Contact – major issues, additional documents identified, etc.
PM conduct 3-4 interviews.

DAY 5: AM - loose ends tied up with Prime Contact – drop off final batch of survey kits
PM – departure.

I need about an hour per interview with 10 minutes in between. I can manage to do about 6 or 7 in a day. I am also happy to meet with people after hours if that would be better for them or, if necessary, by telephone. While my protocol is primarily set for one on one interviews, I am prepared to meet with 2 or 3 people at a time if that is more convenient. For example, I met with 2 help desk people at once and 3 systems developers at once. We could also do a larger group (say 5 or 6) over 1.5 hours if there is an intact group (i.e. privacy task force) that would be important to interview.

Please note that the people I would prefer to interview are those senior enough to have been involved with some of the privacy decisions but not so stratospheric as to be utterly inaccessible.

I would prefer to interview the person with the primary, day to day responsibility for customer information privacy in two one-hour sessions.

[1] The Project Contact is my term to denote someone with whom I can coordinate activities. It does not have to be you but someone you designate. This person may be different from the Project Sponsor. However, I would prefer to keep the Project Sponsor in the loop to the extent he or she wishes and has the time. This can be accomplished this with a quick email or phone call each day.

Re: Surveys

I will assemble the survey kits including stamped, self addressed envelopes for returning completed surveys to Queen's University. All I require from the participating organization is:
1. a list of names (in addition to those being interviewed) up to 50 employees in retail banking/supporting functions with some "expertise" (loosely defined) on customer information privacy in the organization.
2. a set of mailing labels (internal addresses are fine) that I can affix to the surveys for their distribution.

Re: Documents

I would like to be able to review key privacy documents including privacy audits or assessments, privacy policy manuals, privacy training manuals or other materials, privacy program implementation documents, data maps, information strategy documents and the like. Wherever possible, I would prefer to obtain copies of the documents.

Appendix I-5 – Confidentiality & Non-Disclosure Agreement

THIS CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT made effective this < DATE >

< CORPORATE NAME >
a corporation incorporated pursuant to the laws of <PROVINCE/COUNTRY >
< "ABBREVIATION">

- and –

KATHLEEN GREENAWAY
An individual resident in Ontario
("Kathleen")

WHEREAS:

A. <"ABBREVIATION"> and Kathleen wish to enter into Discussions;

B. <"ABBREVIATION"> will provide Kathleen with Confidential Information during the Discussions; and

C. The Parties wish to outline the terms and conditions upon which the Confidential Information will be given to Kathleen.

NOW THEREFORE, IN CONSIDERATION OF the Parties entering into the Discussions, and <"ABBREVIATION"> making available and disclosing Confidential Information, and or other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

ARTICLE 1 – DEFINITIONS AND INTERPRETATION

1.01 **Definitions**

In this agreement, unless the context otherwise requires:

(a) "Agreement" means this Confidentiality and Non-Disclosure Agreement as from time to time supplemented or amended;

(b) "Discussions" means the discussions between the Parties with respect to <"ABBREVIATION">'s privacy practices and policies, as used in the Project;

(c) "Party" means a party to this Agreement; and

(d) "Person" means an individual, partnership, limited partnership, association, body corporate, joint venture, unincorporated syndicate, unincorporated organization, trustee, trust, executor, administrator, legal representative, governmental authority or agency, or any group or combination thereof;

(e) "Project" means Kathleen's "Information Privacy Orientation" doctoral project at the Queen's School of Business, and subsequent publications, presentations, and materials relating to the doctoral project.

1.02 **Interpretation**

For all purposes of this Agreement, except as otherwise expressly provided or unless the context otherwise requires:

(a) all references in this Agreement to designated "sections", "paragraphs" and other subdivisions are to the designated sections, paragraphs and other subdivisions of this Agreement;

(b) the words "herein", "hereof" and "hereunder" and other words of similar import refer to this Agreement as a whole and not to any particular section, paragraph or other subdivision;

(c) the headings are for convenience only and do not form a part of this Agreement nor are they intended to interpret, define or limit the scope, extent or intent of this Agreement, or any provisions;

(d) any reference to any entity shall include and shall be deemed to be a reference to any entity that is a successor to such entity; and

(e) words importing gender include all genders and words importing the singular include the plural and vice versa.

ARTICLE 2 – CONFIDENTIAL INFORMATION

2.01 **Confidential Information**

"Confidential Information" means, subject to section 2.02 below, any of the following types of information provided by <"ABBREVIATION"> to Kathleen:

(a) all data, reports, computer tapes, notes, interpretations and records containing or otherwise reflecting information concerning marketing plans, business plans, strategies, alliances, forecasts, financial information,

supplier information, technical information, statistics, analysis, reports, policies, procedures, regulatory compliance and any customer information;

(b) all of <"ABBREVIATION">'s technical data and know-how relating to both existing and proposed products, processes, infrastructure, methods, systems and equipment;

(c) business practices of <"ABBREVIATION">;

(d) without limitation, all of <"ABBREVIATION">'s trade secrets; and

(e) proprietary and confidential information of <"ABBREVIATION">'s strategic partners which is or may be disclosed by <"ABBREVIATION">to Kathleen.

2.02 **Not Confidential Information**

The following shall not, for the purposes of this Agreement, constitute Confidential Information:

(a) information relating to <"ABBREVIATION"> that is obtained or was previously obtained by Kathleen from a third Person who, insofar as is known to Kathleen after reasonable inquiry, is not obligated to keep such information confidential;

(b) information that is or becomes generally available to the public other than as a result of disclosure by Kathleen's violation of this Agreement;

(c) information that <"ABBREVIATION"> authorizes Kathleen to disclose.

2.03 **Kept in Confidence**

Subject to this Agreement, any and all Confidential Information shall be held in absolute confidence by Kathleen during the Discussions and at all times thereafter, and such Confidential Information shall neither be used, reproduced in any manner nor disclosed at any time without <"ABBREVIATION">'s prior written consent, except for the purposes of the Project.

2.04 **No Benefit, Restricted Use**

Other than for the purposes of the Project, Kathleen shall not, in any manner, derive any benefit, directly or indirectly, from the Confidential Information or the use of such Confidential Information, for any purpose. Kathleen agrees not to appropriate for her own use or exploit in any way whatsoever any of the Confidential Information disclosed to him/her by <"ABBREVIATION">. Notwithstanding this section, Kathleen may use the Confidential Information for the purposes of her Information Privacy Orientation doctoral project.

2.05 **No Disclosure**

Kathleen will not disclose any of the Confidential Information or other facts directly related to the Confidential Information to any Person, other than her supervisor, Dr. Yolande Chan, and her transcriber, who have a need to know and who have been informed of the confidential nature of the Confidential Information. Kathleen will also ensure that said individuals will comply with the terms of this Agreement and will be responsible for any breach of this Agreement by them.

2.06 **Return/Destruction of Confidential Information**

Kathleen shall be permitted to retain the Confidential Information for a period of five (5) years, at the Queen's School of Business, in accordance with the Queen's University document retention policies and procedures. The retention of the Confidential Information is to provide support and evidence with respect to the Project if necessary. After such time, upon <"ABBREVIATION">'s request Kathleen shall: (i) promptly return to <"ABBREVIATION"> all Confidential Information, together with all copies, or (ii) promptly destroy or erase all notes, memoranda and other material prepared by Kathleen which reflect, interpret, evaluate, include or are derived from any Confidential Information. Kathleen shall certify such destruction in writing to <"ABBREVIATION">. Kathleen shall also provide any information about the Queen's University retention and destruction policy upon request. If the Confidential Information is destroyed in accordance with the Queen's University destruction policy and procedures, Kathleen shall information <"ABBREVIATION"> of the destruction.

2.07 **No Proprietary Rights**

Nothing in this Agreement is intended to grant any rights to Kathleen under any issued or pending patent, trade secret or copyright of <"ABBREVIATION">.

2.08 **Responsibility for Others**

Kathleen agrees that she shall be responsible for any breach of this Agreement by any employees, advisors, representatives or agents.

2.09 **Identification of <"ABBREVIATION">**

In all presentations and written materials, other than in her draft working notes which are to be reviewed only by Kathleen, Kathleen shall identify <"ABBREVIATION"> only by a reference to "a financial institution operating in Canada, with retail banking as one line of business." No references to <"ABBREVIATION"> are permitted.

2.10 **Interview Consent Form**

Kathleen shall obtain consent from any <"ABBREVIATION">employee who is interviewed by Kathleen for a) consenting to the interview; and b) consenting to being audio taped (if applicable). Consent shall be in the form of the Interview Consent Form attached s Schedule A. Participation for any <"ABBREVIATION"> employee is voluntary, and can be withdrawn at any time.

ARTICLE 3 – GENERAL PROVISIONS

3.01 **Remedies**

Kathleen acknowledges and agrees that she has entered into this Agreement on the understanding that any breach hereof by her will cause <"ABBREVIATION"> irreparable harm and expressly agrees that, in addition to all other remedies that <"ABBREVIATION"> may be entitled to as a matter of law, <"ABBREVIATION"> shall be entitled to specific performance and any form of equitable relief to enforce the provisions of this Agreement.

3.02 **Continuing Obligations Regarding Confidentiality**

The obligations of confidentiality contained herein shall survive the completion or termination of the Discussions and shall be binding on Kathleen indefinitely.

3.03 **Notices**

All notices, requests, demands or other communications permitted or required by the terms of this Agreement shall be in writing and shall be delivered addressed as follows:

To:	Kathleen Greenaway Queen's School of Business Queen's University, Goodes Hall, Room 401 Kingston, ON K7L 3N6
Telephone:	(613) 387-3973
Fax:	(613) 533-2622

3.04 **Entire Agreement, Amendment**

This Agreement constitutes the entire agreement between the Parties respecting the subject matter hereof, and supersedes all previous discussions, understandings and negotiations. All modifications or/and amendments to this Agreement must be in writing and executed by the Parties.

3.05 **Severability**

If any provision of this Agreement is held invalid in any respect, it shall not affect the validity of any other provision of this Agreement. If any provision of this Agreement is held to be unreasonable as to duration, scope or otherwise, it shall be construed by limiting and reducing it so as to be enforceable under applicable law.

3.06 **Successors and Assigns**

This Agreement shall be binding upon the Parties and their respective successors and assigns.

3.07 **Jurisdiction**

This agreement will be governed in all respects, whether as to validity, construction, capacity, performance or otherwise, by and under the laws of the <_____>.

IN WITNESS WHEREOF the Parties have executed this Agreement as of the day and year noted beside their respective signatures.

Date: _____ Per: _____

Date: _____ Per: _____

_____ _____ _____

Date Witness KATHLEEN GREENAWAY

Schedule A
Interview Consent Form
Research Study: Information Privacy Orientation

I am willing to participate in this study about my company's customer information privacy policies and practices.

I am aware that this participation consists of being interviewed by the principal investigator, Kathleen Greenaway, and completing a survey questionnaire. The purpose of the interview and survey is for the researcher to investigate the range of approaches that different firms have taken in deciding how to respond to the challenge of balancing their legal obligations and their business requirements with their customers' desire for privacy.

I understand that the researcher will be audio recording the interview as well as taking notes.

I am aware that I can contact the principal researcher, Kathleen Greenaway [(613) 387-3973 kgreenaway@business.queensu.ca], her supervisor [Dr. Yolande Chan (613) 533-2364, ychan@business.queensu.ca], Dr. Stephen Salterio, Chair, Unit Ethics Review Committee, Queen's School of Business, (613) 533-6926, ssalterio@business.queensu.ca; or Dr. Joan Stevenson, Chair, general Research Ethics Board, Queen's University, (613) 533-6288, stevensi@post.queensu.ca if I have any questions, concerns or complaints about this study.

I understand that my participation is **voluntary** and that I am free to withdraw at any time.

I understand that my responses will be kept **confidential** and **anonymous** in any reports or publications arising from this research.

Name: _____ Date: _____

Signature: _____

I further agree that my interview may be audio taped:

Name: _____ Date: _____

Signature: _____

Appendix J: Phase One Privacy Policy Evaluation Study – Detailed Findings

Item Number	Title
J-1	Phase One: Privacy Policies Evaluation Study: Evaluation Form

The findings are organized by firm as follows:

1. Privacy Policy Assessment (Comprehensiveness, Readability and Accessibility).
2. Information Privacy Orientation Definition (Principles, Values, Objectives, Decision Rules).
3. IPO Continuum Layers Evidence (Customer Relationship Stance, Customer Information Management Strategy, Customer Information Privacy Philosophy, Customer Information Privacy Behaviors).
4. Placement on IPO Continuum.

Note that no organization is identified and that the numeric designations neither reflect the alphabetical listing in Table 7-1 nor the case identifiers for the final individual research sites.

J-1.1	Firm 1
J-1.2	Firm 2
J-1.3	Firm 3
J-1.4	Firm 4
J-1.5	Firm 5
J-1.6	Firm 6
J-1.7	Firm 7
J-1.8	Firm 8
J-1.9	Firm 9
J-1.10	Firm 10

Appendix J-1: Phase One: Privacy Policies Evaluation Study: Evaluation Form

ORGANIZATION NAME	
INDUSTRY	
WEBSITE URL	
DATE OF EVALUATION	
EVALUATOR	

Checklist:

- ☐ PIPEDA REQUIREMEMENTS
- ☐ PRIVACY POLICY ASSESSMENT
- ☐ IPO DEFINITION
- ☐ OVERALL ASSESSMENT USING IPO CONTINUUM
- ☐ WAS FIRM CONTACTED?
- ☐ HOW?WHEN? _____
- ☐ EXPLANATION:

PIPEDA REQUIREMEMENTS

1. Are all 10 PIPEDA principles addressed in the policy? (ATTACH POLICY)
2. Is each principle defined?
3. Is an example provided for each principle?

	Principle	**Addressed**	**Defined/Explained**
1	Accountability – An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.		
2	Identifying purposes – The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected		
3	Consent – The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.		
4	Limiting Collection – The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.		
5	Limiting Use, Disclosure, and Retention – Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.		

6	Accuracy – Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.		
7	Safeguards – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.		
8	Openness – An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.		
9	Individual Access – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.		
10	Challenging Compliance – An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.		

PRIVACY POLICY ASSESSMENT

Policy Comprehensiveness: *how well and in-depth is the policy explained?*	• Are all PIPEDA/fair information elements addressed?	
	• Is there a summary of the policy that emphasizes key features?	
	• Is responsibility clearly identified?	
Policy Readability: *how easy is it to understand the policy and its implications?*	• What is the readability score for the privacy policy document(s)? • Is the policy written in accessible language (or in "legalese")?	
	• Are key terms explained?	
	• Are examples provided? Are the examples thorough and understandable?	
	• Are consent forms provided?	
Policy Accessibility *how easy is it to find the policy?*	• How easy is it to find the policy? Are there multiple access points?	
	• Are there links to other privacy information (external)?	
	• Is there a webseal or other "seal of approval"?	

IPO Definition

IPO Definition Component	Evidence
Principles	
Values	
Policies	
Objectives	
Legal	
Technical	
Contractual	
Business	
Social	
Ethical	
Decision rules	

OVERALL ASSESSMENT USING IPO CONTINUUM

Customer relationship stance: characterization of customer interests

Predominant characterization of firm's relationship to its customers based on the definition of its obligations to its customers.

Check the box that best describes the firm's overall behaviours:

	Placement on Continuum	
	Buyer exploitation	
	Buyer self-protection	
	Shared responsibility	
	Consumer well being	

☐ Unable to assess:

_____

_____

_____

_____

Provide examples to support this assessment:

_____

_____

_____

_____

_____

Customer information management strategy: Why is information collected?

A firm's predominant strategy with respect to its objectives for gathering and using customer information.

Check the box that best describes the firm's overall behaviours:

	Placement on Continuum	
	Reduce costs	
	Minimize risks	
	Add value	
	Create new reality	

☐ Unable to assess:

Provide examples to support this assessment:

Customer information privacy philosophy: the law is the real reason to do this

A firm's predominant philosophy about the role and impact that customer information privacy norms and laws have on its ability to carry out its business.

Check the box that best describes the firm's overall behaviours:

	Placement on Continuum	
	Privacy ignored	
	Privacy as constraint	
	Privacy as an exchange	
	Privacy as an opportunity	

☐ Unable to assess:

Provide examples to support this assessment:

Customer information privacy behaviours: control and procedural justice writ large

A firm's publicly visible and internal privacy practices.

{Note: for this evaluation, focus is on "publicly visible" behaviours}

Check the box that best describes the firm's overall behaviours:

	Placement on Continuum	
	Non-compliant	
	Minimally compliant	
	Embracing codes	
	Significantly enhanced	

☐ Unable to assess:

Provide examples to support this assessment:

Appendix J-1.1: Firm 1

Firm 1: Privacy Policy Assessment: Score = 5.5 (2.5 +2 +1)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not referenced • All principles covered, more or less
	• Is there a summary of the policy that emphasizes key features?	At beginning of document: Protecting your Privacy Means • we keep your information and the business you do with us in strict confidence • your information is not sold • you have control over how we obtain, use, and give out information about you • you have access to the information we have about you • we respect your privacy when we market our products and services.
	• Is responsibility clearly identified?	• Implied in context of a complaint (speak to Branch) and generic complaints process
	• Are consent forms provided?	• NO
	• Is there a privacy seal or similar privacy symbol?	• NO
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Primarily in plain English using the active voice ("We'll deal quickly with your request to see your information") • Minimum of "legalese" ("We collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.") • Flesch Reading Ease = 46.0, Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• NO
	• Are examples provided? Are the examples thorough and understandable?	• An absence of examples that might help readers to understand the company's real intentions.
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page • Subsequent pages • Bottom left, next to security and legal links • Scroll to bottom to find
	• Are there links to other privacy information (external)?	• NO

Firm 1: IPO Definition Score = 3 (0 + 0 + 1 + 1 + 1 + 0)

IPO Definition Component			Findings
Principles (external)			• There is no reference to PIPEDA or other sources for privacy principles.
Principles (internal)			• The company respects customers' rights to privacy; claims to offer customers control over the collection, use and disclosure of their personal information. However, there is no specific articulation of privacy principles such as are found in the information offered by other firms in this study.
Values			• The company is committed to "service excellence" and "confidentiality".
Policies			• There is a privacy policy that includes practices, procedures and structures ("our policies and procedures which we practices in order to protect your privacy are in place across [FI]").
Objectives			• The objectives for the privacy policy are less clear and there is no overriding objective that I could discern.
		Legal	
	x	Technical	"we protect your information from error, loss and unauthorized access"
	x	Contractual	"we select the company carefully and confirm that it uses security standards comparable to those of [FI]"
		Business	
		Social	
		Ethical	
Decision rules			• There is no evidence of additional rules pertaining to the implementation of the privacy code.

Firm 1: IPO Continuum

IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility	• Some evidence of mutual interest, in the sense an exchange relationship ("understand your needs and eligibility for products and services") although not a strong sense of any ethical link to privacy or obligation to customer, other than to provide excellent service. • No evidence of exploitation, self-protection or well-being positions.
Customer Information Management Strategy	Risk Management → Add Value	• Limited indication of risk management strategies ("help protect you from unauthorized use of your accounts"). Some allusion to add value position (" bring other products and services to your attention"). • No evidence to support "cost reduction strategies" or "create new reality" position.
Customer Information Privacy Philosophy	Constraint → Exchange	• Limited reference to constraints ("if you don't consent to certain uses of information … we may not be able to provide you with a particular product or service"). Some evidence that customers trade information to receive products and services ("understand your eligibility", "recommend particular products and services to meet your needs"). • No evidence to support position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours	Minimally Compliant	• Limited reference to necessity to comply with law ("comply with legal requirements"). Evidence of sufficient control and justice provisions to comply with PIPEDA. • No evidence of application of professional or trade association codes or to support enhanced privacy position.

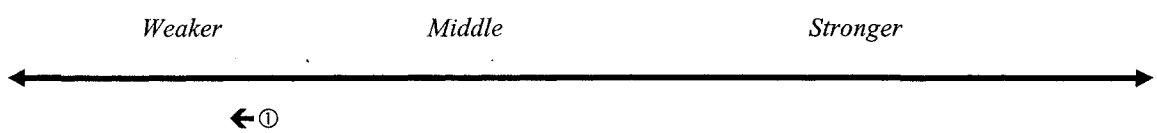
Firm 1: Initial Placement on IPO Continuum Score = 7.5 (0 + 3 + 4.5 + 0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	
	Weaker	←	→	*Stronger*

Overall Assessment

Overall, this company appears to be PIPEDA compliant but they do not appear to be doing very much with privacy beyond compliance. The Canadian legislation places a relatively high hurdle which the firm seems to have met, but without much enthusiasm that is apparent. Based on the evidence mapped to the IPO Continuum, this firm leans towards a weak-middle ground strength of IPO, as shown below.

Summary Placement Score = 20



Appendix J-1.2: Firm 2

Firm 2: Privacy Policy Assessment: Score = 8.5 (4.5 +1.5 +2.5)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not specified • Reference to CSA model code • PIPEDA principles covered thoroughly
	• Is there a summary of the policy that emphasizes key features?	At beginning of document: Protecting your Privacy Means • we keep your information and the business you do with us in strict confidence • your information is not sold • you have control over how we obtain, use, and give out information about you • you have access to the information we have about you • we respect your privacy when we market our products and services.
	• Is responsibility clearly identified?	• Implied in context of a complaint (speak to Branch) and generic complaints process
	• Are consent forms provided?	• NO
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Primarily in plain English using the active voice ("We'll deal quickly with your request to see your information") • Minimum of "legalese" ("We collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.") • Flesch Reading Ease = 46.0, Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• NO
	• Are examples provided? Are the examples thorough and understandable?	• An absence of examples that might help readers to understand the company's real intentions.
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page • Subsequent pages • Bottom left, next to security and legal links • Scroll to bottom to find
	• Are there links to other privacy information (external)?	• NO
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 2: IPO Definition Score = 5.5 (1 + 1 + 1 + 1 + 1.5 + 0)

IPO Definition Component			Findings
Principles (external)			• The commitment statement refers to the Credit Union Central of Canada Model Privacy Code and the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830-96).The company states that it based its own code on these models.
Principles (internal)			• The firm's privacy principles reflect it's "continuing commitment to the protection of your personal information."
Values			• The company expresses its values in terms of customers "inherent rights" to privacy as well as "appropriate conduct".
Policies			• Taken together, the various privacy documents demonstrate that there are practices, procedures and structures in place.
Objectives		Legal	
	x	Technical	"your personal information is protected by security safeguards to protect against theft, as well as unauthorized access, disclosure, copying, use or modification").
	x	Contractual	"... never sells your personal information to any outside company" and "we ensure that all such suppliers employ privacy and security standards and procedures comparable to our own".
	x	Business	"... is proud of its reputation in maintaining the confidentiality and security of personal information" but no reference to enterprise wide objectives such as building trust.
		Social	
		Ethical	
Decision rules			There is no evidence of additional rules pertaining to the implementation of the privacy code.

Firm 2: IPO Continuum

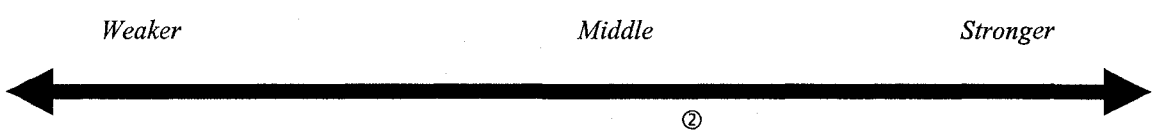
IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility	• Evidence of mutual interest ("we gather and use personal information to provide you the products and services you have requested " and "understand your needs"). There is a great deal of specific information provided to assist customers to understand the reasons for certain actions. • No evidence of exploitation, self-protection or well-being positions.
Customer Information Management Strategy	Minimize risks	• Some evidence of risk management strategies ("detect fraud both to you and the [financial institution]", "establish and verify identity", and "comply with legal requirements"). • No evidence to support "cost reduction, "add value" position. No evidence to support "create new reality" position.
Customer Information Privacy Philosophy	Constraint → Exchange	• Some indication of constraints (collect information only by "fair and lawful means" and "your refusal to provide this information may hamper or seriously impede our ability to offer you certain products and services."). Limited evidence that customers trade information to receive products and services ("assess your suitability and eligibility for products and services"). No evidence to support position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours	Professional Codes	• Customer Information Privacy Behaviours Professional Codes] –The company is clearly compliant. Specific reference is made about their Privacy Code being modelled on their trade association's [CUCC] Model Privacy Code and the CSA Model Code. No evidence to support "significantly enhanced" position.

Firm 2: Initial Placement on IPO Continuum[1] Score = 7.5 (0 + 3 + 4.5 + 0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			✓	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	
	Weaker ⟷			*Stronger*

Overall Assessment

Overall, this company appears to have taken a serious and fairly comprehensive approach to customer information privacy. Good information is provided to address a variety of customer information privacy concerns. The contents of the various statements suggest that this company occupies the middle ground between a weaker and stronger IPO. **Summary Placement Score = 13**



[1] Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.3: Firm 3

Firm 3: Privacy Policy Assessment: Score = 6.0 (1.5 + 2 +2.5)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not referenced • PIPEDA principles covered minimally
	• Is there a summary of the policy that emphasizes key features?	• NO
	• Is responsibility clearly identified?	• Implied in context of a complaint (speak to Branch) and generic complaints process
	• Are consent forms provided?	• NO
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Primarily in plain English using the active voice ("We'll deal quickly with your request to see your information") • Minimum of "legalese" ("We collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.") • Flesch Reading Ease = 46.0, Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• NO
	• Are examples provided? Are the examples thorough and understandable?	• An absence of examples that might help readers to understand the company's real intentions.
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page • Subsequent pages • Bottom left, next to security and legal links • Scroll to bottom to find
	• Are there links to other privacy information (external)?	• NO
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 3: IPO Definition Score = 3 (0 + 0 + .5 + 1 + 1.5 +0)

IPO Definition Component			Findings
Principles (external)			• Reference is made to the development of a "code concerning the protection of personal information" in cooperation with other FIs and the CBA. However, specific details are not provided.
Principles (internal)			• There is no evidence of specific internal privacy principles.
Values			• The company has "always paid special attention to protecting the personal information you entrust to us" and "to make sure that your rights are fully respected."
Policies			• There is some limited information about practices, procedures and structures.
Objectives	x	Legal	• Include compliance with an unspecified law and respect for customer privacy rights.
	x	Technical	• Evidenced by a section in the ABC's of Security which outlines the role of the company's Information Security Group.
	x	Contractual	"require a formal commitment from these suppliers to respect confidentiality of any such information".
		Business	
		Social	
		Ethical	
Decision rules			There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 3: IPO Continuum

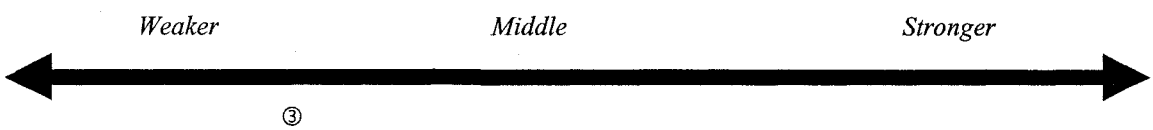
IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility	• Some evidence of mutual interest, in the sense an exchange relationship ("better meet your expectations") although not a strong sense of any ethical link to privacy or obligation to customer, other than to provide service. • No indication of an exploitation or self protection or customer well being position.
Customer Information Management Strategy	Risk Management	• Strong indication of risk management strategies including "identify and manage information security risks" and "assist and advise owners [unspecified] of information in evaluating risks." No evidence to support "Cost reduction", "add value" or "create new reality" positions.
Customer Information Privacy Philosophy	Constraint → Exchange	• Some indication of constraints (i.e., repeated references to "rights" as well as the "consequences" of decisions where consent is denied). Some evidence that customers trade information to receive products and services ("determine your eligibility"). No evidence of "create new reality" position.
Customer Information Privacy Behaviours	Minimally Compliant → Embracing Codes	• Reference to necessity to comply with law. Repeated reference to trade association's [CBA] Code but little evidence presented about how the firm's actions follow the model Code. • No evidence to support enhanced privacy position.

Firm 3: Initial Placement on IPO Continuum[2] Score = 7.5 (0 + 3 + 4.5 + 0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	
	Weaker	⟷		*Stronger*

Overall Assessment

On balance, this company appears to be PIPEDA compliant but they do not appear to be doing very much with privacy beyond compliance. The Canadian legislation places a relatively high hurdle which the firm likely has met, but the manner of communication suggests that privacy is not a priority issue beyond compliance, most particularly with respect to safeguards and security. **Summary Placement Score = 19**



[2] Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.4: Firm 4

Firm 4: Privacy Policy Assessment: Score = 12 (7 + 3 +2)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPAEDA (sic) specified • CSA Model Code referenced • PIPEDA principles covered thoroughly
	• Is there a summary of the policy that emphasizes key features?	• Yes • Also FAQ
	• Is responsibility clearly identified?	• Several references to Privacy Officer but not identified by name; contact information provided • Privacy Representative at each branch for questions, concerns
	• Are consent forms provided?	• YES – opt out form
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	Policy • Flesch Reading Ease = 19.2, • Flesch Kincaid Grade Level = 12 FAQ • Flesch Reading Ease = 35.6 • Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• Legal definitions
	• Are examples provided? Are the examples thorough and understandable?	• Many
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Two links from home page • Links from subsequent pages
	• Are there links to other privacy information (external)?	• External organization (unspecified Privacy Commissioner) identified but not linked
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 4: IPO Definition Score = 7.5 (1.5 + 1 + 1 + 1 + 3 + 0)

IPO Definition Component			Findings
Principles (external)			• The introduction to the Privacy Code refers to the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) and PIPAEDA (sic). The company states that it based its own code on these models.
Principles (internal)			• The firm's privacy principles are adapted from the CSA and PIPEDA principles – "we have tailored our own ten privacy principles to meet these specific needs and expectations of our membership."
Values			• The company expresses its values in terms of legal compliance and "ethical obligations".
Policies			• This is one of the most comprehensive policies reviewed. • Considerable detail is provided about information collection, use, security and other activities that may impinge upon or support customer information privacy. • For example, the Accountability section indicates that the firm "has developed policies and procedures to: protect personal information; receive and respond to complaints and inquiries; train staff regarding the policies and procedures; communicate the policies and procedures to our members." (Note that most firm's refer to employee obligations to maintain confidentiality but seldom is training for personnel specifically indicated.)
Objectives	×	Legal	• Legal compliance objective permeates the Code ("will use methods [of information collection] that are lawful").
	×	Technical	• "changes in technology necessitate that [the company] continually develops, updates and reviews information protection guidelines and controls to ensure ongoing information security".
	×	Contractual	• "will not sell member lists or personal information to Third Parties" and ensuring that contracts with market research firms will have "appropriate security undertakings, such as confidentiality clauses."
	×	Business	• "to serve members as effectively and conveniently as possible" but no reference to enterprise wide objectives such as building trust.
	×	Social	• "understand my financial and banking needs"
	×	Ethical	• "ensuring the accuracy, confidentiality, and security" of personal information is "an ethical obligation." However, this statement is not developed further in any privacy specific documents I reviewed.
Decision rules			• There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 4: IPO Continuum

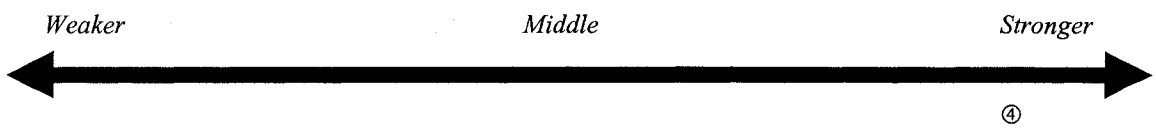
IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility → Consumer Well-Being	• Strong evidence of mutual interest ("the better we know you, the more able we are able to provide the best products and services to meet your financial needs"). • There is a great deal of specific information provided to assist customers to understand the reasons for certain actions. • There is very limited evidence ("an ethical issue") that suggests that the firm feels obliged to promote customer well being (at its own expense). • No indication of an exploitation or self protection position.
Customer Information Management Strategy	Minimize risks → Add Value	• Very limited indication of risk management strategies ("appropriate security measures are employed in the transfer of sensitive information" and "verify identity"). • Limited evidence to support add value position ("In order to provide you with a high level of service and an extensive range of products, we need to know who you are and understand your financial needs"). • No discussion of cost reduction strategies and no evidence to support "create new reality"
Customer Information Privacy Philosophy	Exchange	• Minimal discussion of constraints ("if you [choose not to provide certain information], we may not be able to provide you with the product, service or information that you requested"). • Some evidence that customers trade information to receive products and services ("determine your eligibility"), but language is strongly in the mutual exchange vein. • No evidence to support position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours	Professional Codes	• The company is clearly compliant. • Specific reference is made about their Privacy Code being modelled on professional/trade association CSA Model Code. • Site provides an online Opt Out form and clear information about consequences. Good clear process for complaints and enquiries and specifically indicate Privacy Commissioner role. • No evidence to support "significantly enhanced" position.

Firm 4: Initial Placement on IPO Continuum[3] Score = 11 (0 + 3 + 6 + 2)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓	✓	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	✓
	Weaker ⟷			*Stronger*

Overall Assessment

Overall, this company appears to have taken a serious and comprehensive approach to customer information privacy. The information provided addresses different levels of customer information interests from very general statements in easy to understand language to very specific details in more legalistic language. The contents of the various statements suggest that this company leans towards a stronger rather than weaker strength of IPO. **Summary Placement Score = 5**



[3] Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.5: Firm 5

Firm 5: Privacy Policy Assessment: Score = 11 (5.5 + 3 +2.5)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA specified • CSA Model Code referenced • PIPEDA principles covered thoroughly
	• Is there a summary of the policy that emphasizes key features?	• YES
	• Is responsibility clearly identified?	• Generic reference within Accountability Principle • Contact information provided for Customer Relations Centre •
	• Are consent forms provided?	• NO • 1-800 number provided
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 15.8 • Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• Technical terms
	• Are examples provided? Are the examples thorough and understandable?	• Many
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Two links from home page • Links from subsequent pages
	• Are there links to other privacy information (external)?	• Privacy Commissioner of Canada • Electronic Commerce Branch of Industry Canada
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 5: IPO Definition Score = 8.5 (1.5 + 1.5 + 1.5 + 1 + 3 + 0)

IPO Definition Component			Findings
Principles (external)			• The "values" established in the CSA Model Code and PIPEDA are the basis for the firm's own code.
Principles (internal)			• The firm has adopted the PIPEDA principles as its own "tailored ... to meet the specific needs and expectations of our clients." In addition, the firm is committed to "meeting or exceeding the privacy standards" set by governments and regulatory agencies (although examples of "exceeding" are not provided).
Values			• The company expressly describes "safeguarding your confidentiality and protecting your personal and financial information" as "fundamental to the way we do business."
Policies			• This is one of the most comprehensive policies reviewed. • Considerable detail is provided about information collection, use, security and other activities that may impinge upon or support customer information privacy. • For example, sharing of information with outside service providers is done both within a contractual framework ("strict contractual obligations .. to protect privacy and security of your information") as well as within the privacy framework ("protect your information in a manner that is consistent with the privacy policies and practices that we have established").
Objectives	×	Legal	("meet or exceed the privacy standards established by federal and provincial regulations and industry bodies" and "This privacy policy has been developed to meet the compliance standards established by Canada's *Personal Information Protection and Electronic Documents Act*, the CSA *Model for the Protection of Personal Privacy* and OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*").
	×	Technical	P3P, Freedom software as well as "state of the art technology" that employs safety and security measures ... appropriate to the sensitivity level of your information"
	×	Contractual	("strict contractual obligations .. to protect privacy and security of your information").
	×	Business	("dedicated to protecting your privacy", "one of our highest priorities," and "remains the cornerstone of our commitment to you"). However, there is no statement about, for example, building trust.
	×	Social	"to establish and maintain a positive relationship with you."
	×	Ethical	("all employees .... are required to abide by the privacy standards we have established. They are also required to work within the principles of ethical behavior as set out in our internal Employee Rules"
Decision rules			There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 5: IPO Continuum

IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility → Consumer Well Being	• Strong evidence of mutual interest ("The better we know you, the better we can help you achieve your financial goals"). Comprehensive information to assist customers to understand the reasons for certain actions. • There some evidence to suggest that the firm feels obliged to promote customer well being by arranging to pay for free one year privacy protection software subscription. • No indication of an exploitation or self protection position.
Customer Information Management Strategy	Risk Management → Add Value	• Very limited indication of risk management strategies ("safeguard your interests", "authenticate your identity", "protect yourself against fraud and uninvited intrusion"). • Strong evidence of add value position ("Clients today no longer look to us to simply fulfill their banking requirements, but rather to provide responsible and reliable financial services and value-added advice"). • No discussion of cost reduction strategies and no evidence to support "create new reality" position.
Customer Information Privacy Philosophy	Exchange → Opportunity	• Limited evidence of constraint position. • Language is strongly in the mutual exchange vein ("[PIPEDA]… is essentially about balance. On one hand, it respects an individual's right to privacy while on the other, it recognizes the need for industry and organizations to collect, use and disclose personal information"). • Some evidence to support position of privacy as an opportunity for the firm (" has been a strong supporter of industry privacy standards and related government regulation).
Customer Information Privacy Behaviours	Significantly Enhanced	• Demonstrably compliant and with aspirations to exceed compliance (what constitutes exceeding is not specifically defined). • Evidence of embracing codes ("We played an active role in the development of the Canadian Bankers Association (CBA) *Privacy Model Code* and the Canadian Standards Association's (CSA) *Model for the Protection of Personal Privacy*"). • Strong evidence of enhanced

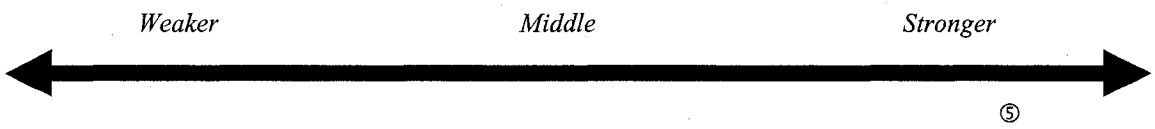
		behaviors, especially with respect to customers exercising control. Two specific enhanced behaviors are evident. First, incorporating P3P ("Although P3P has not yet gained widespread application, we appreciate clients may be anxious to take advantage of it. We want them to be able to do so without impacting their ability to access our Web sites or to conduct on-line transactions. Accordingly, P3P privacy statements have already been deployed in several [of our] sites and, it is our intention to complete this process on all remaining sites"). Second, providing free privacy protection software (" we've arranged for Zero-Knowledge Systems to provide [our] customers with the option of selecting tools that provide an additional level of privacy and security online...[company is] happy to offer a limited time FREE trial of Freedom Parental Control and Freedom Anti-Virus included in the 1-year free subscription version of Freedom for [company's] customers!)".

Firm 5: Initial Placement on IPO Continuum[4] Score = 15 (0 + 3 + 6 + 6)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
			✓	✓
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	✓
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	✓
	Weaker ◄———			———► *Stronger*

Overall Assessment

Overall, this company appears to have attempted to differentiate themselves with their comprehensive, enthusiastic and relatively unique approach to customer information privacy. They clearly are on the stronger side of the IPO continuum. **Summary Score = 4**



[4] Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.6: Firm 6

Firm 6: Privacy Policy Assessment: Score = 8.5 (3 + 3 +2.5)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not specified • PIPEDA principles covered minimally
	• Is there a summary of the policy that emphasizes key features?	• YES
	• Is responsibility clearly identified?	• No mention of a designated Privacy Officer • Contact information provided for Customer Relations Centre, Ombudsman
	• Are consent forms provided?	• No • 1-800 number provided
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 43.6 • Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• NO
	• Are examples provided? Are the examples thorough and understandable?	• Many
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Two links from home page • Links from subsequent pages
	• Are there links to other privacy information (external)?	• External organization (Privacy Commissioner of Canada) identified but not linked, contact info provided • Ombudsman for Banking Services and Investments
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 6: IPO Definition SCORE = 4.5 (0 + .5 + 1.5 + 1 + 1.5 +0)

IPO Definition Component			Findings
Principles (external)			• There is no reference to PIPEDA, CSA model code or CBA model code.
Principles (internal)			• The company's privacy policy is based on five principles - collection and use, release, protection, access and accuracy, and respecting and responding to concerns.
Values			• The company has always treated "protecting your privacy and the confidentiality of your personal information" as "fundamental" to their way of conducting business. Other values appear to be "best customer service" which means treating customers "fairly and with respect" and "meeting your customer service expectations."
Policies			• There is a privacy policy that includes practices, procedures and structures. However, there is little information on accountability for the success of the policy (i.e., no mention of a privacy officer or manager, no email link to the privacy staff).
Objectives		Legal	
	x	Technical	• Limited evidence ("We will protect your information with appropriate safeguards and security measures") but the privacy policy is not hotlinked to the security section of the website.
	x	Contractual	• The firm has confidentiality requirements in place with third party contractors
		Business	
	x	Social	• suggested by an exchange proposition ("sharing your information helps us to determine your financial needs … and offer you other products and services … that we believe will be of interest to you").
		Ethical	
Decision rules			There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 6: IPO Continuum

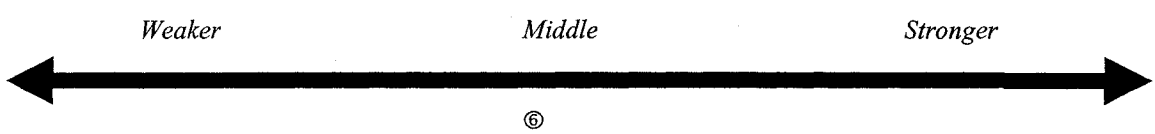
IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Self Protection to Shared Responsibility	• Limited evidence of a customer self protection position is offered in the section concerning transfers of business – " ... [as the company continues]to develop and grow, we may buy or sell parts of our businesses. As our businesses consist primarily of our customer relationships, personal customer information and information regarding the particular account or service being purchased or sold would generally be one of the transferred business assets." There is no apparent provision for advising customers and allowing them to exercise choice in having the "assets" transferred to other entitities. • Some evidence of mutual interest, in the sense an exchange relationship although not a strong sense of any ethical link to privacy or obligation to the customer, other than to act according to their policy. Neither is there evidence that the firm feels obliged to promote customer well being. • No indication of an exploitation or a customer well being position.
Customer Information Management Strategy	Risk Management → Add Value	• Limited indication of risk management strategies ("thorough security standards to protect our systems and your information against unauthorized access and use"). • Some allusion to add value position ("lets us instantly recognize your total relationship with [us]" and "offer you other ... products and services.")– including special promotions"). • No discussion of cost reduction strategies and no evidence to support "create new reality" position.
Customer Information Privacy Philosophy	Constraint → Exchange	• Legal constraints appear either "as law requires or permits" or "explanations of decisions not to consent." • Some evidence that customers trade information to receive products and services ("assess your eligibility", "ensure that advice is appropriate" and "required for some products"). • No evidence of opportunity position.
Customer Information Privacy Behaviours	Minimally Compliant	• Appears to have sufficient control and justice provisions likely to comply with PIPEDA. • No reference to additional codes or practices. No evidence to support enhanced privacy position.

Firm 6: Initial Placement on IPO Continuum[5] Score = 8.5 (0 + 4 + 4.5 =0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
		✓	✓	
	Weaker	⟷		*Stronger*

Overall Assessment

Overall, this company appears to be PIPEDA compliant but they do not appear to be doing very much with privacy beyond compliance. The Canadian legislation places a relatively high hurdle which the firm seems to have met, but without much enthusiasm. **Summary Placement Score = 14**



5

Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.7: Firm 7

Firm 7: Privacy Policy Assessment: Score = 2 (0 + 2 + 0)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not specified • PIPEDA principles not covered
	• Is there a summary of the policy that emphasizes key features?	• NO
	• Is responsibility clearly identified?	• No mention of a designated Privacy Officer •
	• Are consent forms provided?	• NO
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 28.0 • Flesch Kincaid Grade Level = 12).
	• Are key terms explained?	• NO
	• Are examples provided? Are the examples thorough and understandable?	• NO
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page and subsequent pages
	• Are there links to other privacy information (external)?	• NO
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 7: IPO Definition Score = 1.5 (0+ 0+ .5 + 0 + 1 + 0)

IPO Definition Component			Findings
Principles (external)			• There is no reference to PIPEDA only to "applicable legislation."
Principles (internal)			• There are no stated privacy principles.
Values			• The company acknowledges that customer information privacy is an obligation.
Policies			• There is no posted privacy policy. However, there is very limited information to suggest that there is some understanding of very basic practices. In the absence of a framework (such as PIPEDA principles) it is difficult to discern what the exact policy might be.
Objectives	x	Legal	• overriding objective appears to be a legal concern to save harmless the financial institution.
	x	Technical	• also apparent given the discussion of encryption, password protection, etc.
		Contractual	
		Business	
		Social	
		Ethical	
Decision rules			• There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 7: IPO Continuum

IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Self-Protection to Shared Responsibility	• Evidence that customers are expected to protect themselves when dealing with the firm. • Evidence of mutual interest, in the sense an exchange relationship although not a strong sense of any ethical link to privacy or obligation to customer. The language is very "transactional" (in the behavioural sense of the word). For example, the section entitled "Our respective responsibilities", states: "If fraudulent activity occurs on your accounts because of a breach in computer security, we will restore your account balances to what they should be as long as you are not responsible in any way for the breach of security. In other words, we expect you to do your own part in preventing fraud". • No indication of an exploitation position and no evidence that the firm feels obliged to promote customer well being.
Customer Information Management Strategy	Risk Management	• Strong indication of risk management strategies especially fraud prevention. • No discussion of cost reduction strategies and no evidence to support add value or create new reality positions.
Customer Information Privacy Philosophy	Insufficient data to assess	
Customer Information Privacy Behaviours	Not compliant	• Does not supply sufficient information to indicate compliance with PIPEDA.

Firm 7: Initial Placement on IPO Continuum[6] Score = 4 (1 + 1.5 + 1.5 + 0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
	✓			
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
	✓			
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓		
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
		✓	✓	
	Weaker	⟷		*Stronger*

Overall Assessment

Overall, this company appears not to be PIPEDA compliant. The Canadian legislation places a relatively high but arguably explicit hurdle which does not appear to have been met. In fairness, it may be that the firm provides detailed privacy information within the secure online banking section of the website but I could not enter that area as it is password protected. This suggests an interesting choice given that no other financial institution in this study has treated providing privacy information in this way. **Summary**

Placement Score = 24

[6] Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.8: Firm 8

Firm 8: Privacy Policy Assessment: Score = 10 (5.5 + 3 +1.5)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA specified • (Provincial) trade association privacy code • Consistent with CSA standards
	• Is there a summary of the policy that emphasizes key features?	• YES
	• Is responsibility clearly identified?	• Generic reference within Accountability Principle • Several references to Privacy Officer but not identified by name; available through email link
	• Are consent forms provided?	• NO
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 37.8 • Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• Legal definitions
	• Are examples provided? Are the examples thorough and understandable?	• Some examples
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page and subsequent pages
	• Are there links to other privacy information (external)?	• External organization (provincial Privacy Commissioner) identified but not linked
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 8: IPO Definition Score = 5.5 (2 + 0 +1 + 1 + 1.5 +0)

IPO Definition Component			Findings
Principles (external)			• Reference is made to CSA standards, the Alberta Credit Union Model Code, PIPEDA and Alberta's Personal Information Protection Act. The ACU Model Code's 10 principles form the basis for the Credit Union's privacy approach.
Principles (internal)			• There are no stated internal principles other than the evidence that the ACU Privacy Code's external principles have been adopted by the credit union.
Values			• The company expresses its values in terms of legal compliance, respecting rights, and maintaining confidentiality.
Policies			• The firm asserts that it has established policies and procedures and ensure that employees follow them carefully. Details of many of these procedures are evident in all three documents.
Objectives	x	Legal	"in order to comply with new privacy laws".
	x	Technical	"We will protect your personal information with appropriate security safeguards."
	x	Contractual	"Our suppliers and their employees are required to protect your information in a manner that is consistent with our Privacy Code."
		Business	
		Social	
		Ethical	
Decision rules			• There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 8: IPO Continuum

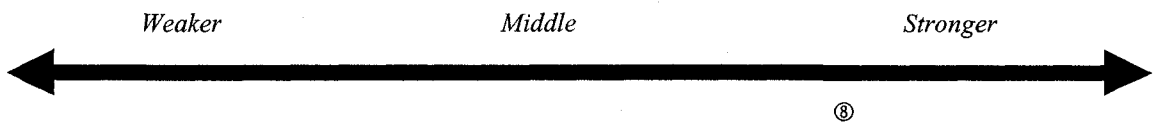
IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility	• Evidence of mutual interest ("We hold personal information about members to help us meet and maintain the highest standards of financial service"). There is specific information provided to assist customers to understand the reasons for certain actions. There is no evidence that suggests that the firm feels obliged to promote customer well being (at its own expense). • No indication of an exploitation or self protection position.
Customer Information Management Strategy	Risk Management → Add Value	• Limited indication of risk management strategies ("establish your identification", protect you from illegal activity", and "ensure that [your] personal and financial information is secure"). • Stronger evidence to support add value position ("provide you with information or advice on products and services that may interest you" and "conduct research to assist us in designing products and services, and determining products and services that may be of interest to you, and to obtain your feedback on current products and services"). • No discussion of cost reduction strategies and no evidence to support "create new reality" position.
Customer Information Privacy Philosophy	Exchange	• Minimal discussion of constraints ("Withdrawing consent to collect, use, or disclose personal information could mean that the credit union cannot provide the member with the product, service, information of value, or even continued membership"). • Some evidence that customers trade information to receive products and services ("operate and administer products and services which you have requested"). • No evidence to support position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours	Professional Codes	• The company is clearly compliant. • In addition, there is strong evidence for Professional Codes position. Specific reference is made to the CSA standards" (i.e., Model Code) serving as the basis for the Alberta Credit Unions Privacy Code and that the Alberta Code serves as the credit union's code. ("[credit union] not only meets that requirements of these laws, but we also subscribe to the Alberta Credit Unions Privacy Code adopted in April 2001"). Some evidence is that control and justice provisions are linked to the attainment of benefits. Good clear process for complaints and enquiries and specifically indicate Provincial Privacy Commissioner role. • No evidence to support "significantly enhanced." position.

Firm 8: Initial Placement on IPO Continuum[7] Score = 9 (0 + 3 + 6 +0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓	✓	
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	
	Weaker ←			→ Stronger

Overall Assessment

Overall, this company appears to have taken a serious and comprehensive approach to customer information privacy. The information provided addresses different levels of customer information interests from very general statements in easy to understand language to very specific details in more legalistic language. The contents of the various statements suggest that this company leans towards a stronger rather than weaker strength of IPO. **Summary Placement Score = 9**



7

Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.9: Firm 9

Firm 9: Privacy Policy Assessment: Score = 9 (4.5 + 3 +1.5)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not specified • PIPEDA principles covered thoroughly
	• Is there a summary of the policy that emphasizes key features?	• Yes • Also FAQ
	• Is responsibility clearly identified?	• Generic reference within Accountability Principle • Several references to Privacy Officer but not identified by name; available through email link
	• Are consent forms provided?	• No • Contact Centre number provided
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	Policy • Flesch Reading Ease = 16.4 • Flesch Kincaid Grade Level = 12 FAQ • Flesch Reading Ease = 34.9 • Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• Legal definitions
	• Are examples provided? Are the examples thorough and understandable?	• Many examples
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page and subsequent pages
	• Are there links to other privacy information (external)?	• Canadian Marketing Association • Other external organizations (Credit Union Central of Canada, to a regulator, or to an independent mediator or arbitrator), no contact info provided
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 9: IPO Definition Score = 5 (0 + .5 +1.5 + 1 + 2 +0)

IPO Definition Component			Findings
Principles (external)			• No specific reference is made to external principles.
Principles (internal)			• "Respect for your privacy and protection of your personal information have always been foremost among our fundamental principles of business." The Privacy Pledge states 10 principles that reflect the PIPEDA/CSA and various model code principles without referring to them specifically.
Values			• The company expresses its values in terms of respect for privacy, and corporate compliance ("consistent with our mission and beliefs" and "inherent responsibility to be open and accessible").
Policies			• The firm asserts that it has established policies and procedures and ensure that employees, officers and directors follow them carefully. Details of many of these procedures are evident in all privacy related documents.
Objectives	×	Legal	• compliance objective ("in preparation for new legislation expected in January 2004").
	×	Technical	• "[FI] will protect personal information with security safeguards appropriate to the sensitivity of the information."
	×	Contractual	• "before we release any personal information, we ensure that the organization will abide by our high standards for protection of your privacy."
		Business	
		Social	
	×	Ethical	• ×"Employees, officers and directors are individually required to sign an oath of ethical conduct, including a commitment to keep members' personal information in strict confidence".
Decision rules			There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 9: IPO Continuum

IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility	• Limited evidence of mutual interest ("understand your financial needs" and "protect you and the credit union"). • There is specific information provided to assist customers to understand the reasons for certain actions. • There is no evidence that suggests that the firm feels obliged to promote customer well being (at its own expense). • No indication of an exploitation or self protection position.
Customer Information Management Strategy	Risk Management to Add Value	• Some evidence of risk management strategies ("help safeguard the financial interests of the credit union and its members by detecting and preventing criminal activity). • Stronger evidence to support add value position ("provide members with about products and services that may be of interest to them" and "research, develop and present products and services that may interest you"). • No discussion of cost reduction strategies and no evidence to support "create new reality" position.
Customer Information Privacy Philosophy	Exchange	• Minimal discussion of constraints ("It is important to know that your decision to withhold information may limit the services we are able to provide you."). • Some evidence that customers trade information to receive products and services ("Provide you with the services and products you request"). • No evidence to support position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours	Minimally compliant to Professional Codes	• The company is clearly compliant. • There is limited evidence for Professional Codes position. It appears that either the Alberta Credit Unions Privacy Code (as certain wording is familiar – see Website 8) or the Credit Union Central of Canada Code (reference is made to CUCC for dispute resolution) has been consulted and, perhaps, adapted. However, this is not stated anywhere in the documents I consulted. • Some evidence is that control and justice provisions are linked to the attainment of benefits. Good clear process for complaints and enquiries and specifically indicate Provincial Privacy Commissioner role.[8] • No evidence to support "significantly enhanced" position.

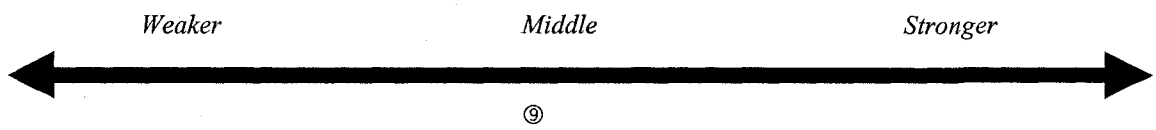
[8] Despite my inferring that the firm uses a "professional or trade group" approach, I do not identify this position on the IPO continuum (next page). This was done to ensure consistency and fairness in the determination of positions.

Firm 9: Initial Placement on IPO Continuum[9] Score = 6 (0 + 3 + 3 + 0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	
	Weaker	◄———	———►	Stronger

Overall Assessment

Overall, this company appears to have taken a serious and comprehensive approach to customer information privacy. The information provided addresses different levels of customer information interests from very general statements in easy to understand language to very specific details in more legalistic language. The contents of the various statements suggest that this company is in the middle ground between weaker and stronger IPO. **Summary Placement Score = 14**



9

Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix J-1.10: Firm 10

Firm 10: Privacy Policy Assessment: Score = 8 (3 + 3 +2)

Descriptor	Indicators	Evidence
Policy Comprehensiveness	• Are all PIPEDA information elements addressed?	• PIPEDA not specified • PIPEDA principles covered thoroughly
	• Is there a summary of the policy that emphasizes key features?	• YES
	• Is responsibility clearly identified?	• Several references to Privacy Officer but not identified by name; contact info provided
	• Are consent forms provided?	• NO
Policy Readability	• Is the policy written in accessible language (or in "legalese")?	• Flesch Reading Ease = 34.3 • Flesch Kincaid Grade Level = 12
	• Are key terms explained?	• Some technical terms
	• Are examples provided? Are the examples thorough and understandable?	• Some examples
Policy Accessibility	• How easy is it to find the policy? Are there multiple access points?	• Home page and subsequent pages
	• Are there links to other privacy information (external)?	• External organization (Privacy Commissioner of Canada) identified but not linked, contact info provided • Ombudsman for Banking Services and Investments
	• Is there a privacy seal or similar privacy symbol?	• NO

Firm 10: IPO Definition Score = 3.5 (0 + 0+.5 + 1 + 2 +0)

IPO Definition Component			Findings
Principles (external)			• There is no reference to PIPEDA, CSA or similar external sources for privacy principles.
Principles (internal)			• There is not reference to specific set of privacy principles.
Values			• The company is committed to providing confidential and secure banking services and views the provision of privacy as "critical".
Policies			• The privacy policy demonstrates that there are practices, procedures and structures. While on the surface this is similar to other organizations, there is a level of detail that exceeds some other sites. For example, the term "personal information" is defined and several examples are provided.
Objectives		Legal	
	×	Technical	"we work hard to protect your confidential information and privacy online"
	×	Contractual	("if we obtain client lists from other organizations, we first require that the organizations to confirm that they comply with all relevant privacy legislation"
	×	Business	better customer service
	×	Social	"establish a lasting relationship with you that will grow and change as your financial needs evolve"
		Ethical	
Decision rules			There is no evidence that there are additional rules pertaining to the implementation of the privacy code.

Firm 10: Applying the IPO Continuum

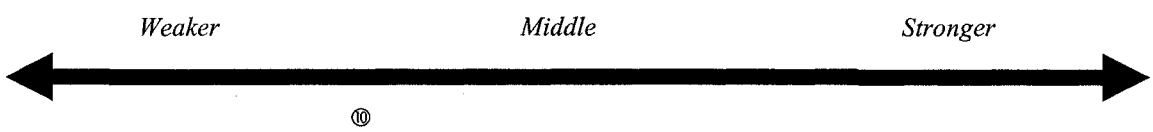
IPO Continuum Layer	Positioning	Evidence
Customer Relationship Stance	Shared Responsibility	• Strong evidence of mutual interest ("the better we know you, the better we are able to serve you"). A goodly amount of information to assist customers to understand the reasons for certain actions. • However, there is no evidence that the firm feels obliged to promote customer well being (at its own expense). • No indication of an exploitation or self protection position.
Customer Information Management Strategy	Risk Management to Add Value	• Very limited indication of risk management strategies ("verify your identity and protect against fraud"). • Strong evidence of add value position ("to provide you with value-added service … and to establish a lasting financial relationship"). • No discussion of cost reduction strategies and no evidence to support "create new reality" position.
Customer Information Privacy Philosophy	Constraint to Exchange	• Minimal discussion of constraints ("if you [choose not to provide certain information], we may not be able to provide you with the product, service or information that you requested"). • Some evidence that customers trade information to receive products and services ("determine your eligibility", but language is strongly in the mutual exchange vein. • No evidence to support position of privacy as an opportunity for the firm.
Customer Information Privacy Behaviours	Minimally compliant to Professional Codes	• No reference to privacy law. • However, demonstrably compliant with PIPEDA. • Some evidence is that control and justice provisions are linked to the attainment of benefits despite lack of connection to trade association codes or similar. For example, providing contact information goes beyond the requirement to appoint a responsible person. • No evidence to support enhanced privacy position.

Firm 10: Initial Placement on IPO Continuum[10] Score = 6 (0 + 3 + 3 + 0)

Customer Information Privacy Behavior	Non Compliant	Minimally Compliant	Professional or Trade Group Codes	Enhanced Privacy
		✓		
Customer Information Privacy Philosophy	No Awareness or Concern for Privacy	Privacy as Constraint	Privacy as Exchange	Privacy as Differentiator
		✓	✓	
Information Management Strategy	Manage to Reduce Information Costs	Manage to Minimize Risks	Manage with Information to Add Value	Manage with Information to Create New Reality
		✓	✓	
Customer Relationship Stance	Buyer Exploitation	Buyer Self-Protection	Shared Responsibility	Consumer Well-being
			✓	
	Weaker	⟷		*Stronger*

Overall Assessment

Overall, this company appears to have taken on the privacy challenge with some enthusiasm and to demonstrate their concern for their customers. This firm appears to be at the weak edge of the middle ground between weaker and stronger IPO. **Summary Placement Score = 18**



[10] Note: Weaker evidence (i.e., statement with no supporting evidence) is indicated by using a smaller check mark. Stronger evidence (i.e., statement with evidence, multiple supported statements) is indicated using a larger and bolded checkmark.

Appendix K: Case A (Pilot Study) - Supplementary Information from Case Study Database

This appendix includes information from the Case A case study database as indicated in the following table:

Item Number	Title	Description
K-1	Research Setting	Describes the setting and data collection activities.
K-2	Interviews	Lists the individuals interviewed by position.
K-3	Statistics	Distribution of Completed Surveys
K-4		Survey Respondent Characteristics
K-5	Documents	Desirable privacy documents.
K-6		Frequencies and Means from IPO Survey

Appendix K-1: Case A - Research Setting and Site Visit

A regional financial institution in Canada with retail banking as one of its lines of business was recruited for the pilot test. I was "sponsored" by a senior marketing executive but negotiated entry with the Project Manager for Compliance Initiatives ("Project Manager") who is located in the Sales Operations division. This individual reports to the *de jure* Chief Privacy Officer. We agreed on the wording of a Confidentiality and Non-Disclosure agreement and arranged for a 3 day site visit. The Project Manager and I exchanged a series of telephone calls and emails in which we discussed the range of potential interview subjects available and agreed upon an approach. The Project Manager contacted the interview subjects and arranged the meeting schedule. The company and its staff were very welcoming and provided meeting facilities. The site visit was conducted June 1-3, 2004 at the company's head office complex.

A few aspects of the pilot test setting require comment. The organization is subject to provincial privacy legislation, not the federal privacy legislation. I did not consider this an issue as the provincial legislation is deemed "substantially similar" to the federal statute[1]. Second, the pilot site is smaller than any of the national chartered banks in scope, scale and network but equivalent to a large credit union. I considered this to be a "good" problem in that it reduced the level of organizational complexity with which I had to contend at the formative stage in my research. Third, the organization was in the early stages of its privacy program. The risk was that there would be little to talk about in the interviews. I was prepared to accept this risk given that my main purpose was to test instruments rather than conduct specific case research at this site[2].

---

[1] The federal statute required that all organizations that were not deemed to be "federal concerns" were to comply with PIPEDA effective January 1, 2004. The exception was for organizations within jurisdictions with private sector protection legislation that was deemed "substantially similar." The legislation passed by the jurisdiction within which the pilot site is situated will be deemed "substantially similar" in the summer of 2004 (PCC 2004). A previous federal Privacy Commissioner defined substantially similar in the following manner: "In assessing provincial legislation, I will interpret substantially similar to mean equal or superior to the PIPED Act in the degree and quality of privacy protection provided" (PCC 2003).

[2] It should be noted that the pilot test organization has requested both a detailed report from this research exercise and that I return next summer for follow-up interviews. Therefore, this site may serve as a longitudinal case site for other research projects about information privacy orientation.

Appendix K-2: Case A - Interviews

Title/Role	Interview Guide	Interview type	
1. Vice President, Legal and Corporate Compliance	Legal	In person, audio taped	Individual
2. Legal Counsel	Legal	In person, audio taped	Individual
3. Vice President, Sales Operations and Chief Privacy Officer	General	In person, audio taped	Individual
4. Project Manager Compliance Initiatives	Privacy I & Privacy II	In person and telephone	Individual
5. Corporate policy	General	In person, audio taped	3 staff at once
6. Operations Help Desk	Privacy 1	In person, audio taped	2 staff at once
7. IT project management office	IT	In person, audio taped	Individual
8. IT system security	IT	In person, audio taped	Individual
9. Project business lead, CSA project	General plus some IT questions	In person, audio taped	Individual
10. Vice-President, Personal and Business Banking – Marketing	Marketing	Telephone, not taped	Individual
11. Senior Manager Marketing Data Base	Marketing plus some IT questions	In person, audio taped	Individual
12. Customer Privacy Manager and Ombudsman	General	Telephone, no tape	Individual
13. Public Affairs Manager	General	Telephone, audio taped	Individual
14. Employee privacy manager and employee advocate	General	In person, audio taped	Individual
15. Vice-President, Credit Risk and Portfolio Management	General	In person, audio taped	Individual
16. Regional Operations Manager	General	In person, audio taped	Individual
17. Retail branch manager	General	Telephone, not taped	Individual

Appendix K-3: Case A - Distribution of Completed Surveys

Survey Version	Received on or before July 30	Received after July 30	Total
4.1	3	2	5
4.2	3	2	5
4.3	1	1	2
4.4	2	2	4
**	9	7	16

Appendix K-4: Case A - Survey Respondent Characteristics

Respondent Characteristics		Received on or before July 30	Received after July 30	Total
Gender:	Male	4	3	7
	Female	5	4	9
Age:	Less than 30	0	0	0
	30 – 39	1	1	2
	40 – 49	7	4	11
	50 – 59	1	2	3
	60 and older			0
Education:	High School	1	1	2
	Some College	2	2	4
	College Diploma	3	0	3
	Some University	1	1	2
	Bachelor degree	1	1	2
	Grad./Prof. degree	1	2	3
	Other			0
Tenure with Firm	Less than 1 year	0	0	0
	1 to 5 years	2	2	4
	6 to 10 years	2	1	3
	More than 10 years	5	4	9
Location within Firm	Head Office	8	7	15
	Regional Office	1	0	1
	Branch Office	0	0	0
	Call Centre	0	0	0
Received Privacy Law training	Yes	4	3	7
	No	5	4	9
	Don't remember	0	0	0
Received Company privacy policy training	Yes	4	3	7
	No	5	4	9
	Don't remember	0	0	0
Privacy as part of Performance appraisal	Yes	1	2	3
	No	7	5	12
	Don't know	1	0	1

Appendix K-5: Case A - Desirable Privacy Documents

Document description	Salience to my research
Consultant or in-house privacy evaluation/ impact assessment/gap analysis	Establishes the starting point for the development of the official privacy program
Privacy Business Case	Outlines the objectives for the program, required financial and human resources required, structure, and likely impacts on operations; location of privacy function (i.e., marketing or customer relationship management, IT, compliance, legal)
Organization chart/Privacy structure, Policy Manuals and other operational materials	Provides insight into the internal control choices (i.e., "diffused" or "islands of competence"); use of committees, champions; role of regional and branch personnel
Training Manuals and other employee materials	Establishes the desired privacy relationship between the front line staff and customers
Privacy Committee agendas and minutes	Identifies issues, priorities, key influencers and overall objectives
Data maps, systems development approaches and operational materials related to the information resource	Defines the information resources and its handling
Drafts of preliminary policies	Illustrates evolution of thinking about customer information privacy in specific firm context
Information privacy maps for business processes	Defines the impact of information privacy on how actual work is carried out
Documents obtained from outside sources	Provides insight into external influencers, the issues raised by them, and the remedies suggested
Risk management/compliance briefings	Illustrates a particular perspective on the view of customers in an important area of the firm
Customer Relationship Management/database marketing information guidelines	Establishes the view of the customer, the use and value of personal information
Privacy "disaster" debriefing reports	Suggests the priority accorded privacy – what happened, what actions were taken, what lessons were learned and what changes were made. Has the incident been repeated.

Appendix K-6: Case A - Frequencies and Means from IPO Survey

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[3]	Means	Means of means	Interpretation
CRSA: Buyer exploitation				
CRS1	75 (1 – 3)	2.69	2.72 = **3**	There was consistent disagreement with statements related to buyer exploitation.
CRS2	68 (1 – 3)	2.94		
CRS3	62.5 (1 – 3)	3.19		
CRS4	93.3 (1 – 3)	2.07		
CRSB: Buyer self-protection				
CRS5	50/50 (1- 3; 5-6)	3.75	4.01= **4**	The responses were "neutral" – neither agreeing nor disagreeing with statements.
CRS6	68.8 (5 – 7)	4.75		
CRS7	33/33/33 (1-3; 4; 5)	3.38		
CRS8	25/44/31 (1 – 3; 4; 5 – 7)	4.19		
CRSC: Shared Responsibility				
CRS9	92 (5 - 7)	6.00	6.12 = **6**	Consistent and strong agreement with statements indicating a mutuality of interest in commercial relationships.
CRS10	81.3 (5 – 7)	5.81		
CRS11	87.5 (6 – 7)	6.06		
CRS12	87.5 (6 – 7)	6.60		
CRSD: Customer well-being				
CRS13	100 (5 – 7)	6.13	5.18 = **5**	Neutral on statements that would "cost" such as engaging in unprofitable activities. Somewhat agree with statements more proactive on customers' behalf.
CRS14	45/55 (1-3; 5 -6)	4.13		
CRS15	50/50 (2 – 4; 5-6)	4.56		
CRS16	93.7 (5 – 7)	5.88		

[3] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5).

Case A: Frequencies and Means from IPO Survey (cont'd)

IMSA: **Manage to reduce information costs**				
IMS1	44/19/37 (1 – 6)	4.00	3.61 = **4**	Largely neutral on statements about the application of customer information for cost management. Customer information plays a role but likely small.
IMS2	56.3 (2 – 3)	3.44		
IMS3	56.3 (1 - 4)	3.56		
IMS4	50.1 (1 – 3)	3.44		
IMSB: **Manage to minimize risks**				
IMS5	81.3 (5 – 7)	5.38	5.30 = **5**	Consistent agreement with statements having to do with the application of customer information for risk management.
IMS6	81.3 (5 – 6)	5.07		
IMS7	68.8 (5 – 7)	5.38		
IMS8	75 (5 – 7)	5.38		
IMSC: **Manage with information to add value**				
IMS9	75.1 (5 – 6)	5.00	5.07 = **5**	Consistent agreement with statements having to do with the application of customer information for adding value to products and services.
IMS10	87.5 (5 - 6)	4.81		
IMS11	75.1 (5 – 7)	5.00		
IMS12	87.6 (5 – 7)	5.50		
IMSD: **Manage with information to create new reality**				
IMS13	68.9 (5 – 7)	4.75	4.44 = **4**	Largely neutral on statements about the application of customer information for creating new reality.
IMS14	56.3 (5 - 6)	4.31		
IMS15	50 (5 – 6)	4.44		
IMS16	62.5 (5 – 6)	4.25		

Case A: Frequencies and Means from IPO Survey (cont'd)

PHILA: **No awareness or concern for privacy**				
PHIL1	100 (1 – 2)	1.13	1.69 = **2**	Consistent awareness that their firm (and industry) is required to operate within the terms of the relevant privacy statute.
PHIL2	100 (1 – 3)	1.38		
PHIL3	68.8 (1 – 3)	3.06		
PHIL4	100 (1 – 3)	1.19		
PHILB: **Privacy as a constraint**				
PHIL5	56.3 (1 – 3)	3.31	4.19 = **4**	Consistent awareness that a privacy program is underway but neutral in assessment of its impact on business function.
PHIL6	68.8 (5 – 7)	4.56		
PHIL7	87.5 (5 – 7)	5.31		
PHIL8	44/25/31 (1 – 6)	3.56		
PHILC: **Privacy as an exchange**				
PHIL9	68.8 (1 – 3)	3.06	3.09 = **3**	Largely in disagreement with statements that would suggest that privacy legislation provides for greater opportunities for securing customer information.
PHIL10	44/25/19 (1 – 6) note: 2 "no opinion"	2.81		
PHIL11	44/31/19 (1 – 6) note: 1 "no opinion"	3.25		
PHIL12	62.5 (1 – 3)	3.25		
PHILD: **Privacy as Opportunity**				
PHIL13	31/31/38 (2 – 6)	4.00	3.50 = **4**	Largely in disagreement with statements suggesting that privacy laws provide any opportunity for the bank. (Note that placement in category due to rounding to 4).
PHIL14	32/25/33 (1 - 3; 4; 5 – 6) note: 1 "no opinion"	3.69		
PHIL15	50.1 (1 – 3) note: 1 "no opinion"	2.94		
PHIL16	44/25/25 (1 – 3; 4; 5 - 6) note: 1 "no opinion"	3.38		

Case A: Frequencies and Means from IPO Survey (cont'd)

BHVA: Non compliant				
BHV1	87.5 (1 – 3)	1.81	2.47 = **2**	Consistently in disagreement with statements that would indicate a lack of privacy action.
BHV2	62.5 (1 – 3)	3.63		
BHV3	62.5 (1 – 3)	2.88		
BHV4	93.8 (1 – 3)	1.56		
BHVB: Minimally compliant				
BHV5	75 (5 – 7)	5.13	4.29 = **4**	Largely neutral in consideration of the extent to which privacy has been incorporated into operations. Stronger agreement that some action is taking place beyond minimum compliance.
BHV6	62.6 (5 – 7)	4.67		
BHV7	62.5 (1 – 3) note: 1 "no opinion"	2.63		
BHV8	56.4 (5 – 7)	4.73		
BHVC: Professional or trade group codes				
BHV9	68.6 (5 – 7)	5.06	5.25 = **5**	There is agreement that the firm is engaged in more than minimal privacy activities that are at least comparable with their competitors.
BHV10	87.6 (5 – 7)	5.31		
BHV11	87.6 (5 – 7)	5.75		
BHV12	75 (5 – 7) note: 1 "no opinion"	4.88		
BHVD: Enhanced privacy				
BHV13	56.3 (1 – 3) note: 2 "no opinion"	2.63	3.52 = **3**	There is consistent disagreement with statements that suggest that the firm is a privacy leader.
BHV14	75.1 (5 – 6)	4.94		
BHV15	56.3 (1 – 3)	3.38		
BHV16	44/13/31 (1 – 3; 4; 5 – 6) note: 2 "no opinion"	3.13		

Appendix L: Case B - Supplementary Information from Case Study Database

This appendix includes information from the Case B case study database as indicated in the following table:

Item Number	Title	Description
L-1	Research Setting	Describes the setting and data collection activities.
L-2	Interviews	Lists the individuals interviewed by position.
L-3	Statistics	Distribution of Completed Surveys
L-4		Survey Respondent Characteristics
L-5	Documents	Lists the documents used for this present research.
L-6		Frequencies and Means from IPO Survey

Appendix L-1: Case B - Research Setting and Site Visit

A regional financial institution in Canada with retail banking as one of its lines of business was recruited for this case study (Case B). This research site was one of the desired sites that was identified in the Privacy Policy Evaluation Study described in Chapter Seven. I was "sponsored" by the President and Chief Executive Officer but negotiated entry with the Senior Manager, Compliance and Audit who is also the firm's Privacy Officer. We agreed on the wording of a Confidentiality and Non-Disclosure agreement (see Appendix XX) and arranged for a 4 day site visit. The Privacy Officer and I exchanged a series of telephone calls and emails in which we discussed the range of potential interview subjects available and agreed upon an approach. The Privacy Officer contacted the interview subjects and arranged the meeting schedule. The company and its staff were very welcoming and provided meeting facilities, a work station and generous access to their privacy documents. The site visit was conducted July 12-15, 2004 at the company's head office complex and at three branch locations.

There are a few aspects of the setting that require comment. This organization is a provincially regulated financial institution. It is subject to the federal privacy legislation only because the provincial legislature failed to pass a "substantially similar" statute[1]. However, the effective date for compliance was January 1, 2004 and not 2001 as this organization is not a "federal work" (i.e., not subject to the federal Bank Act). The Case B site is smaller than any of the national chartered banks in scope, scale and network but is equivalent to one of the country's largest credit unions. Third, the organization had substantively completed the implementation of their privacy program one and half years ahead of the requirement to comply with PIPEDA. As a result, this site had some experience working with the statute. It also provided a contrast to firms that were "playing catch up" as was the case with the pilot site. However, the privacy compliance

[1] The federal statute required that all organizations that were not deemed to be "federal concerns" were to comply with PIPEDA effective January 1, 2004. The exception was for organizations within jurisdictions with private sector protection legislation that was deemed "substantially similar."

effort was sufficiently recent as to be relatively fresh in the memories of the participants and of apparent salience to them.

Data Collection

I collected data from three sources – interviews, a survey and documents.

Interviews: I conducted 14 formal interviews at Head Office and in three branches. Table L-2 identifies the Case B interview subjects, the interview guide administered, and whether or not the interview was audio taped. I also had several additional conversations with the CPO and the Deputy CPO.

I would have preferred to have interviewed more of the top management team. However, the company was very busy with certain strategic initiatives that were placing serious demands on the executive. I am grateful that despite these activities (some of which were unforeseen at the time the research request was agreed to) and summer holiday schedules, the company was generous in offering what staff they could to assist my research. I am convinced that the staff I dealt with offered useful information and that this research did not suffer unduly because of the necessarily (and understandably) restricted access to the TMT.

All interviews were conducted face-to-face and most were audio-taped. (I experienced some technical problems but had extensive handwritten notes as a back up). All interviewees signed consent forms (which formed Schedule A to the Confidentiality and Non-Disclosure Agreement). The Privacy Officer explained the participants' general and privacy specific roles and responsibilities which helped me to match the Interview Guide to the interviewee. The recorded interviews were subsequently transcribed by a third party. I prepared transcripts from my handwritten notes for the interviews that I was unable to record. I provided all individuals with the opportunity to review the transcripts of their interviews.

IPO Survey: While at the Case B site, the Privacy Officer and I reviewed the company organization chart and discussed which personnel would be best positioned to offer insight into

information privacy orientation via the survey. I had prepared 55 "paper and pencil" survey kits (divided among the four versions) in advance of the site visit. (I would have preferred to offer the site an online survey but was unable to complete the necessary testing by the time of this visit). The completion incentive was a $100 donation to a charitable organization supported by the company. We selected a group of 54 individuals including those interviewed as well as several members of the TMT. The company's HR department provided mailing labels and I finalized the kits. The survey kits were prepared as follows.

1. I prepared a cover letter. Consistent with my practice at the pilot site and all other case sites, I promised to donate $100 to a charitable foundation supported by the financial institution, as an incentive for completion of the surveys.
2. I photocopied the different sections of the survey onto different coloured paper. I used this approach as a tactic to make the survey look less intimidating, and to provide me with an easy way to identify the different parts at data entry.
3. I provided a self-addressed postage prepaid envelope. Respondents were instructed to complete the survey and return it in the provided envelope (which ensured return directly to the School of Business).
4. I arranged with the Queens School of Business PhD Program Office to receive the surveys and indicate the date of receipt in order to track early and late respondents.

The surveys were distributed on July 15 and requested to be completed by July 28, 2004. The Privacy Officer sent an email message to all recipients requesting their cooperation in completing and returning the survey directly to Queen's University as soon as possible. At my request, the Privacy Officer issued a follow-up email on August 4, 2004 to solicit additional responses. Table xx summarizes the distribution of the completed surveys.

I received 33 completed surveys, representing a 61% response rate. Appendix L-4 summarizes the respondent characteristics. There was a good distribution of respondents but I discerned no significant differences among respondents by version, date or personal characteristics.

The surveys were analyzed in SPSS for frequencies and basic descriptive statistics (i.e., frequencies, means, standards deviations). The information gleaned from the surveys was used as

part of the triangulation strategy. The interpretation of the results is discussed in the section on applying the IPO Continuum to Case B.

Documents: The firm was very generous in sharing their privacy documents. I collected 67 documents in total. Upon my return from the research site, I reviewed the assembled documents, classified them by type and entered them into a database. I selected a number for specific analysis. Appendix L-5 lists the documents used in the present analysis. Note that the numbering reflects my classification schema and therefore there will appear to be "missing" documents. These are documents not used in the present research.

Appendix L-2: Case B: Interviews

Title/Role	Interview Guide	Comments
1. Vice President, Finance	No guide[2]	Transcription by author from handwritten notes
2. Senior Manager, Compliance & CPO	CPO – Privacy 1	Transcription by author from handwritten notes
3. Compliance & Internal Audit Specialist & Deputy CPO	Privacy Team General	
4. Senior Manager, Central Operations	CIO/IT/Electronic Services	Transcription by author from handwritten notes
5. Senior Manager, HR	Privacy Team General	Transcription by author from handwritten notes
6. Business Analyst – Information Systems	Privacy Team + CRM questions	Transcription by author from handwritten notes
7. Assistant Manager – Personal Lending (Corporate Services & Risk Management)	Privacy Team General	
8. Senior Manager – Wealth Management (Service & Sales) and Wealth Management Coordinator	Privacy Team Expanded	2 staff at once
9. Assistant Manager – Contact Centre	Branch/Contact Centre	
10. Senior Brand Manager	Marketing	
11. Senior Manager – Business Process Innovations	Privacy Team Expanded	
12. Branch 1: Manager	Privacy Team General	
13. Branch 2: Manager	Branch/Contact Centre	
14. Branch 3: Manager	Branch/Contact Centre	

Appendix L-3: Case B - Distribution of Completed Surveys

Survey Version	No. distributed/ % of total	No. returned on or before July 28	No. returned after July 28	Total No. Received	% by version of total received
4.1	14 / 26	7	2	9	27
4.2	14 / 26	8	2	10	30
4.3	13 / 24	5	2	7	21
4.4	13 / 24	5	2	7	21
	54 / 100	25 / 46	8 / 15	33 / 61	Not = 100 due to rounding

Note that there were four survey versions (to minimize order effects). See Chapter Eight for additional information.

[2] I had not expected to be able to interview this individual. However, he was able to provide me with 30 minutes and I conducted the interview "on the fly."

Appendix L-4: Case B - Survey Respondent Characteristics

Respondent Characteristics		Returned on or before July 28	Returned after July 28	Total
Gender:	Male	11	2	13
	Female	14	6	20
Age:	Less than 30	0	0	0
	30 – 39	4	6	10
	40 – 49	14	1	15
	50 – 59	6	1	7
	60 and older	1	0	1
Education:	High School	2	2	4
	Some College	2	2	4
	College Diploma	2	1	3
	Some University	5	0	5
	Bachelor degree	9	3	12
	Grad./Prof. degree	5	0	5
	Other	0	0	0
Tenure with Firm	Less than 1 year	1	1	2
	1 to 5 years	9	2	11
	6 to 10 years	3	2	6
	More than 10 years	10	3	13
Location within Firm	Head Office	11	1	12
	Regional Office	N/A	N/A	N/A
	Branch Office	10	7	17
	Call Centre	0	0	0
Received Privacy Law training	Yes	24	5	29
	No	1	3	4
	Don't remember	20	0	0
Received Company privacy policy training	Yes	23	7	30
	No	2	1	3
	Don't remember	0	0	0
Privacy as part of Performance appraisal	Yes	10	6	16
	No	11	2	13
	Don't know	3	0	3

Note: Not all respondents answered every question.

Appendix L-5: Case B - Privacy Documents

#	Document Title	Explanation/Description
General		
B1.1	Organizational Chart	26 page visual display of head office organization by major function (June 9, 2004)
B1.2	Code of Conduct Policy (A)	8 page excerpt from Policies & Procedures Manual outlining expectations of conduct by employees; includes Privacy and Confidentiality standards (May 1999)
B1.3	Code of Conduct Policy (B)	1 page form signed by employees annually
B1.4	Untitled	1 page excerpt from Annual report outlining Vision, Mission, Commitment
Privacy Process (Internal)		
B2.1	Project Charter	12 page Business Case prepared for senior management approval (May 29, 2001)
B2.2	Post Implementation Review	5 page Review of the process used to implement the Money Laundering and Privacy Project
Privacy Policy & Procedure (Internal)		
B3.1	Our Commitment to Protecting Your Personal Information	8 panel full colour brochure explaining company's approach to privacy protection (includes consent and limiting consent form)
B3.2	Our Commitment to Protecting Your Personal Information	Advertisement in local newspaper
B3.3	General Information – Privacy	3 pages printed from company intranet – information for staff (June 2004)
B3.4	What's New: Privacy - Our Commitment to Protecting Your Personal Information	4 pages printed from company website (downloaded 14 July 2004 by Deputy CPO)
B3.15	New Policy – Providing/ Obtaining Information Over the Phone – Effective Immediately	Memo to Branch Managers (July 12, 2002)
B3.16	Re: A customer company that is downsizing	Email correspondence regarding marketing services to laid off/ terminated employees who are customers (September 27, 2002)
B3.17	Changes to the IVR at the Call Centre	2 page memo describing Script changes made to IVR at Call Centre
B3.18	Re: Question	Email correspondence regarding pulling customer information for branch marketing purposes (December 23, 2002)
B3.19	Re: Question	Email correspondence regarding pulling customer information for branch marketing purposes (January 27, 2003)
Privacy External – FI Industry		
B4.1	FI Industry Association Code for the Protection of Personal Information: Model Privacy Package	18 page overview and explanation of the Code (January 2003)
B4.2	Model Privacy Package – Privacy Implementation Plan	12 page overview of implementing privacy code (June 2002)
B4.3	Model Privacy Package – Board Resolution and Privacy Policies	18 page overview and explanation of Board obligations for code implementation (June 2002)
B4.4	Model Privacy Package – Privacy Officer, Senior Management and Staff training Plan	15 page guide to training requirements (February 2003)
B4.5	Model Privacy Package –	9 page guide to communicating privacy code to customers

	Communication Kit (vers. 1.0)	(June 2002)
B4.7	Privacy Officer Responsibilities	11 page memo outlining the responsibilities of a Privacy Officer under the Act (May 2001)
Privacy External – Government		
B5.2	Your Privacy Responsibilities – Canada's Personal Information Protection and Electronic Documents Act – A guide for Businesses and Organizations	30 page explanation of PIPEDA from business implementation perspective from Office of the Privacy Commissioner of Canada (December 2000)
B5.3	The Security-Privacy Paradox: Issues, Misconceptions, and Strategies	19 page joint report by the Information and Privacy Commissioner/Ontario and Deloitte and Touche (August 2003)

Appendix L-6: Case B - Frequencies and Means from IPO Survey

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[3]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
CRSA: Buyer exploitation						
CRS1	78(1 – 3)	32/1		2.28	2.23	There was consistent disagreement with statements related to buyer exploitation.
CRS2	82 (1 – 3)	32/1		2.50		
CRS3	68.8 (1 – 3)	32/1		2.47		
CRS4	93.8 (1 – 3)	32/1		1.66		
CRSB: Buyer self-protection						
CRS5	65.7 (1- 3)	32/1	1	3.09	3.52	Largely in disagreement with statements suggesting that their customers must look after their own interests without support from the bank
CRS6	33/1048 (1 – 3; 4; 5 – 7)	32/1	2	4.22		
CRS7	75 (1-3)	32/1		2.88		
CRS8	36;15;45 (1 – 3; 4; 5 – 7)	32/1		3.88		
CRSC: Shared Responsibility						
CRS9	87.9 (5 – 7)	32/1		6.00	5.99	Consistent and strong agreement with statements indicating a mutuality of interest in commercial relationships.
CRS10	78.8 (5 – 7)	32/1		5.94		
CRS11	60.6 (5 – 7)	32/1		5.59		
CRS12	84.8 (5 – 7)	32/1		6.25		
CRSD: Customer well-being						
CRS13	87.8 (5 – 7)	32/1		6.22	5.34	Slightly less in agreement with statements that would "cost" such as engaging in unprofitable activities. Somewhat more in agreement with statements suggesting more proactive on customers' behalf.
CRS14	66.7 (5 – 7)	32/1	2	4.56		
CRS15	60.6 (5 – 7)	32/1		4.94		
CRS16	78.8 (5 – 7)	32/1		5.66		

[3] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix L-6: Case B - Frequencies and Means from IPO Survey (cont'd)

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[4]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
IMSA: Manage to reduce information costs						
IMS1	54.5 (1 – 3)	33	3	3.15	3.03	Consistent disagreement with statements having to do with the application of customer information for cost reduction.
IMS2	57.6 (1 – 3)	33	1	2.97		
IMS3	51.6 (1 – 3)	33	3	2.94		
IMS4	40;30;21 (1 – 3; 4; 5 – 6)	33	3	3.06		
IMSB: Manage to minimize risks						
IMS5	57.6 (5 – 7)	32 / 1	4	4.06	4.54	Consistent agreement with statements having to do with the application of customer information for risk management.
IMS6	51.4 (5 – 7)	33	3	4.00		
IMS7	78.8 (5 – 7)	33		5.03		
IMS8	72.7 (5 – 7)	33		5.06		
IMSC: Manage with information to add value						
IMS9	69.7 (5 – 7)	33	3	4.58	5.07	Consistent agreement with statements having to do with the application of customer information for adding value to products and services.
IMS10	81.9 (5 – 7)	33	1	5.15		
IMS11	87.9 (5 – 7)	33	1	5.45		
IMS12	69.7 (5 – 7)	32 / 1		5.09		
IMSD: Manage with information to create new reality						
IMS13	57.5 (5 – 7)	33	4	4.06	4.22	Largely neutral on statements about the application of customer information for creating new reality.
IMS14	60.6 (5 – 7)	33	2	4.42		
IMS15	60.6 (5 – 7)	33	1	4.58		
IMS16	27;12;45 1 – 3; 4; 5 – 7)	33	5	3.82		

[4] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix L-6: Case B - Frequencies and Means from IPO Survey (cont'd)

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[5]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
PHILA: No awareness or concern for privacy						
PHIL1	93.9 (1)	33		1.3	1.67	Consistent awareness that their firm (and industry) is required to operate within the terms of the relevant privacy statute.
PHIL2	87.9 (1 – 3)	33		1.58		
PHIL3	78.8 (1 – 3)	33		2.42		
PHIL4	93.9 (1 – 2)	33		1.36		
PHILB: Privacy as a constraint						
PHIL5	93.9 (1 – 3)	33		1.7	2.95	Consistent awareness that a privacy program is underway but disagreement with a negative assessment of its impact on business function.
PHIL6	24;30;43 (1 – 3; 4; 5 – 7)	33		4.12		
PHIL7	40;10;45 (1 – 3; 4; 5 – 7)	33		3.55		
PHIL8	63.6 (1 – 3)	33		2.42		
PHILC: Privacy as an exchange						
PHIL9	81.8 (1 – 3)	33	3	1.61	2.66	Largely in disagreement with statements that would suggest that privacy legislation provides for greater opportunities for securing customer information.
PHIL10	40;36;12 (1 – 3; 4; 5 – 6)	33	4	2.79		
PHIL11	39;30;12 (1 – 3; 4; 5 – 6)	33	2	3.24		
PHIL12	45;24;21 (1 – 3; 4; 5 – 7)	33	3	3.00		
PHILD: PRIVACY as opportunity						
PHIL13	33;36;27 (1 – 3; 4; 5 – 7)	33	1	3.64	3.96	Largely in disagreement with statements suggesting that privacy laws provide any opportunity for the bank.

[5] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix L-6: Case B - Frequencies and Means from IPO Survey (cont'd)

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[6]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
BHVA: Non compliant						
BHV1	87.9 (1 – 2)	33		1.73	1.88	Consistently in disagreement with statements that would indicate a lack of privacy action.
BHV2	81.8 (1 – 3)	33	2	1.97		
BHV3	78.1 (1 – 3)	32 / 1		2.44		
BHV4	97 (1 – 3)	33		1.39		
BHVB: Minimally compliant						
BHV5	42;12;42 (1 – 3; 4; 5 – 7)	33	1	3.7	3.5	Largely neutral in consideration of the extent to which privacy has been incorporated into operations. Stronger agreement that efforts go beyond the minimum.
BHV6	30;15;48 (1 – 3; 4; 5 – 7)	33	1	4.06		
BHV7	81.8 (1 – 3)	33	2	2.58		
BHV8	30;15;48 (1 – 3; 4; 5 – 7)	33	2	3.76		
BHVC: Professional or trade group codes						
BHV9	69.7 (5 – 7)	33	5	4.73	5.13	There is agreement that the firm is engaged in more than minimal privacy activities that are at least comparable with their competitors.
BHV10	75.8 (5 – 7)	33		4.94		
BHV11	90.9 (5 – 7)	33		5.88		
BHV12	75.8 (5 – 7)	33	3	4.97		
BHVD: Enhanced privacy						
BHV13	27;24;33 (1 – 3; 4; 5 – 7)	33	2	3.55	4.22	Largely neutral on the issue of whether the firm is a privacy leader.
BHV14	60.6 (5 – 7)	33		4.7		
BHV15	18;27;45 (1 – 3; 4; 5 – 7)	33	2	4.12		
BHV16	78.9 (5 – 7)	33	3	4.52		

[6] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix M: Case C - Supplementary Information from Case Study Database

This appendix includes information from the Case C case study database as indicated in the following table:

Item Number	Title	Description
M-1	Research Setting	Describes the setting and data collection activities.
M-2	Interviews	Lists the individuals interviewed by position.
M-4	Documents	Lists the documents used for this present research.

Appendix M-1: Case C - Research Setting and Site Visit

Case C is a regional financial institution (FI) in Canada with retail banking as one of its lines of business. This FI is a very well established and strong competitor in its territory and is recognized as a financial services leader in Canada. There is some debate over whether the bank was to be PIPEDA compliant effective January 2001 or 2004. The bank sought external legal advice and determined that they should be complaint "sooner than later." They announced a basic privacy policy to meet the 2001 requirement and then initiated a comprehensive project to develop and implement the bank's privacy policy. The bank considered itself fully PIPEDA compliant by January 2003.

I had previously researched this firm (and was personally familiar with their reputation as a leader among Canadian FIs). I wrote to the Chief Privacy Officer (of record) and included the standard information package. I was contacted by the person with day to day responsibility for managing privacy compliance (the Privacy Specialist) and we began a series of telephone and email conversations that eventually lead to their agreement to participate. The Privacy Specialist and I set the date for the site visit for July 18-22, 2004.

As I had done with previous visits, I provided the company with the Confidentiality and Non-Disclosure Agreement (exactly as the one used for the previous sites) and the Privacy Specialist and I discussed the types of personnel I wanted to interview and the documents I wanted to review. All the site arrangements were made by the Privacy Specialist. As with previous research site visits, the staff at Case C were very welcoming and seemed very sincere and thoughtful in sharing with me their opinions and experience with information privacy at their company.

In general, I conducted interviews, collected documents and posed questions to the Privacy Specialist throughout the days at the site location. In the evenings, I skimmed and sorted documents and entered them into the database. I did "quick and dirty" transcriptions from my

handwritten notes for the interviews I was unable to audiotape. I also tried to maintain a diary of activities.

Interviews: I conducted 16 formal interviews with 20 staff at Head Office and in three branches. I also had several additional conversations with the Privacy Specialist. I would have preferred to have interviewed more of the top management team. However, I am grateful that despite summer holiday schedules, the company was generous in offering what staff they could to assist my research. I am convinced that the staff I dealt with provided a broad perspective and offered useful information.

All interviews were conducted face-to-face and most were audio-taped. (I experienced some technical problems but had extensive handwritten notes as a back up). All interviewees signed consent forms (which were attached to the Confidentiality and Non-Disclosure Agreement as Schedule A). The Privacy Specialist helpfully explained the participants' general and privacy specific roles and responsibilities which helped me to try to match the guide to the interviewee. Appendix M-2 identifies the interview subjects and the related interview guides.

The recorded interviews were subsequently transcribed by a third party. I prepared transcripts from my handwritten notes for the interviews that I was unable to record. I was unable to arrange for the transcripts to be reviewed. However, I am confident that I have successfully captured the conversations given the extensive notes that I made as well as having the tapes.

Documents: Case C was also very generous with providing me access to the company's information privacy documentation. I collected 76 documents ranging from an organization chart to the Project Charter and Close Out Report, as well as training materials, policies and procedures amendments and internal audit reports. I sorted and catalogued the documents into 6 categories as indicated in M-3. Note that some titles have been disguised.

Upon my return from the research site, I reviewed the assembled documents. I selected a number for specific analysis.

Surveys: Prior to the site visit, the Privacy Specialist and I had discussed the best approach to take with respect to the IPO survey. We agreed to use the online version as she was of the opinion that the online version would be more appealing to staff and, hence, increase the likelihood and rate of participation. However, we did not agree upon the actual participants as I needed more time to digest the company's organization structure and privacy governance model. These decisions delayed the survey rollout to Case C personnel. However, we agreed that once I was in a position to launch the web version, she would advise the selected personnel. On my return from the research visit, I reviewed the company organization chart and various other documents and advised the company of my preferences for the survey. The completion incentive was a $100 donation to a charitable organization supported by the company. At the same time, I engaged with the Unix programmer and we were able to mount the four different versions of the survey. However, we were unable to obtain consent to mount the online version because of other corporate initiatives. I then attempted to have the "paper and pencil" version circulated to the interview participants but there were additional difficulties. AS a result, Case C did not participate in the IPO Survey.

Summary: I conducted the research site visit for Case C in July 2004. I interviewed 14 executives, managers and senior staff about how the company had gone about organizing and implementing their customer information privacy program. I also collected more than 65 documents related to privacy. I was unable to engage Case C's participation in the IPO Survey.

Appendix M-2: Case C - Interviews

Title/Role		Interview Guide	Comments
1.	VP, Products & Services and Privacy Officer (Marketing & Planning)	Privacy Team General	Transcribed by author from handwritten notes
2.	Privacy Specialist (Marketing & Planning)	Privacy Team Expanded/Privacy II	Transcribed by author from handwritten notes
3.	Manager, Interactive Services (Marketing & Planning)	CIO/IT/Electronic Services	Transcribed by author from handwritten notes
4.	DataBase Analyst (Marketing & Planning)	Marketing	
5.	Senior Procedures Analyst	Privacy Team General	
6.	Operations Officer (Sales& Services)	Privacy Team General	
7.	Security Specialist – IT subsidiary	CIO/IT/Electronic Services	
8.	Privacy Specialist – subsidiary	Privacy (I)	Previously with parent company in privacy role
9.	Call Centre Manager - subsidiary	Branch/Contact Centre	
10.	Lender, Call Centre – parent company	Branch/Contact Centre	
11.	Director, Wealth Management Compliance	Privacy Team General	
12.	Branch 1: Manager	Branch/Contact Centre	
13.	Branch1: Account Manager Branch1: Financial Services Representative	Branch/Contact Centre	2 staff at once
14.	Branch 2: Account Manager	Branch/Contact Centre	
15.	Branch 2: Financial Services Manager Branch 2: Financial Services Representative	Branch/Contact Centre	2 staff at once
16.	Branch 3: Customer Services Manager Branch 3: Account Manager Branch 3: Financial Services Representative	Branch/Contact Centre	3 staff at once

Appendix M-3: Case C - Documents

#	Document Title	Explanation/Description
Documents: General		
C1.1	Organizational Chart	1 page overview of organization (July 9, 2004)
C1.2	Baseline Ethical Policy	6 panel brochure summarizing Statement of Values and Commitments; available in branches (02/04)
C1.3	Statement of Values and Commitments – staff copy	2 page explanation of values and commitments based on theme of integrity, innovation, responsibility (2000)
C1.4	Statement of Values and Commitments	4 panel brochure summarizing mission, purpose, values and commitments; available in branches (02/04)
Privacy Process (Internal)		
C2.1	VanCity Privacy Project Assessment & Recommendations	37 page PPT (handout) explaining status of privacy project including assessment of state of readiness against 10 privacy principles (undated)
C2.2	Privacy Information Management Project (PIM) Phase II	3 page overview of the development of privacy project "enablers" (undated)
C2.3	Privacy Information Management Project – Project Charter	24 page detailed description of the process to implement Phase II of the project; includes subsequent amendments to scope (March 2002)
C2.4	Privacy Information Management Project Presentation to Branch Managers	2 page memo with agenda and issues analysis (March 8, 2002)
C2.10	Privacy Information Management Project Presentation to Privacy Team	4 page memo with agenda, privacy principles and compliance approach (May 15, 2002)
C2.11	Privacy Information Management Project Privacy Team Kickoff Meeting	4 page PPT (handout) providing overview for first meeting of privacy team (May 15, 2002)
C2.12	Privacy Information Management Project Department Feedback – Stage One – Where are we now?	11 page handout requiring departmental representatives to complete an inventory against the 10 privacy principles
C2.15	Privacy Information Project – Training Update	1 page memo to Branch Managers and Head Office Managers outlining staff training requirements and registration (09/17/2002)
C2.16	Privacy Information Project – Marketing and Planning Division Update	2 page memo (includes copy of Privacy Statement) provides overview of rationale for the privacy project (October 31, 2002)
C2.17	Privacy Policy Workshop Kit	Kit Contents: • The 10 Principles of the Federal Privacy Act • Customer Privacy Code • Formal Customer Request for Information Form • Customer Privacy Statement • Customer Policies and Procedures – ONLINE • Staff as Customers • Privacy Commissioner Case Study • Sample Scripts – Privacy Situations • Employee Privacy Code • Formal Employee Request for Information Form

		• Employee Policies and Procedures – ONLINE • Privacy Policy Support Documents o Credit Assessment FAQ o Your Personal Information o Privacy Choices – Opt-Out Request Form o Third Party Organizations o Commonly Used Abbreviations
C2.18	Protecting Your Privacy	2 page memo to Branch Management and National Call Centre Management advising of customer communication initiatives and providing question and answer assistance (12/18/2002)
C2.22	Personal Information and Management Project 2002 Project Compliance Summary to PIPED Act (Bill C-6)	10 page project closeout report (Undated)
C2.23	Recap of Mystery Shopping Surveys Privacy Policy - January 2003	4 page report of test of employee responses to general customer inquiries relating to the Privacy Code (January 2003)
C2.24	Evaluation Brief – Privacy Implementation	1 page request for budget for follow-up research on implementation of privacy policy (12 August 2003)
C2.25	Privacy Compliance Regime Detailed Internal Audit Report with Joint Response from CPO and Employee Privacy Officer	19 page internal audit report detailing compliance with PIPEDA (Reported February 2004; final version April 5, 2004)
C2.26	Appendix 4.0 VanCity 2004 Privacy Audit Action Plan	1 page chart of findings, actions and responsibilities resulting from internal audit report
C2.27	Response to Audit Finding #8 (version 2.0)	3 page draft of policy concerning privacy breaches (09/07/2004)
C2.28	VanCity Privacy Governance Framework (version 7.0)	33 page report to Executive Committee recommending the governance structure for privacy compliance (June 30, 2004)
C2.29	Summary Document – amendment to VanCity Privacy Governance Framework (version 7.0)	3 page summary of Executive Committee decision with respect to the privacy governance framework (07/07/2004)
Privacy Policy & Procedure (Internal)		
C3.1	Privacy at a Glance	1 page visual description of privacy processes (undated)
C3.2	Protecting your Privacy	8 panel brochure explaining privacy approach including the Privacy Statement; available in branches (12/02)
C3.4	Privacy Choices – Opt-Out Request Form	1 page Opt-out form (undated)
C3.5	Formal Privacy Request	1 page form for customers to use to request information about themselves (undated)
C3.6	Third Party Organizations	2 page information sheet explains the types of third party organizations the bank deals with and the types of personal information that may be collected and used (undated)
C3.7	Commonly Used Abbreviations	4 page information sheet explains the variety of

		acronyms used by the bank (undated)
C3.9	Your Personal Information	1 page information sheet explains what information is collected and its use (undated)
C3.10	Privacy Policy – Privacy Statement	1 page information sheet explains why information is collected and how it is protected
C3.11	Privacy Code	4 page information sheet providing an overview of the bank's privacy process according to the 10 privacy principles
C3.12	Procedures for the Privacy Administrator: Process a formal Privacy Request	6 page document outlining the steps for investigating and fulfilling a request for information (undated)
C3.13	Flow chart for formal privacy request process	1 page visual document of the steps for investigating and fulfilling a request for information (undated)
C3.14	Policy and Procedure Policy A: Accountability – Roles and Responsibilities	4 page excerpt from policies and procedures manual (January 2, 2003)
C3.15	Policy and Procedure Policy B: Customer Contact Procedures	5 page excerpt from policies and procedures manual; (January 2, 2003)
C3.16	Policy and Procedure Policy C: General Information on VanCity's Privacy Policy	2 page excerpt from policies and procedures manual; (January 2, 2003)
C3.17	Policy and Procedure Policy D: Changing Personal Information	3 page excerpt from policies and procedures manual; (January 2, 2003)
C3.18	Policy and Procedure Policy E: Formal Privacy Requests	4 page excerpt from policies and procedures manual; (January 2, 2003)
Privacy External – FI Industry		
C4.1	Personal Information Protection Act	6 page letter from external legal counsel outlining legal issues related to compliance to PIPEDA (December 20, 2000)
C4.2	Personal Information Protection and Electronic Documents Act	13 page legal report from external legal counsel outlining legal issues related to compliance to PIPEDA (February 2001)
C4.3	Privacy Project – Clarification Issues	7 page letter from external legal counsel addressing specific issues raised by Privacy Specialist (September 13, 2002)
C4.4	Is Orwell Your Banker?	1 page article (undated; source unknown) circulated to Privacy Team members at "kickoff" meeting on May 15, 2002
Privacy External – Other		
C6.1	Making the CSA Privacy Code Work for You – Stage 6: Periodic review and auditing	5 page overview of process for compliance verification; source unknown (December 1996)
C6.2	Canada's Privacy Legislation – What it means for your organization (The Canadian Institute of Chartered Accountants)	6 panel pamphlet overview of the Act and compliance issues; introduces CICA and AICPA Enterprise-Wide Privacy task Force (Undated)
C6.3	Privacy Compliance – A Guide for Organizations & Assurance Practitioners (The Canadian Institute of Chartered Accountants)	71 page comprehensive guide to privacy as a compliance issue for both companies needing to comply and accounting firms wanting to provide privacy assurance services (February 2002)
C6.4	Regulatory Compliance: Adding Value (PricewaterhouseCoopers)	41 page general guide to compliance / corporate governance activities (Undated)

C6.5	2003 Benchmark Study Corporate Privacy Practices (iapp and Ponemon Institute)	13 page survey questionnaire of privacy practices (copy was completed by Privacy Specialist) (2003)
C6.6	Privacy: Beyond Compliance – Responsible Information Stewardship (Peppers & Rogers Group)	11 page "white paper" addresses inadequacy of "risk management" approach and arguing for "intelligent and responsible use of relevant data"
C6.8	Inside 1 to 1 Privacy: The Value Proposition of Privacy (Larry Ponemon)	2 page email letter discusses how to establish the value of privacy programs (August 12, 2003)
C6.9	Inside 1 to 1 Privacy: The Practice of Trust (Susan Jayson)	2 page email letter discusses trust as a way to achieve profitable privacy (August 12, 2003)
C6.11	New Guidelines Match Privacy with CRM (Marji McClure)	1 page email letter discusses PIPEDA and marketing (June 10, 2004)

Appendix N: Case D - Supplementary Information from Case Study Database

This appendix includes information from the Case A case study database as indicated in the following table:

Item Number	Title	Description
N-1	Research Setting	Describes the setting and data collection activities.
N-2	Interviews	Lists the individuals interviewed by position.
N-3	Statistics	Survey Respondent Characteristics
N-4	Documents	Lists the documents used for this present research.
N-5	Survey	Frequencies and Means from IPO Survey

Appendix N-1: Case D - Research Setting and Site Visit

Case D is a national financial institution (FI) in Canada with retail banking as one of its lines of business. This FI is a very well established and strong competitor in Canada. The company was subject to the federal privacy legislation (PIPEDA) effective January 1, 2001 given its status as a nationally chartered bank subject to the federal Bank Act. I had previously met their Chief Privacy Officer at a presentation about the bank's approach to complying with PIPEDA and had discussed the possibility of the bank serving as a case site. I wrote to this individual a few months later and included the standard information package described in Appendix I. The CPO replied and after an exchange of emails and telephone calls, I secured the company's agreement to participate. I was contacted by an individual from the company's privacy office with day to day responsibility for managing privacy compliance (the Privacy Manager) and set the date for the site visit for August 16-20, 2004.

As I had done with previous visits, I provided the company with the Confidentiality and Non-Disclosure Agreement (exactly as the one used for the previous sites) and the Privacy Manager and I discussed the types of personnel I wanted to interview and the documents I wanted to review. The Privacy Manager made all the site arrangements. As with previous research site visits, the staff at Case D were very welcoming and seemed very sincere and thoughtful in sharing with me their opinions and experience with information privacy at their company.

In general, I conducted interviews, collected documents and posed questions to the Privacy manager and other Privacy staff throughout the days at the site location. In the evenings, I skimmed and sorted documents and entered them into the database. I did "quick and dirty" transcriptions from my handwritten notes for the interviews I was unable to audiotape. I also tried to maintain a diary of activities.

Interviews: I conducted 16 formal interviews with 20 staff at Head Office and in three branches. I also had several additional conversations with the Privacy Manager. I would have preferred to have interviewed more of the top management team. However, I am grateful that

despite summer holiday schedules, the company was generous in offering what staff they could to assist my research. I am convinced that the staff I dealt with provided a broad perspective and offered useful information.

Most interviews were conducted face-to-face (some were by telephone) and most were audio-taped. (I experienced some technical problems but had extensive handwritten notes as a back up). All interviewees signed consent forms (which were attached to the Confidentiality and Non-Disclosure Agreement as Schedule A). The Privacy Manager helpfully explained the participants' general and privacy specific roles and responsibilities which helped me to try to match the guide to the interviewee. Appendix N-2 identifies the interview subjects and the related interview guides. The recorded interviews were subsequently transcribed by a third party. I prepared transcripts from my handwritten notes for the interviews that I was unable to record. I provided all individuals with the opportunity to review the transcripts of their interviews.

IPO Survey: While at the Case D site, the Privacy Officer and I reviewed the company organization chart and discussed which personnel would be best positioned to offer insight into information privacy orientation via the survey. Case D opted for the web-based version of the survey. The completion incentive was a $100 donation to a charitable organization supported by the company. The Privacy Manager invited , by email, 50 personnel to respond to the survey, specifically to respond between Aug.27 – Sept. 15, 2004. At my request, the Privacy Officer issued a follow-up email on September 10, 2004 to solicit additional responses. I received 17 completed surveys, representing a 34% response rate. Appendix N-4 summarizes the respondent characteristics. There was a good distribution of respondents but I discerned no significant differences among respondents by version, date or personal characteristics.

The surveys were analyzed in SPSS for frequencies and basic descriptive statistics (i.e., frequencies, means, standards deviations). The information gleaned from the surveys was used as part of the triangulation strategy. The interpretation of the results is discussed in the section on applying the IPO Continuum to Case D in Chapter Eleven.

Documents: The firm was reluctant to share too many documents that they considered "proprietary". However, I was able to review several policy documents and make notes. Upon my return from the research site, I reviewed the documents and notes, classified them by type and entered them into a database. I selected a number for specific analysis. Appendix N-5 lists the documents used in the present analysis. Note that the numbering reflects my classification schema and therefore there will appear to be "missing" documents. These are documents not used in the present research.

Appendix N-2: Case D - Interviews

Title/Role	Interview Guide
1. Chief Privacy Officer (Canada and U.S.)	CPO
2. Privacy Officer, U.S.	Privacy Practitioner
3. Director, Information Management Initiative	IT/CII/Security/Tech Solutions
4. Legal, U.S. Subsidiary	Privacy Team General
5. Business Consultant, IT Account Management (Retail Banking)	IT/CII/Security/Tech Solutions
6. Director, Compliance Private Banking	Audit/Risk/Governance/Compliance
7. Executive Resource	IT/CII/Security/Tech Solutions
8. VP, Corporate Communications	Privacy Team expanded
9. Assistant Chief Auditor (Corporate)	Audit/Risk/Governance/Compliance
10. Senior VP, Technology Solutions	IT/CII/Security/Tech Solutions
11. VP, Information Security	IT/CII/Security/Tech Solutions
12. Director, Privacy Office (Canada)	Privacy Practitioner
13. Legal (with Privacy responsibility) (Can)	Privacy Team expanded
14. Senior Manager, Compliance (Retail Banking)	Audit/Risk/Governance/Compliance
15. Privacy Manager, Canada	Privacy Practitioner
16. Privacy Manager, Canada	Privacy Practitioner

Appendix N-3: Case D - Survey Respondent Characteristics

Respondent Characteristics		
Gender:	Male	7
	Female	9
Age:	Less than 30	1
	30 – 39	5
	40 – 49	6
	50 – 59	7
	60 and older	
Education:	High School	0
	Some College	0
	College Diploma	2
	Some University	1
	Bachelor degree	6
	Grad./Prof. degree	7
	Other	0
Tenure with Firm	Less than 1 year	0
	1 to 5 years	5
	6 to 10 years	5
	More than 10 years	6
Location within Firm	Head Office	14
	Regional Office	2
	Branch Office	0
	Call Centre	0
Received Privacy Law training	Yes	13
	No	3
	Don't remember	0
Received Company privacy policy training	Yes	13
	No	3
	Don't remember	0
Privacy as part of Performance appraisal	Yes	8
	No	8
	Don't know	0

Note: Not all respondents answered every question.

Appendix N-4: Case D: Privacy Documents

#	Document Title	Explanation/Description
General		
D1.1	Welcome	8 panel brochure with overview of organization (5701456; 09/02)
Privacy Process (Internal)		
D2.1	Message to Colleagues from CPO on Privacy – Your Rights and Obligations	Corporate Communication to employees advising of further obligations effective Jan 1/04 (with respect to provincially regulated entities) (10 February 2004)
D2.2	Privacy Policy for provincially regulated entities takes effect January 1, 2004	1 page communication to Private Client Division staff re: now having to comply with PIPEDA (with respect to provincially regulated entities)
D2.3	Your Privacy	Privacy Code (from website)
D2.5	What is Personal Information	Detailed explanation of what constitutes personal information and how it is used by the bank (from website)
D2.6	Managing a Privacy Breach: A case study	PPT presentation of learning from a privacy breach (April 29, 2004)
D2.7		PPT presentation by CPO to external IT management group (date)
Documents reviewed on site related to internal process		
D3.1	Corporate Policy: Privacy	Explains purpose, philosophy, fundamental premise, motivations, risks, governance re: privacy policy
D3.2	Corporate Policy: Customer Information	Addresses purposes for collecting customer information, ownership, quality issues and compliance
D3.3	Corporate Policy: Operational Risk Management	Addresses different kinds of operational risk (obliquely includes privacy) including definition of reputation and reputational risk
D3.4	Corporate Policy: Information Management	Addresses reasons for an information management policy, value of information, information management principles, defines information and the information resource and lists requirements for the IM policy to take effect
D3.5	Corporate Policy: Information Security	Overviews key aspects of Security Policy Note that VP Information Security has made some public presentations – will download from net
D3.6	Corporate Policy: Code of Business Conduct and Ethics	Addresses key aspects of ethical business conduct
D3.7	Privacy Governance Charter	Overview of privacy structure
D3.8	Privacy Governance – Responsibility and Accountabilities	Detailed presentation about accountabilities and responsibilities for privacy across the enterprise
D3.9	Privacy online training module	Screen shots of basic training
D3.10	Privacy Operational Procedures	Detailed explanation of handling privacy issues at frontline
D3.11	Privacy Circular re: Jan 2001 PIPEDA compliance	Explanation of basic legal compliance issues; included information about Privacy Code 1998 (voluntary compliance with CBA Model Code which was based on 1996 CSA Model Code)
D3.12	Privacy Risk Assessment	Study prepared by Privacy Office of how privacy issues represent risks in different areas – sorted by high, medium, low; shows privacy as overwhelmingly an operational risk matter, especially reputational risk but acknowledges as well importance of customer information (accuracy, etc.)

Appendix N-5: Case D - Frequencies and Means from IPO Survey

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[1]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
CRSA: Buyer exploitation						
CRS1	81.3 (1-3)	16		2.44	2.3	Strong disagreement with statements indicating a willingness to exploit customers.
CRS2	68.8 (1-3)	16		2.88		
CRS3	86.7 (1-3)	15/1		2.13		
CRS4	100 (1-3)	16		1.56		
CRSB: Buyer self-protection						
CRS5	31;13;56 (1-3;4;6)	16		4.5	4.3	Neutral position on buyer self-protection (likely reflects a concern for contracts)
CRS6	56.3 (5-6)	16		4.25		
CRS7	56.3 (1-3)	16		3.56		
CRS8	75 (5-7)	16		5.06		
CRSC: Shared Responsibility						
CRS9	100 (6-7)	16		6.44	6.3	Consistent and strong agreement with statements indicating a mutuality of interest in commercial relationships.
CRS10	93.8 (5-7)	16		6		
CRS11	93.8 (5-7)	16		6.13		
CRS12	100 (5-7)	16		6.44		
CRSD: Customer well-being						
CRS13	87.6 (5-7)	16		5.81	4.7	Largely neutral to statements about customer well-being. Slightly less in agreement with statements that would "cost" such as engaging in unprofitable activities. Somewhat more in agreement with statements suggesting more proactive on customers' behalf.
CRS14	62.5 (1-3)	16		3.69		
CRS15	56.4 (5-7)	16	1	4.25		
CRS16	75 (5-7)	16		5		

[1] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix N-5: Case D - Frequencies and Means from IPO Survey (cont'd)

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[2]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
IMSA: Manage to reduce information costs						
IMS1	44;6;44 (1-2;4;5,7)	16	1	3.5	3.5	Consistent disagreement with statements having to do with the application of customer information for cost reduction.
IMS2	56.3 (1-2)	16		3.13		
IMS3	50 (1-3)	16		3.81		
IMS4	56.3 (1-3)	16		3.56		
IMSB: Manage to minimize risks						
IMS5	75 (5-7)	16		5	4.78	Apparent neutrality to slight agreement with statements about the use of customer information for managing risk.
IMS6	86.3 (5-6)	16		4.25		
IMS7	68.9 (5-7)	16	1	4.81		
IMS8	75 (5-7)	16	1	5.06		
IMSC: Manage with information to add value						
IMS9	81.3 (5-7)	16		5.44	5.1	Consistent agreement with statements having to do with the application of customer information for adding value to products and services.
IMS10	56.4 (5-7)	16	1	4.31		
IMS11	81.3 (5-7)	15/1		5.67		
IMS12	75 (5-7)	16	1	4.88		
IMSD: Manage with information to create new reality						
IMS13	87.5 (5-7)	16		5.44	4.9	Largely neutral on statements about the application of customer information for creating new reality.
IMS14	56.3 (5-7)	16	1	4.5		
IMS15	75 (5-7)	16		5.13		
IMS16	68.8 (5-7)	16		4.63		

[2] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix N-5: Case D - Frequencies and Means from IPO Survey (cont'd)

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[3]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
PHILA: No awareness or concern for privacy						
PHIL1	100 (1-3)	16		1.31	1.33	Consistent awareness that their firm (and industry) is required to operate within the terms of the relevant privacy statute.
PHIL2	100 (1-3)	16		1.19		
PHIL3	93.8 (1-3)	16		1.69		
PHIL4	100 (1-3)	16		1.13		
PHILB: Privacy as a constraint						
PHIL5	87.5 (1-3)	16		2.06	2.51	Consistent awareness that a privacy program is underway but disagreement with a negative assessment of its impact on business function.
PHIL6	56.4 (1-3)	16	2	2.88		
PHIL7	66.7 (1-3)	15/1		3.27		
PHIL8	81.3 (1-3)	16	1	1.94		
PHILC: Privacy as an exchange						
PHIL9	75(1-2)	15/1	1	1.87	2.95	Largely in disagreement with statements that would suggest that privacy legislation provides for greater opportunities for securing customer information.
PHIL10	50 (1-3)	16	2	2.94		
PHIL11	50 (1-3)	16	1	3.25		
PHIL12	31;13;44 (2-3;4;5-7)	16	2	3.75		
PHILD: PRIVACY as opportunity						
PHIL13	56.4 (5-7)	16	3	4.69	4.48	Neutral with respect to statements suggesting that privacy laws provide any opportunity for the bank.
PHIL14	68.8(5-7)	16		5.25		
PHIL15	19;25;38 (1-2;4;5-6)	16		3.94		
PHIL16	43;13;44 (1-3;4;5-7)	16		4.06		

[3] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.

Appendix N-5: Case D - Frequencies and Means from IPO Survey (cont'd)

IPO Component	Frequency (Cumulative Percent) % (response range of accumulation)[4]	No. of responses (valid/ missing)	No. of "no opinion"	Means	Means of means	Interpretation
BHVA: Non compliant						
BHV1				1.13	1.25	Consistently in disagreement with statements that would indicate a lack of privacy action.
BHV2				1.25		
BHV3				1.44		
BHV4				1.19		
BHVB: Minimally compliant						
BHV5				3.56	4.1	Largely neutral in consideration of the extent to which privacy has been incorporated into operations. Stronger agreement that privacy is taken into consideration in business plans. Somewhat stronger in agreement with statement that approach reflects industry consensus.
BHV6				5.31		
BHV7				3.38		
BHV8				4.13		
BHVC: Professional or trade group codes						
BHV9				5.69	5.69	There is agreement that the firm is engaged in more than minimal privacy activities that are at least comparable with their competitors.
BHV10				6.25		
BHV11				5.75		
BHV12				5.06		
BHVD: Enhanced privacy						
BHV13				3.00	3.85	Disagreement idea that their firm is a privacy leader. Stronger agreement that privacy is given priority in business decisions.
BHV14				5.38		
BHV15				2.94		
BHV16				4.06		

[4] Note: Individual percentages (e.g., 75) and response range (e.g., 1 – 3) indicate that 75% of the responses came from an accumulation of strongly disagree (value = 1), disagree (value = 2) and somewhat disagree (value = 3). Percentages shown with more than one number (e.g., 33/33/33) and more than one response range (e.g., 1 – 3; 4; 5) indicate that 33% of responses were cumulative from strongly disagree, disagree and somewhat disagree (1 – 3); neutral (neither agree nor disagree, value = 4); and somewhat agree (value = 5). Some percentages shown with more than one number will not equal 100% either due to rounding or because there were "no opinion" responses.