

Politicizing Privacy:
'Focussing Events' and the Dynamics of Conflict

by

David Jeffrey Allan Todd
B.A., University of Manitoba, 1996

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF ARTS

In the Department of Political Science

We accept this thesis as conforming
To the required standard


Dr. C.J. Bennett, Supervisor (Department of Political Science)


Dr. N. Ruff, Departmental Member (Department of Political Science)


Dr. D.H. Flaherty, Outside Member (Professor Emeritus, University of Western Ontario)


Mr. C. D. Raab, External Examiner (Professor of Government, University of Edinburgh)

© David J. A. Todd, 2001

University of Victoria

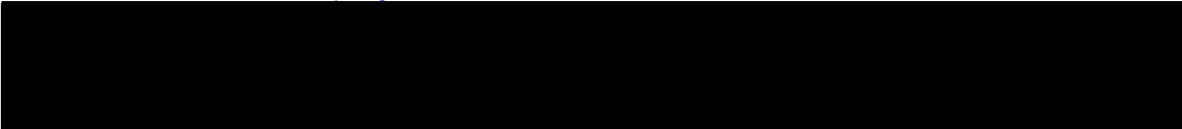
All rights reserved. This thesis may not be reproduced in whole or in part, by
photocopy or other means, without the permission of the author.

Supervisor: Dr. Colin J. Bennett

ABSTRACT

In the past, the issue of information privacy has rarely captured the attention of the political agenda beyond the enactment of national data protection regimes. However, there is compelling evidence to suggest that privacy is an “issue whose time has come”. While analysis of the politics of privacy has tended to examine the various dimensions of the policy cycle, a rationalistic and technocratic approach obscures the often neglected and politically salient dimensions of privacy: the politicization of privacy issues and the dynamics of privacy conflicts. To explore this notion, two recent high-profile privacy conflicts are presented, one in the public sector of Canada over Human Resource Development Canada’s ‘Longitudinal Labour Force File’, and one in the private sector involving the Internet advertiser DoubleClick Inc.. Evidence of shared processes and similar dynamics is presented, as well as insights into the new politics of privacy and the emergence of a privacy industry.

Examiners:


Dr. C.J. Bennett, Supervisor (Department of Political Science)


Dr. N. Ruff, Departmental Member (Department of Political Science)


Dr. D.H. Flaherty, Outside Member (Professor Emeritus, University of Western Ontario)


Mr. C. D. Raab, External Examiner (Professor of Government, University of Edinburgh)

Table of Contents

Title Page.....	i
Abstract.....	ii
Table of Contents.....	iii
Acknowledgements.....	v
<i>Introduction: The Emergence of a Consciousness of Privacy.....</i>	<i>1</i>
<i>Chapter One: The Origins and Evolution of the Concept of Privacy.....</i>	<i>6</i>
Introduction.....	6
The Origins and Evolution of the Concept of Privacy.....	7
The Problem with Privacy.....	7
Privacy as a Philosophical Concept	8
Privacy as a Legal Concept.....	10
The Emergence of Privacy Pragmatism	12
The Origins of Data Protection and the emergence of Fair Information Principles	15
Trends in the Politics of Privacy	19
Comparative Policy and the Convergence of Processes	20
Public Policy Formation and the Competition between Ideas and Interests	24
Implementation and Evaluation	29
Politicizing Privacy: Lessons from Activists	36
Policy Analysis and the Dynamics of Agenda-Setting	41
Focusing on Focusing Events.....	49
Organization of the Case Studies.....	51
<i>Chapter Two: The Politicization of the Longitudinal Labour Force File.....</i>	<i>53</i>
Introduction.....	53
The Policy Landscape and the Privacy Problem.....	54
The Policy Landscape in Canada	54
The Privacy Alarm	58
Origins of the Policy Problem: The Creation of HRDC	59
The Audit of the Longitudinal Labour Force File.....	61
The Privacy Problem.....	62
The Internal Debate Between HRDC and the PCO	64
The Dynamics of Conflict	68
Initial Publicity.....	68
Escalation	71
Intensification.....	75
Denial	77
Reaction.....	79
Fallout.....	81
Aftermath	85
<i>Chapter Three: The DoubleClick Conflict.....</i>	<i>87</i>
Introduction.....	87
The Policy Landscape and the Privacy Problem.....	88
The Policy Landscape in the United States	88
Origins of the Policy Problem: The Commercialization of the Internet	91
The Privacy Problem.....	94

A Closer Look: Online Profiling.....	95
The Privacy Alarm	99
The Dynamics Conflict.....	101
Initial Publicity	101
Escalation	103
Intensification.....	108
Denial	116
Reaction.....	119
Fallout.....	121
The Aftermath	125
<i>Chapter Four: Privacy Politicized</i>	<i>127</i>
Introduction	127
Justification of Cases.....	127
The Dynamics of the Conflict.....	131
Initial Publicity	131
Escalation	132
Intensification.....	134
Denial	135
Reaction.....	136
Fallout.....	137
Rhythm and Processes	137
The Emergence of a Privacy Industry and the New Politics of Privacy.....	141
Works Cited.....	146

Acknowledgements

First and foremost, I would like to thank Colin Bennett for his guidance and support from the idea stage through to the completion of this project. It was a pleasure to work with you during my time in Victoria. I would also like to thank David Flaherty, Charles Raab, and Norman Ruff for their suggestions, editorial comments, and dialogue. It is a rare opportunity to have such a talented, experienced and respected committee. I thoroughly enjoyed the experience.

I would also like to thank my friends and colleagues in the Department of Political Science. It was a long road, and you were good company for the trip. I hope our lives will continue to intersect. To the team at CyberAlumni, your enthusiasm and drive helped me to believe that we could build something new and think outside of the box, and I learned a great deal in the process.

A sincere thanks to the Policy Research Initiative of the Government of Canada and the Social Sciences and Humanities Research Council for their generous Canadian Policy Research Award. I would also like to acknowledge the assistance of the Usenix Association for their generous travel scholarship.

Last but not least, I would like to thank my family for their support, financially, emotionally and unconditionally. I would also like to thank Sheri for her proof-reading and editing, but most of all for the support and encouragement that made such a project worthwhile.

Introduction: The Emergence of a Consciousness of Privacy

In the past, concerns over issues of information privacy, defined as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others"¹ have largely been contained within an elite community of policy makers, technocrats, lawyers, and computer specialists. This community came together in the late 1960's and early 1970's to address new privacy concerns that emerged as a result of the increased ability of governments and corporations to collect, compile, and match information on individuals in massive databanks. The policy problems at the time were studied independent of domestic politics, and the participants in the privacy community were charged with the task of disseminating the conclusions of the community to their respective societies and governments.² This resulted in the development of a number of privacy and data protection laws in advanced industrial states, which raised the issue of information privacy to the political agenda for the first time. The issue of privacy, however, has for the most part never been a particularly politically salient issue. Although the task of maintaining privacy has been a concern of some government officials and policy makers, it has never been an issue of such importance that it has been politicized much beyond the enactment of public policies around commonly accepted principles of information management.

Today, however, there is compelling evidence that this trend is changing. The issue of privacy has recently emerged as a "hot topic". A number of books, including Simson Garfinkel's *Database Nation: The Death of Privacy in the 21st Century*³, Jeffrey Rosen's *The Unwanted Gaze: The Destruction of Privacy in America*⁴, and Reg

¹ Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 7.

² See Colin J. Bennett, Colin J. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Information?" in Philip E. Agre and Marc Rotenberg's *Technology and Privacy: The New Landscape*. (Cambridge: MIT Press, 1996).

³ Simson Garfinkel. *Database Nation: The Death of Privacy in the 21st Century*. Boston: O'Reilly and Associates. 2000.

⁴ Jeffrey Rosen. *The Unwanted Gaze - The Destruction of Privacy in America*. Random House, 2000.

Whitaker's *The End of Privacy: How Total Surveillance Is Becoming a Reality*⁵ offer indicting commentary and criticism of the current privacy landscape. These books also provide dystopic predictions of things to come if we choose not to speak out against the adoption and integration of increasingly pervasive and sophisticated technologies of surveillance. In a similar spirit, the privacy issue has also attracted the attention of the major television network broadcasters, popular culture magazines, and the daily news press, all of whom have recently drawn attention to the privacy crisis. In addition, privacy has emerged as one of the most important issues on the Internet, and the issue is often considered the greatest barrier to entry into participation in the 'new economy'. There is impressive evidence that suggests that the recent attention devoted to the issue has resulted in a heightened consciousness of privacy risks. Given the increased salience of privacy concerns, it appears that privacy may be "an issue whose time has come".

Many of the larger questions and problems that surround the politics of privacy are concerned with philosophy, law, technology, and policy standards for ensuring privacy. As such, the first chapter of this thesis is dedicated to exploring the broad literature that is devoted to studying the concept of privacy, and in particular to a specific dimension of the concept, namely information privacy. In this regard, the philosophical and legal origins of privacy will be reviewed. This is followed by an analysis of how the privacy problem has come to be articulated as a policy problem, and how policy solutions have been enacted to provide safeguards for the protection of personal information of individuals living in the modern state. Because this thesis is primarily concerned with the *politics* of privacy, contributions from prominent scholars in the discipline of political science are also explored. Where privacy has been addressed by political scientists, it has typically been examined through the various dimensions of policy analysis, and specifically to the particular aspects of policy formation, implementation, and evaluation. Because political scientists have typically examined the more esoteric dimension of data protection, their analysis tends to be rationalistic and technocratic, and thus obscures some of the more interesting, politically salient, and often neglected phenomena that are less concerned with these aspects of policy analysis. Thus, this thesis embarks on an

⁵ Reg Whitaker. *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York: New Press. 1999.

examination of one of these neglected dimensions of the politics of privacy, namely the politicization of privacy issues and an analysis of the dynamics of privacy conflicts. To approach this aspect of policy analysis, a number of important contributions from the sub-field of agenda-setting are reviewed. Political scientists often mention that sudden, dramatic focussing events can act as triggering mechanisms for policy change. However, few studies explore the dynamics of these focussing events, and privacy scholars have generally not paid much attention to them at all.

To address this silence and fill a void in both the privacy and political science literature, Chapters Two and Three are dedicated to examining two recent high profile privacy conflicts that attracted the attention of both the political agenda and the public at large. The first case entails an analysis of a public sector privacy conflict in Canada. The dispute over the 'Longitudinal Labour Force File' (LLFF) operated by the Department of Human Resources Development Canada attracted a great deal of media attention and public concern, and the conflict was elevated to the political agenda. The LLFF is a comprehensive database that contains up to 2,000 bits of highly personal information about more than 30 million citizens. It includes information collected from tax returns, child tax benefit payments, welfare files, federal job programs, job training and employment services, employment insurance files and the national health insurance master file. In many regards, this case is representative of the type of privacy concerns that individuals have regarding the collection and storage of personal information by governments.

The second case addresses a private sector privacy conflict in the United States. DoubleClick, the Internet's most prolific ad-serving company, has recently drawn much attention over their plans to merge an off-line database containing information on 88 million U.S. households with their on-line database of consumer profiles containing Internet transaction and navigation information. DoubleClick justifies the collection and amalgamation of this information because it allows them to deliver advertising that is allegedly relevant to Internet users interests and preferences. However, privacy advocates oppose DoubleClick's practices because it allows the company to track the online activities of Internet users without their explicit consent and profile their online activities.

The business practices of DoubleClick thus have broad implications for privacy protection on the Internet.

Both of these case studies have in common a privacy conflict that has captured the imagination of a wide audience and a diverse range of actors and interests. They are also both fundamentally concerned with the detailed organization of sensitive information on individuals in databases, fears about record linkages, and anxieties about the practice of profiling. However, the actual substances of the conflicts, their scope and magnitude, the actors involved, the motives surrounding the conflicts, the context in which the conflicts emerged, the mechanisms in place to address the conflicts, and the paths to their resolution, are very different. These case studies are in many respects paradigmatic of the concerns of individuals, the privacy community, and the institutions that govern privacy over a practice that has seemingly become the norm in this 'information age'. These conflicts are also interesting in that they involve values that threaten long held assumptions about personal privacy, and because the resolution of these conflicts could contribute to a reconfiguration of how the limits of privacy are defined and conceptualized.

Each of these respective cases is presented in a similar fashion. The first part of the chapters is devoted to exploring the background conditions of the conflict, including an examination of the policy landscape in each of the political jurisdictions, the origins of the policy problem, the privacy problem inherent in the use of the particular technologies, and the privacy alarm that triggered publicity of the problem. This is followed by the second part of the analysis, which considers the dynamics of the privacy conflict as a 'focussing event'. In this regard, the dynamics and rhythm of the conflict are sub-divided into a series of component stages, which have been devised for conceptual and analytical clarity. The stages of the conflict are identified as *initial publicity*, *escalation*, *intensification*, *denial*, *reaction*, and *fallout*. This is followed by a brief description of the immediate *aftermath* of the conflict.

The accounts of these conflicts have been developed by documenting and analyzing a number of sources, including policy documents, press releases, journalistic materials such as newspaper articles and magazine coverage, online media coverage and sources on the Internet, newsgroup postings, and a meeting with a representative of the

Privacy Commissioner of Canada's Office. The dynamics of the conflicts were then constructed based on this material, and deconstructed into their component stages.

In the concluding chapter, I reflect on the nature and context of the case studies, and provide a justification for their analysis. In doing this, I compare and contrast these conflicts, and highlight their similarities and differences. The analysis of these cases offers some important insights into the nature of privacy conflicts, and in addition they reveal some important dimensions of the dynamics of 'focussing events'. In particular, I consider the evidence that there are a number of similar processes at work that may provide valuable lessons to those interested in the nature of conflict and the politics of privacy. The thesis concludes by considering the emergence of a 'privacy industry' and indications that there is a 'new politics of privacy'. However, the first task is to explore the problem with privacy, and investigate the origins of the concept.

Chapter One: The Origins and Evolution of the Concept of Privacy

Introduction

One of the indisputable hallmarks of the twentieth century has been the emergence of the 'information age' and the widespread adoption and use of information and communications technologies. In many respects, the invention of the computer has transformed the economy, society, culture, and how individuals interact within these dimensions of modern life. However in another respect, it has also transformed ideas about individuality, autonomy, anonymity, control, and the distinction between public and private. One consequence of this transformation has been marked by the increased capabilities of organizations, both public and private, to collect, aggregate, manipulate, and disseminate vast amounts of information about ourselves, with or without our knowledge, often without our consent, and perceivably out of our control. One of the predominant impacts of this transformation has been the increasing sense that the technologies we have developed to empower us have resulted in the erosion of our privacy.

The intent of this chapter is threefold. First, I will consider the inherent problems that are associated with the concept of privacy, and explain how the notion has evolved from its philosophical and legal origins into a more technical value that can be regulated in public policy. Secondly, I will review the literature in political science that speaks to the problem of privacy, and explore the contributions that political scientists have made to the understanding of privacy. Privacy scholars in political science have tended to undervalue the significance of unforeseen privacy conflicts and the ways in which 'focussing events' can be exploited to attract public and political attention and gain access to the political agenda. This is the primary contribution of this thesis. As such, I will conclude the chapter by exploring a number of theoretical contributions from political scientists who study agenda-setting and the transformation of ideas into issues. I will now turn to examine the problem of privacy.

The Origins and Evolution of the Concept of Privacy

The Problem with Privacy

In much of the literature on privacy, there is an implicit recognition of the inherent difficulty with defining the term "privacy". It is a vague, ambiguous, and controversial concept that has led commentators to conclude that "(f)ew values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists".⁶ Others conclude that "(p)erhaps the most striking thing about the right to privacy is that nobody seems to have a clear idea of what it is."⁷ Despite a clear consensus regarding the difficulty in coming to terms with what privacy is, it is commonly recognized as an important value for individuals living in modern society.

Claims to privacy are invoked for a number of justifications. These range from the wiretapping of communications devices, the invasive and intrusive characteristics of police searches by the state, the overstepping of boundaries into personal matters by journalists, employee workplace monitoring, drug and genetic testing, control over the disclosure of deeply intimate and personal concerns such as health conditions or matters of abortion, the right to die, the ability of an individual to make private decisions, and the ability to control the collection, distribution, storage, and disclosure of information about one's self. This list is by no means exhaustive, but it represents a sample of common concerns in which the idea of privacy is often championed. This also reveals one of the interesting aspects of privacy - its multi-dimensionality. Some dimensions of privacy are personal, some are social, and some are legal. As such, privacy is invoked to refer to the exclusiveness of the physical space around an individual, to signify the autonomy of an individual to make a decision without the outside interference of others, and to express the right of individuals to control the circulation of personal information about themselves.⁸ This thesis will focus on the latter dimension of privacy.

⁶ Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 7.

⁷ Judith Jarvis Thomson, "The Right to Privacy". *Philosophy and Public Affairs* 4, no. 4, summer 1975. p.295.

⁸ Colin J. Bennett. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press. London. 1992. p. 13.

Although it would be impossible to enumerate a comprehensive inventory of concerns enveloped under the rubric of privacy, it is possible to trace the philosophical and legal origins of the concept that have informed its construction. Privacy is an idea, a cultural artifact whose origins can be traced and its many meanings deciphered or understood. To understand how this individualistic conception of privacy has been developed over time, the legal and philosophical literature will be reviewed to demonstrate how the concept of privacy has come to be defined as a policy goal and how lawyers and philosophers have reinforced this conception.

Privacy as a Philosophical Concept

The ontological roots of the concept of privacy can be traced back to the metaphysical speculations of Plato. Plato argued that there was an irreducible dualism between the body as material and observable, and the soul, as immaterial and unobservable. Plato argued that reason resided in the soul, hidden from others until it was disclosed to them or revealed through conduct or action. Although Plato did not discuss the concept of privacy in explicit terms, implicitly he articulated a distinction between public and private that established the significance of the private realm for personal development.

Since Plato, the concept of the "rational soul" has been defined against the physical and emotional nature of man. St. Augustine elaborated on the divine significance of the inner life and introduced an understanding of the private realm that has had a significant impact on Christianity, and on modern conceptions of the private realm. St. Augustine reasoned that the conduct of a person's soul was of greater significance than their outward conduct and appearances, and that it was the state of one's soul, measured in thoughts, motives, intentions, fantasies, and fears that determined whether or not one was virtuous in the eyes of God.⁹ However, because the conduct of the soul can be easily hidden from others, regulation of the soul by human law was problematic. The lack of regulation over the inner, private realm of the person often resulted in the application of techniques of torture, perfected by the Inquisition, on subjects to persuade the reluctant to reveal their inner thoughts and desires. This problem later inspired St. Thomas Aquinas

⁹ Robert Holmes, "Privacy: philosophical foundations and moral dilemma's" in *Privacy Disputed*, edited by Pieter Ippel, Guus de Heij and Bart Crouwers. SDU. Den haag, 1995. p. 16

to develop the concept of 'divine law' in the thirteenth century. The idea of divine law overcame the limitations of human law because it could regulate both the 'inner lives' of people as well as their outer conduct through reward or punishment in the afterlife by God. Without divine law, sins committed in the absence of others, or even in the private thoughts of one's mind, would go unpunished.¹⁰

In the 17th Century, renewed interest in epistemology and the nature, limits, and criteria of human knowledge reinvigorated ideas of the private realm and the role of the autonomous individual within the larger society. Perhaps the most profound influence on contemporary conceptions of privacy was the development of liberal thinking, and in particular a certain type of liberalism associated with the work of John Locke. This *Lockean liberalism* emphasizes the notion that individuals possess certain natural rights within the larger social and political environment. The individual is conceptualized as a self-interested atomistic unit, and the role of government is to ensure the protection of that individual's natural rights. The distribution of these natural rights also serves to restrict the power of the government. Within this tradition, a justification for privacy resides in the individual by virtue of being an individual, and privacy is important to the individual for purposes of self-development and to establish intimate human relationships. Fundamental to Locke's ideas of the individual within the larger society is the notion of difference: my privacy claims and interests are different from yours.¹¹ Its importance is thus framed in individualistic terms that emphasize both separateness and self-interest.

One of the consequences of the development of the secular nation state was an increasing interest in the private inner lives of the individual for the benefit of political order and stability. In re-theorizing the distinction between the public and private realms, John Stuart Mill argued that there should be certain "self-regarding" activities of concern to the private individual, separate from the "other-regarding" activities of concern to community interest and regulation.¹² This 'domain of consciousness' recognized the inner

¹⁰ *ibid.* p. 17.

¹¹ Colin Bennett, "The Political Economy of Privacy: A Review of the Literature".
<http://sitka.dcf.uvic.ca/poli/bennett/research/gnom.htm#anchor3>

¹² *Op. Cit.*, Bennett, "The Political Economy of Privacy".

private realm within each person, and Mill suggested that it was the focal point of human liberty:

This, then, is the appropriate region of human liberty. It comprises, first, the inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological.¹³

The recognition of the domain of consciousness and the subsequent liberties accorded to it contributes to an individualistic liberalism that measures the value of particular social, economic, or political systems against the interests of the individual. It was this line of reasoning that contributed to the development of the legal concept of privacy.

Privacy as a Legal Concept

Twentieth Century legal conceptions of privacy as a specific right and value have their roots in Samuel Warren and Louis Brandeis's 1890 *Harvard Law Review* Article entitled "The Right to Privacy".¹⁴ The article was written in consideration of the development of new techniques that were deemed to undermine the privacy of an individual, namely the ability of the newspapers in Boston and elsewhere to report on events in which they were not in physical attendance. The problem was articulated in consideration of the emergence of a new technology: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'"¹⁵ Their argument was based on the notion that the common law protected a "right to privacy" and that "now the right to life has come to mean the right to enjoy life - the right to be let alone."¹⁶

Warren and Brandeis argued that the central assumption of the 'the right to be let alone' is part of a broader, "more general right to the immunity of the person - the right to one's personality."¹⁷ This idea grounded a right to privacy in common law based on existing protections afforded to intellectual and artistic property:

¹³ As cited in Ippel et al., *Privacy Disputed*. p. 17.

¹⁴ Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. 4, 1890.

¹⁵ *ibid.* p. 195.

¹⁶ *ibid.*

¹⁷ *ibid.* p. 207.

The protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the more general right of the individual to be let alone. . . . The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of inviolate personality.¹⁸

The argument put forward here by Warren and Brandeis emphasizes the importance of privacy to an individual. New developments in technologies and the increasing complexity of modern life "have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual."¹⁹

There were few significant legal developments regarding privacy until William Prosser published an influential 1960 *California Law Review* article that led him to conclude that "at the present time the right of privacy, in one form or another, is declared to exist by the overwhelming majority of the courts."²⁰ One of the shortcomings of privacy law was that there was only one tort action for "privacy", when in reality the general concept of privacy encompasses a variety of interests. Prosser overcame this problem by isolating four distinct categories of torts in state law decisions that he argued represented four different types of privacy invasions. The first tort, the tort of Intrusion, protects the plaintiff's interest in being free from unwarranted "intrusions" into his or her personal privacy "zones" which each person may reasonably expect the law to protect in relation to their physical persons.²¹ The second privacy tort, "Appropriation", is based upon the fact that an individual's privacy (or an aspect of it) is akin to a "property" interest and is entitled to legal protection in much the same ways as any other personal property interest.²² The third tort, "Public Disclosure" (of private facts), is intended to

¹⁸ *ibid.* p. 205.

¹⁹ *ibid.* p. 196.

²⁰ William L. Prosser, "Privacy". *California Law Review* 48, no. 3, August 1960. p. 386.

²¹ Edward C. Martin, "Privacy Torts". *Cumberland School of Law*, Samford University.

<http://netlaw.samford.edu/Martin/AdvancedTorts/privacyhome.htm> . The specific elements of the tort of Intrusion are: 1). Intrusion by the Defendant (either intentionally or even accidentally); 2). into an area in which the Plaintiff has a reasonable expectation of privacy; and 3). which intrusion is highly offensive to reasonable persons.

²² *ibid.* The tort of "Appropriation" requires these specific elements: 1). Wrongful appropriation by the Defendant (either intentionally or even accidentally); 2). of the Plaintiff's name, likeness, or other purely personal aspect; 3). for some commercial gain or advantage.

protect an individual's interest in being free from unwarranted invasions of his or her private, personal matters. It is primarily intended to protect one's mental or emotional state of mind.²³ The final tort that Prosser isolated was the tort of "False Light". "False Light" is considered one of the more problematic of the privacy torts, because it requires some type of false (or at least misleading) statement, and for this reason it often appears to overlap somewhat with the separate tort of "Defamation". This tort is also intended to protect an individual's mental and emotional well-being.²⁴

Although Prosser's four categories of privacy Tort were widely accepted, critics claimed that the privacy torts were too far removed from the philosophical foundations of Warren and Brandeis. Furthermore, tort law has been criticized because it does not protect an individual before a violation occurs, nor does it prevent the violation from occurring. It only provides a means of redressing grievances after an invasion.²⁵

The Emergence of Privacy Pragmatism

In the early 1960's, renewed philosophical interest in privacy concerns were triggered by the emergence of new technologies, and in particular by computerized data systems that could store vast quantities of information on individuals. Alan Westin's foundational analysis of privacy in *Privacy and Freedom* develops the concept beyond that of Warren and Brandeis by examining the issue of privacy within the larger social context. Westin examines a number of social, economic, technological and political changes that had emerged to impair claims to privacy. This work has shaped much of the thinking about privacy as a public issue in North America. Westin's work provides a comprehensive and scholarly interpretation of privacy, and he also put forth a detailed and carefully expressed agenda for action.

Westin's work begins by addressing the nature of privacy and its role in social and political thought. He suggests that man's desire for privacy is rooted in his animal origins, that privacy played an important role in primitive societies, and that privacy

²³ *ibid.* The specific elements of the tort of Public Disclosure are: 1). A public disclosure by the defendant (either intentionally or even accidentally); 2). of private facts relating to the plaintiff; and 3). which would be highly offensive (i.e., embarrassing) to reasonable persons.

²⁴ *ibid.* False Light consists of the following elements: 1.). A publication by the defendant about the plaintiff; 2). made with actual malice; 3). which places the plaintiff in a false light; and 4). that would be highly offensive (i.e., embarrassing to reasonable persons.)

continues to be a significant component of the Western liberal political tradition that places limits on the surveillance powers of governments.²⁶ He defines privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”.²⁷ Within the larger context of the individual within society, Westin contends that “privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.”²⁸ Westin stresses, however, that the value of privacy is not an “absolute” value, because participation in the society from which the individual removes themselves is an equally powerful desire. Hence, privacy is understood as a claim, and not a right. Thus, the measure of the value of privacy must be considered as a compromise in which “each individual is continually engaged in a personal adjustment process in which he *balances* the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.”²⁹

Westin further situates the importance of privacy to the individual in individualistic terminology. In his discussion of the four states of individual privacy, which he designates as solitude, intimacy, anonymity, and reserve, and the functions that these basic states render by providing the individual with a sense of personal autonomy, namely emotional release, self-evaluation, and limited and protected communication, Westin concludes that “the right of individual privacy” amounts to “the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public.”³⁰

In Westin’s conception of privacy, an individual’s privacy is in competition with the competing desire of social participation. It is the responsibility of the individual to strike a balance between the two competing interests. This balance is problematized however by “privacy-invading phenomena” characterized as other individual’s inherent

²⁵ Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, Chapel Hill. 1995. p. 35.

²⁶ Westin, *Privacy and Freedom*, pp. 8-22.

²⁷ *ibid.* p. 7.

²⁸ *ibid.*

²⁹ *ibid.* emphasis added.

curiosity and the wider universal value of surveillance by authorities to enforce “rules and taboos” within the larger social structure.³¹

Westin sees the “privacy problem” as a result of new kinds of intrusions that have disrupted previously balanced social relationships. These intrusions are brought about by developments in technology that resulted in increasing pressures against privacy that were not anticipated by privacy-protecting conventions before the emergence of these technologies. In the “imbalanced” state that has resulted, people are less protected than they were previously by these threats. Legislation and policy is thus necessary to “restore the balance”.³²

Because the effects of new technologies make personal information more easily available, American constitutional, statutory, and common law have developed “shields of privacy” to protect both individual and organizational autonomy. Action is thus necessary to “redress the balance” between privacy and other interests. As Westin notes:

If privacy is to receive its proper weight on the scales in any process of balancing competing values what is needed is a structured and rational weighing process with definite criteria that public and private authorities can apply in comparing the claims for disclosure or surveillance through new devices with the claims to privacy.³³

Westin suggests that five broad concerns should be addressed to guide the reform of the management of personal information: Is the need for information strong enough to warrant its collection? Are there other ways of satisfying the need for this information? Is the form of inquiry reliable? (does it allow for the judgements that the situation requires?) What form of consent (if there is any) do individuals provide for the collection of information? How trustworthy is the agency that administers the collection of information? When questions such as these are posed, Westin believes that a number of restraints may affect whether or not information is to be collected. These include enhanced public consciousness of the issues, scientific developments to counter technologies of surveillance, policy decisions within organizations to avoid practices that

³⁰ *ibid.* p. 42.

³¹ *ibid.* p. 20.

³² James Rule, Douglas McAdam, Linda Stearns, David Uglow, *The Politics of Privacy*. Elsevier, New York. 1980. p. 74.

³³ Westin, *Privacy and Freedom*. p. 370.

may be privacy invasive, agreements among organizations to limit surveillance in the workplace, and the adoption of privacy protecting standards by professional bodies.³⁴

The underlying structure of Westin's analysis and his recommendations for public policy have influenced the privacy debate in North America. His work has also affected how the issue of privacy has been articulated in political attempts to resolve threats to privacy and insure a balancing approach to mediate between the conflicting interests of an individuals private and social goals. In the next section, I will demonstrate how the notion of "balance" as articulated by Westin and the definition of privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" has informed the public policy debate and process.

The Origins of Data Protection and the emergence of Fair Information Principles

The vague and subjective character of privacy has made it difficult to articulate as a problem for public policy.³⁵ This ambiguity has required the development of a more explicit concept in which to frame threats brought about by information and communication technologies; that of data protection. As Flaherty notes, there is an important distinction to be made between 'protecting privacy' and 'data protection'. Whereas privacy is a broad, all-encompassing concept that envelops a wide range of concerns, data protection, on the other hand, is an aspect of privacy protection that is concerned with the control of the collection, use and dissemination of personal information.³⁶ Data protection is thus implemented to limit the surveillance capabilities of organizations and other individuals and to preserve an individuals personal privacy.

The term 'data protection', as with the term privacy, is not without its definitional problems. It is a more technical and esoteric term, and has little meaning to most individuals.³⁷ As such, most English speaking nations have chosen to employ the term 'information privacy' to encompass the idea of data protection and provide a more popular appeal to the statutes enacted by various governments. The concept of information

³⁴ Rule et al., *The Politics of Privacy*. p. 75.

³⁵ Bennett, *Regulating Privacy*. p. 13.

³⁶ David Flaherty, *Protecting Privacy in Surveillance Societies*. University of North Carolina Press, Chapel Hill, 1989. pp.xiii-xiv.

privacy draws attention away from the more generalized philosophical and legal debates about privacy and instead focuses on particular problems which are emerging or have emerged through the increased proliferation of information systems. As such, it moves from a concept of privacy as an 'aesthetic' value, that of restricting information as an end in itself, to a concept of privacy as a 'strategic' value, where personal information is restricted as a means to some other end.³⁸

This notion of a 'strategic' value of privacy as the restriction of information for some other end embodies the spirit of data protection rules. These rules have their origins in Westin's conception of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" and they have been articulated in the development of a set of 'fair information principles'. The idea of fair information principles was borrowed from American labor and trade law and the notion of fair and unfair labor or trade practices.³⁹ This way of thinking about principles of fair information practice was first evident in the 1970 Fair Credit Reporting Act, and the world's first attempt to apply the fair information principles was the 1974 United States Privacy Act. The notion of fair information principles arose directly out of the work of the Health, Education, and Welfare (HEW) Advisory Committee. The committee convened to address the growing public and private use of automated data systems that contained information about individuals and the government's increased use of computers. They concluded that the increasing computerization of personal records required new controls on technology and that new protections for individuals were necessary in light of these developments. The HEW committee offered the following formulation of privacy as it pertains to personal-data record keeping:

An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information. Any recording, disclosure, and use of identifiable personal information not

³⁷ Bennett, *Regulating Privacy*. p. 13

³⁸ Rule et al., *The Politics of Privacy*. p. 22-23.

³⁹ Bennett, *Regulating Privacy*. p. 96.

governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.⁴⁰

The assumptions articulated in the above statement provided the basis for the creation of the fair information principles. At virtually the same time, the Younger Committee in Britain was establishing a similar set of principles. The substance of each of these sets of principles was quite similar, although the American principles were directed toward the protection of an individual's information in general while the British principles pertained to data stored on computers.⁴¹

Most privacy legislation is based on some variation of the fair information principles. Although different jurisdictions have developed slightly different articulations of the fair information principles, Flaherty's enunciation of "Data Protection Principles and Practices for Government Information Systems" provides a good example of the principles being put to use. For Flaherty, information privacy protection can be afforded by adherence to the following list of interrelated principles:

1. The principles of publicity and transparency (openness) concerning government personal information systems (no secret data banks).
2. The principles of necessity and relevance governing the collection and storage of personal information.
3. The principle of reducing the collection, use, and storage of personal information to the maximum extent possible.
4. The principle of finality (the purpose and ultimate administrative uses for personal information must be established in advance).
5. The principle of establishing and requiring responsible keepers for personal information systems.
6. The principle of controlling linkages, transfers, and interconnections involving personal information.
7. The principle of requiring informed consent for the collection of personal information.

⁴⁰ U.S. HEW, *Records, Computers and the Rights of Citizens*. As cited in Bennett, *Regulating Privacy*. p. 97.

⁴¹ *ibid.*

8. The principle requiring accuracy and completeness in personal information systems.
9. The principle of data trespass, including civil and criminal penalties for unlawful abuses of personal information.
10. The requirement of special rules for protecting sensitive personal information.
11. The right of access to, and correction of, personal information.
12. The right to be forgotten, including the ultimate anonymization or destruction of almost all personal information.⁴²

This list captures the essential quality of fair information principles. With respect to privacy, the articulation of fair information principles has likely been the most significant policy development in the computer age.⁴³ The principles were designed specifically to facilitate an increase in trust by allowing "the lid to be taken off" off the black box of the database to reveal the processing techniques of personal information.⁴⁴

The nineteen sixties were a transformative era for the evolution of the concept of privacy. Governments were faced with a new technological problem - the 'rise of the information society' - and they responded with a new technical solution - 'fair information principles'. In a number of ways, the idea of data protection is true to its philosophical origins. It is embodied by a liberal conception of rights, it serves as a protection against the invasive curiosity of the state and civil society, and it provides an individual with the opportunity to take action against a perceived violation. But it is also characteristically different from previous conceptions of privacy in that it provides a concrete solution to an abstract problem. It is no longer concerned with establishing the 'domain of consciousness'; instead its function is to implement rules. The concept of privacy, once historically abstract, vaguely defined, and contextually ambiguous evolved into something clearly identifiable with standards, rights, obligations, and procedures.

Whereas consideration of privacy was once the exclusive domain of philosophers and lawyers, the development and application of data protection has largely been

⁴² Flaherty, *Protecting Privacy in Surveillance Societies*. p. 380.

⁴³ Robert Gellman, "Does Privacy Law Work?" in Philip E. Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape*. MIT Press, Cambridge. 1996. p. 196.

⁴⁴ Bennett, *Regulating Privacy*. p. 121.

attended to by technocrats and specialists. Flaherty argues that data protection, like issues of nuclear or environmental regulation, requires a cadre of specialists to oversee implementation.⁴⁵ This is because data protection is a complex issue that requires balance between a strong commitment to data protection, a talent for public administration, and an understanding of the technocracy and technology.⁴⁶ It has also become an increasingly important subject for democratic political systems, because the state, in pursuit of justice and efficiency, will develop the capacity and ability to take action against activities that privacy assists, such as fraud and organized crime. Technocracy and specialization are thus both essential components of data protection.

The concept of privacy, once considered irrational, was rationalized through the development of data protection. The distinctive feature of the data protection model is the utilization of a comprehensive and systematic legislative regime based on universal principles to regulate data treatment. It offers simple rules and defined boundaries for information use. However, in specifically delineating the parameters of information privacy, it also sets limits on the traditional conception of privacy, thus constraining its ambiguous and diverse nature. Awareness of this constraint also reveals perhaps the most interesting aspect of privacy: privacy is more a question of *politics* than it is an issue that can be settled by systematic and comprehensive legislative regimes.⁴⁷ This is because the complex and contextual character of privacy often necessitates a need to examine and judge competing and diverse claims and interests to privacy. Given the inherent political dimensions of privacy, how has the discipline of political science addressed the privacy issue?

Trends in the Politics of Privacy

Within the field of political science, the question of privacy intersects with a wide spectrum of its sub-disciplines, including political theory, public policy, political behaviour, public administration, comparative politics, and international relations. Despite this, few political scientists have examined the political aspects of privacy and

⁴⁵ Flaherty, *Protecting Privacy in Surveillance Societies*. p. 389.

⁴⁶ *ibid.* p. 388.

⁴⁷ See W.B.H.J. van de Donk, Colin J. Bennett, and Charles D. Raab, "The politics and policy of data protection: experiences, lessons, reflections, and perspectives". *International Review of Administrative Sciences*, Vol. 62, No. 4, December 1996.

data protection. Where privacy has been a topic of political scientists, it has primarily addressed the various dimensions of policy analysis, specifically policy formation, implementation, and evaluation. Others outside of the discipline of political science also speak to an important aspect of the politics of privacy, namely the role of advocacy and political activism. In what follows, I will review the important contributions to the privacy debate by political scientists and activists to situate its significance for understanding the politics of privacy.

Comparative Policy and the Convergence of Processes

One of the most predominant themes examined by the political science literature is the process by which data protection has been introduced and enacted in various national agendas. For example, Colin Bennett seeks to explain the motivations of different countries that have enacted data protection regimes, and to explore why different countries around the globe have enacted similar responses to a common problem. Bennett employs a theory of 'convergence' from the field of comparative public policy which explains the tendency of different societies to grow more alike, and in the process develop similarities in the various and sundry structures, processes, and performances throughout society.⁴⁸

Bennett's analysis demonstrates that from the beginning, the issue of data protection was undeniably an international issue on an international stage.⁴⁹ One force that influenced this development is the process of *elite networking*. This is represented by the emergence of a group of international experts that created a network of contacts to

⁴⁸Colin J. Bennett, "Review Article: What is Policy Convergence and What Causes It?", *British Journal of Political Science*, vol. 21, 1991. p. 215. From a policy perspective, convergence can mean one of five things. First, there can be a convergence of policy *goals*. The convergence of policy goals refers to a coming together with a common desire to address a common policy problem. Secondly, there can be a convergence of policy *content*. Policy content refers to formal arrangements that are enacted by a particular government, such as statutes, administrative rules and procedures, the development of regulatory standards, and decisions ordered by the court. Thirdly, there can be a convergence of policy *instruments*. These are the institutional tools that are employed by governments to administer policy. Policy instruments can take a number of forms, including regulative, administrative, and judicial. Fourthly, policy convergence can be recognized through policy *outcomes*. Policy outcomes are the actual observable results, the impacts and consequences of the implementation of a policy. Fifthly, there can be a convergence of a particular policy *style*. Policy style refers to the way in which responses to a policy problem are formulated. The style of a policy can be reflected by the ideological persuasions of the policy maker and the political doctrines of the legislating regime.

⁴⁹Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press. London. 1992. p. 101.

discuss the effects that the new technologies had on society and consequently on an individual's data security. The group developed into a cross-national policy community over time, compelled by a shared concern for privacy and the desire to emulate successful policies in other jurisdictions.⁵⁰ Consequently, improved communication between experts and pressure by the policy community in the early 1970's resulted in a consensus on the codification of fair information principles, and this culminated in the introduction of the non-binding guidelines of the Organization for Economic Cooperation and Development and the Council of Europe.⁵¹ By the 1980's, the international policy community became increasingly more institutionalized around the desirable content of data protection, and emerged as a cross-national epistemic community.⁵² The organization of the cross-national policy community, including individuals from government, the business sector, academia, and consumer and public interest groups contributed to another process of convergence: the harmonization of international data protection standards.

Convergence through the process of harmonization requires a clear group of transnational actors, however, it also requires authoritative action to be taken by inter-governmental organizations. In this sense, the harmonization of policy is made possible through the existence of both intergovernmental and supranational institutions that facilitate the way in which a unified response to a common problem is shaped. Bennett suggests that the development of the 1995 "European Union Directive on the Protection of Personal Data and the Free movement of Such Data" is an attempt to *harmonize* international policy approaches. The purpose of the Data Protection Directive is to "ensure a high level of protection for the privacy of individuals in all member states . . . and also to help ensure the free flow of information society services in the Single Market by fostering consumer confidence and minimizing differences between the Member

⁵⁰ Bennett, Colin J. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Information?" in Philip E. Agre and Marc Rotenberg (eds.) *Technology and Privacy: The New Landscape*. MIT Press, Cambridge. 1996. p.99.

⁵¹ *ibid.* p. 101.

⁵² For a more comprehensive examination of this process, see Colin Bennett's "The International Regulation of Personal Data: From Epistemic Community to Policy Sector", presented at the 1992 convention of the Canadian Political Science Association in Prince Edward Island.

States' rules".⁵³ In this sense convergence through the process of harmonization is driven by a mutual recognition of *interdependence*.⁵⁴ The Directive explicitly specifies the functions and character of a state's supervisory authority and mechanisms, which further harmonizes for the first time in the history of international agreements the convergence of policy instruments.⁵⁵

Bennett suggests that not only is the E.U. Directive representative of a process of harmonization, it also exemplifies a process of *penetration*. Policy convergence through penetration results when states are forced to conform to the standards, regulations, and policies of other states by external actors.⁵⁶ For example, Article 25 of the Directive states that data transfers to a "third country" can only be conducted if the country can ensure an "adequate level of protection". "Adequacy" here is appraised "in light of all the circumstances surrounding a data transfer operation or set of data transfer operations."⁵⁷ Article 26 however sets out a number of derogations to counter the strong language of Article 25, by providing a provision that data can be transferred to a state with "inadequate" protection if the controller of the data agrees to enter a contract that "adduces sufficient guarantees with respect to the protection of privacy and fundamental rights and freedoms of individuals."⁵⁸ If it is determined that a third country does not provide adequate protection, EU states are to "take the measures necessary to prevent the data of the same type to the third country in question" until proper steps can be taken where the Commission "shall enter into negotiations with a view to remedying the situation".⁵⁹ The European Directive has certainly affected how countries outside the EU have addressed the data protection problem. While it is not the only reason why states have implemented data protection regimes, it has been a significant influence.

The EU Directive has also been the force for another cause of convergence, namely the process of *emulation*. The central characteristic of emulation is the use or

⁵³ *ibid.* See also Charles D. Raab and Colin J. Bennett "Protecting Privacy Across Borders: European Policies and Prospects". *Public Administration*, Vol. 72, Spring 1994.

⁵⁴ Bennett, "What is policy convergence and what causes it?" p. 225.

⁵⁵ Bennett, *Convergence Revisited*. p. 108.

⁵⁶ *ibid.* p. 227.

⁵⁷ See the "European Union Directive on the Protection of Personal Data and the Free movement of Such Data (1995)" Article 25 [1].

⁵⁸ *ibid.* see Article 26 [2].

⁵⁹ *ibid.* Article 25 [5].

application of foreign evidence to draw lessons from an external experience. It is through evidence of lesson drawing where a convergence of the policy experience can be recognized.⁶⁰ Bennett suggests that with the advent of more sophisticated technologies, data protection policies have become a necessary condition for being on the global information highway, and data protection is frequently regarded as a requirement of the modern state.⁶¹ In this regard, the EU Directive can be seen as more than simply an instrument of pressure - it is also a comprehensive legal framework for other nations to emulate. Not only does it represent the international consensus on data protection rights, it also provides an existing model for nations who have yet to adopt comprehensive privacy laws.

Bennett concludes that "data protection is a learning exercise that involves a mutual process of education and mediation from the bottom up as much as it involves regulatory command from the top down".⁶² The application of convergence theory to the data protection experience reveals that the European Union has extended a process of policy convergence with regard to *policy content*, as most advanced industrial nations have agreed to the main principles of data protection policy. Furthermore, the EU Directive also encourages a greater convergence of *policy instruments* that enforce, oversee, and implement protection.⁶³ He suggests, however that it is far more difficult to trace evidence of policy convergence at the *outcome* level. Although Flaherty argues that data protection requires a cadre of specialists much like the fields of environmental and nuclear policy, Bennett suggests that at the outcome level, data protection is not like environmental protection. The reason, he suggests, is conceptual rather than political, technological, or economic.⁶⁴ The EU Directive aims for a "high and common level of protection", but it does not define how that level is to be achieved. Environmental policy can be measured based on the desirable level of toxins in the air, soil or water. Data protection can only compare the letter of the law to actual practice, observe indicators of

⁶⁰ Bennett, What Is Policy Convergence and What Causes It?. p. 221.

⁶¹ Bennett, Convergence Revisited. p. 112.

⁶² Bennett, Convergence Revisited. p. 120.

⁶³ *ibid.* p. 120. Bennett notes that there is evidence of a divergence from the convergence model as well. This includes what he calls 'American Exceptionalism' - The public sector is governed by the 1974 Privacy Act, and the private sector has a patchwork of sectoral regulation and codes of practice that govern the private sector. American privacy policy is explored further in Chapter 3.

⁶⁴ Bennett, Convergence Revisited. p. 119.

the scope of the law, and compare and contrast the functions and powers of the policy instruments.

Bennett's examination of the politics of data protection is important because it reveals a number of important processes that have contributed to the convergence of data protection policy in a number of advanced western nations. However, the focus of the analysis is restricted to particular nations, and it is also limited insofar as it is concerned specifically with the policies and structures of data protection. While it explains the motivations for nations to enact policy to limit conflict by implementing rules and instruments, it does not speak to the nature of privacy conflicts or the processes by which conflicts over privacy come to be politicized and resolved within civil society. This thesis therefore attempts to address these silences by specifically examining how privacy conflicts are identified by the relevant agents of the state, and in a similar spirit, by identifying processes that explain the dynamics of conflict.

Whereas Bennett identifies the various processes that have culminated in the development of data protection policy across nations from a comparative perspective, much of the political science literature on the politics and policy of data protection focuses on particular aspects of policy analysis, specifically policy formation, implementation, and evaluation.

Public Policy Formation and the Competition between Ideas and Interests

The goal of data protection policy is to satisfy a highly subjective and elusive value, namely the right to privacy. In *Legislating Privacy*, Priscilla Regan examines policy processes in the areas of information privacy, communications privacy, and psychological privacy to understand how congressional politics in the United States resolved questions concerning fundamental values and technological change. In each of these areas, technological changes raised a number of policy issues that were initially defined by invasions of personal privacy. Regan's analysis is primarily concerned with examining the dynamics of congressional formulation and the adoption of policy in light of perceived threats, and she seeks to explain why the accepted understanding of the value of privacy did not receive more support for stronger legislation to protect privacy. Specifically, to demonstrate the problems with policy formation in the U.S., Regan examines the roles of 'ideas' and 'interests' in the formulation of privacy policy.

The role of ideas is important in the public policy process. How an idea is defined as an issue is critical to how that issue will be ultimately resolved. In the congressional and legislative process in the U.S., the issue was defined broadly as one of 'privacy'.⁶⁵ Defining the issue as 'privacy' has some obvious advantages, insofar as it provides a powerful symbol with broad public appeal. However, it is also problematic because protecting privacy entails costs to already defined interests, including the interests of government agencies. As such, interests, including government agencies, were concerned with redefining the issue from an idea of privacy to a different idea, such as one of 'efficiency'. In this process, as Regan notes, the politics of interests dominated, and the idea of privacy made it relatively easy to move from an emphasis on ideas to a politics of interests.⁶⁶

The main weakness of privacy as an idea is that it couches privacy in a language of individual rights, for example the right of an individual to control access to information about him or herself. This has two major consequences. First, privacy is taken as an 'individual utility'; if one has not experienced a privacy invasion, they will not likely consider it as particularly salient. Second, because privacy is taken as a 'right', it is not taken as an absolute. Thus, privacy must compete with other rights and social interests. The obvious result is a politics of balancing rights against competing social interests.⁶⁷

Regan suggests that although the idea of privacy initially framed the definition of the problem and set the agenda, it was primarily interests that dominated both policy formulation and adoption. The governmental changes that were introduced to address the applications of new technologies generated patterns of interests that were previously non-existent. Those who had a vested interest in the benefits of privacy invasive practices sought to define their interests and develop support for their positions. This meant that the policy issue could be redefined from one of privacy to one that was more consistent with their concerns.⁶⁸

⁶⁵ Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, Chapel Hill. 1995. p. 175.

⁶⁶ *ibid.*

⁶⁷ *ibid.* p. 178.

⁶⁸ *ibid.* p. 181.

There is an inherent difficulty in distinguishing between ideas and interests. Regan asserts that recognizing that ideas and interests work together can help in understanding the policy dynamics involved in the process.⁶⁹ As Regan explains,

The idea of privacy as the state of “being let alone” appears synonymous with self-interest; it does not elicit broader values. This individualistic idea of privacy does not *add* to self-interest; it merely restates it. But the ideas of government efficiency, effective law enforcement, and an honest work force provide a higher-order, or broader, rationale for the narrow self-interests of government bureaucrats, law enforcement officials, and employers.⁷⁰

If privacy is articulated in terms of self-interest, however, then it elicits the interests of the individual as a political motivator, making it difficult to employ ideas that are consistent with a broader purpose or meaning.⁷¹

Regan’s analysis emphasizes the evidence that privacy as an individual right or interest is a weak basis for formulating an effective privacy policy. If privacy is defined as an individual right, then policy formulations will require the balancing of the individual right to privacy against a competing interest or right, and this is often a social interest.⁷² Because this will tend to amount to competing claims between social and individual interests, the individual and their claim to privacy will have to defend their allegation that privacy has been invaded and that the ‘social’ benefit gained from the conflict of values is less important than the individual’s harm from the intrusion. This insight can also serve as a valuable insight for the understanding of privacy conflicts as well, because if one recognizes the sources and effects of the threat to privacy, then the notion of privacy can be considered from a social perspective rather than from an individual perspective.⁷³

In this sense, privacy is not only valuable to the individual as an individual, but it is also important to society as well. Regan suggests that there are three aspects of the

⁶⁹ *ibid.* p. 182.

⁷⁰ *ibid.*

⁷¹ *ibid.*

⁷² *ibid.* p. 212.

⁷³ *ibid.* The fact that surveillance practices using databases are not generally techniques used by individuals against other individuals is a case in point. As Regan notes, “(i)n modern society, then, privacy pertains to relations between individuals and corporate or government organizations as well as to relations among individuals. When these organizations are part of the public realm, privacy concerns cross the boundary between public and private.” p. 213

social importance of privacy. This includes privacy as a common value, privacy as a public value, and privacy as a collective value. As a common value, "some rights, which protect individual interests, are regarded as so fundamental that all individuals in common have a similar interest in them".⁷⁴ Even though individuals may define what they feel is their right to privacy in different ways, draw different lines between the public and private realms, and have varying degrees of sensitivity about what is known about them, they have a common interest in a right to privacy. This common core gives *social importance* to the right to privacy. Insofar as this observation is important for understanding why legislation may or may not be pursued, it is equally important for understanding what types of conflicts might receive the support of members of society to such an extent that they will take offense against the techniques of privacy-invading phenomena.

In the legal and philosophical analysis of privacy, a public value of privacy is deemed important for the exercise and fulfillment of other values. This relates to the notion of privacy as an 'instrumental' or 'strategic' value - having value as a means of achieving some other end. A public value of the right to privacy can be important for the exercise of other rights, such as values protected by the First Amendment in the United States, and other values protected in the constitutions of different nations. As Regan notes, the Supreme Court in the U.S. has upheld privacy interests such as 'associational privacy', 'political privacy', and the 'right to anonymity and public expression'.⁷⁵ Privacy in these cases is not considered as an independent right, but rather it was deemed important to protect other values protected by the First Amendment. As a public value, the social importance of privacy is also consistent with the liberal belief in limiting the powers of government, or more specifically, as restrictions on the arbitrary and capricious use of power.⁷⁶ Privacy in this sense is important to civil or social liberty in that it helps to establish boundaries for the exercise of power, and as such has value to the democratic system.

Finally, Regan asserts that privacy should be conceived as a collective value. The concept of a collective value that Regan employs has its roots in economists' conception

⁷⁴ *ibid.* p. 221.

⁷⁵ *ibid.* p. 225.

of collective or public goods, which are those goods that are defined as indivisible or non-excludable, meaning that an individual within society cannot enjoy the collective good without other members of society benefiting as well.⁷⁷ Most policies and policy proposals treat privacy as a 'private good', which provides individuals the opportunity to establish the level of privacy they desire.⁷⁸ This 'private good' conception suggests that privacy is in fact 'divisible' - one can choose the level of privacy pertaining to their information. However, treating privacy as a 'private good' is also problematic. Our information is often held by third parties where data on individuals is part of a record that is the property of the organization, not of the individual. This information is used and manipulated, and often commodified and sold to other third parties. Although individuals often have an opportunity to remove themselves from the market in the trade of information, few individuals have the time, energy, or adequate information to do so. In reality, the overwhelming majority of individuals are limited in their ability to control third party use of information.⁷⁹ Another way in which privacy can be seen as a collective, indivisible quality is that one cannot set the level of privacy that one requires. This is true of information collected and used by governments such as social security or tax records.⁸⁰ Finally, privacy can be seen as a collective good because of the inherent complexity and inter-relatedness of the communication infrastructure makes it very difficult to 'divide' privacy. In this regard, the level of privacy that is possible for an individual is dependent upon the hardware and software in the communication system. It is difficult to isolate one record from a system of records to give a particular record a level of privacy.⁸¹

⁷⁶ *ibid.*

⁷⁷ *ibid.* p. 227.

⁷⁸ For example, if an individual is concerned that an organization that they are dealing with does not provide the protections that they desire, as in the case of a direct marketing company selling personal information about an individual in a list, that individual may choose to 'opt out' of the distribution list to satisfy their privacy concerns.

⁷⁹ The third chapter of this thesis concerning the DoubleClick conflict considers this problem.

⁸⁰ The second chapter of this thesis concerning the conflict over the Longitudinal Labour Force File considers this dimension of the problem. This is also true to a large extent with regard to information held by credit or bank records. One may choose not to have a bank account or credit card to ensure their privacy, but this is unreasonable considering these types of institutional-individual relationships are necessary to function in modern life.

⁸¹ *ibid.* p. 230.

Thus, a common value in a right to privacy of personal information is possible by re-framing the right of information privacy as a social claim rather than as an individual claim.⁸² A consideration of the public value of privacy as a right of public access to information about themselves *rather* than as a right of individual access could be viewed as a public good because individuals could discover how government agencies and corporate interests are using personal information, which affects each member of society as a whole.⁸³ Finally, viewing privacy as a collective value could also generate significant changes in the types of policy that are considered appropriate to protect privacy.⁸⁴ Regan thus concludes that developing an appreciation for the social importance of privacy is important for gaining philosophical clarity about privacy, but perhaps more importantly, because the emphasis on privacy as an individual right has been a weak basis for formulating policy to protect privacy:

In policy debates about the marketing of consumer information.... The primary policy question does not involve what type of individual we want but what type of society we want, including concerns about the relationships between individuals and social/political/economic organizations and the powers these organizations have. If these social goals are the relevant policy goals, an understanding of privacy's importance to society is likewise relevant.⁸⁵

Regan's analysis of the social dimensions of privacy is an important contribution to the privacy literature. However, while her analysis highlights the inherent difficulty in gathering support for privacy protections because of the focus on privacy as an individual utility, it does not explicitly prescribe how the public, common, and collective values of privacy can be realized. In this regard, the analysis of privacy conflicts in this thesis will attempt to bridge this gap by exploring examples in which the social dimensions of privacy were exploited to achieve agenda-setting status.

Implementation and Evaluation

Regan demonstrates that interests can play a tremendous role in developing privacy legislation. However, as Charles Raab suggests, "legislation is one thing;

⁸² *ibid.* p. 232.

⁸³ *ibid.* p. 233.

⁸⁴ *ibid.*

⁸⁵ *ibid.* p. 242.

implementation is another."⁸⁶ Although aspects of the legal regime are of importance to how policy goals are achieved, the mere presence of legislation is an insufficient indicator of how privacy protection is actually carried out in practice. Raab's analysis of data protection in the United Kingdom is illustrative of a potential problem faced by implementation regimes: the data protection implementation strategy of Great Britain shifts attention from the *principles* and *ideas* that are established in the legislation, to the *instruments* and *institutions* that are created to implement and enforce the legislation.⁸⁷ As it is the case in other data protection models, the humanistic aspects of privacy take a back seat to a technocratic approach, and ideas fail to receive the attention they deserve.

Other analyses of the implementation process reveal similarly interesting lessons. Van de Donk and van Duivenboden also examine the implementation of data protection policy, and in particular, they are concerned with evaluating the level of data protection at the 'shopfloor level' in the Netherlands.⁸⁸ They observe that because the legislative regimes enacted to safeguard personal data are often considered symbolic laws, there has been little attention paid to the implementation and enforcement of these laws from a policy perspective.⁸⁹ Their primary concern is to consider whether their current legal data protection regime delivers a level of protection that is desirable, and assess to the extent to which other mechanisms can yield the type of data-use behaviour that the goal of data protection seeks to attain.

Van de Donk and van Duivenboden describe the Dutch Data Protection system, and focus on the results of a series of case studies that systematically explore, inventory, and analyze the factors and circumstances that hinder or facilitate the implementation of data protection.⁹⁰ They conceptualize successful implementation as meeting three criteria: 1) an adequate level of acceptance to implement protections; 2) an adequate preparatory introduction; and 3) an actual an enduring application of procedures, rules, and routines

⁸⁶ Charles Raab, "Implementing data protection in Britain". *International Review of Administrative Sciences*, vol. 62, no. 4. 1996. p. 497.

⁸⁷ *ibid.* p. 462.

⁸⁸ Wim B. H. J. van de Donk and Hein van Duivenboden, "Privacy as Policy: a policy implementation perspective on data protection at shopfloor level in the Netherlands". *International Review of Administrative Sciences*, vol. 62, no. 4. 1996. pp. 513-24.

⁸⁹ *ibid.* p. 515.

⁹⁰ *ibid.* p. 523. In particular, they examine six case studies which include organizations such as a hospital, a polytechnic, a bank, a social services department, a mail order firm, and the regional office of a tax authority.

that envisage the practice of data protection in accordance to the principles in the legislation.⁹¹ Their findings reveal that the Dutch implementation of data protection is only moderately obeyed at the shopfloor level. In fact, they argue that the level of protection expected by data-controllers and data-subjects is much more dependent on non-statutory factors, such as organizational self-interests, cultures which stress values like discretion and secrecy, dominant attitudes towards the value of data protection at management levels, compulsory administrative technology, a critical environment, data protection accidents, and a centrally directed design and organization of work processes.⁹² They conclude that a bottom-up perspective of data protection behaviour, that is from the shopfloor up, reveals that the *type* of data behaviour that is *desired* can be explained by these heterogeneous 'patchwork' factors and circumstances that are not even directly controllable by data protection law.

Analysis of implementation at the shopfloor level is important because it is at this level that the principles of the legislation must be recognized and translated into routines and behaviour for those involved in the collection processing and use of personal information on a daily basis. The authors conclude that in the Dutch case, meaningful and satisfactory fair information behaviour is implemented not only through recognized general and legal data protection regimes, but also via the use of specific instruments, institutions, and procedures that address specific characteristics of data processing and the appropriate points at which the application of data protection can control the desired behaviour of the different domains for the information society.

The conclusion that data protection is only moderately obeyed at the shopfloor level says something important about existing data protection regimes. If bureaucrats and specialized technocrats have had limited success in establishing the necessary components of an effective data protection strategy, then it is safe to assume that agents in the private sector with fewer resources devoted to data protection will face similar obstacles. In this regard, the quality of protection in both the public and the private sectors is likely less stringent and meaningful than is generally understood. If the level of protection that is anticipated is not achieved, then reliance on data protection standards to

⁹¹ *ibid.* p. 524.

⁹² *ibid.* p. 514.

protect privacy is less likely to be effective. This also raises the possibility that violations of privacy will more likely go unnoticed. In this sense, it is important to examine particular instances in which privacy issues do not receive the weight they deserve in order to identify trends and areas of concern so that we can learn from experience and prevent future violations from occurring.

Although much of the literature on policy evaluation is concerned with judging the ability and effectiveness of legislative regimes and policy instruments to satisfy particular policy goals, other analyses of evaluation have examined the desirability and usefulness of key concepts. For example, the notion that information privacy in both law and practice involves a 'balance' between competing values is a widely accepted contention. It is, after all, this notion of balance that provides for the safeguarding of privacy interests while also accommodating often equally important social, economic, or political ends. However, the difficulty in defining privacy, and moreover, the fact that privacy as a value does not take precedence over all uses of personal information often results in an under-emphasis of privacy costs that are amassed by the exploitation of one's personal information. Furthermore, the questionable boundary between a privacy claim and a competing interest makes data or information privacy protection as inherently a political or policy problem as other problems attended to inside and outside of government.

Charles Raab explores the notion of balance by questioning what balance means and what the notion might obscure or interfere with in the regulation of privacy. As Raab notes, these are important questions to raise "lest 'striking a balance' or 'getting the balance right', remains a *mantra* rather than a practical philosophy for decision-making in difficult circumstances where fundamental issue are at stake".⁹³

In the case of data protection, Raab argues that balancing comes down to a matter of locating an acceptable solution within a particular society or political system at a particular time, with due consideration of the configuration of the particular information activities.⁹⁴ This involves a recognition of the changing characteristics of technologies,

⁹³ Charles D. Raab, "From Balancing to Steering: New Directions for Data Protection", in Colin J. Bennett and Rebecca Grant, *Visions of Privacy: Policy Choices for the Digital Age*. University of Toronto Press, Toronto. 1996. p. 69.

⁹⁴ *ibid.* p. 73.

that an acceptable balance at one point in time or jurisdiction might not be sufficient at a different time or location, that it will likely involve interpreting rules and vague principles, and that there may be a number of competing perspectives as to how to best achieve the balance.⁹⁵ However, if the 'balancers' also have the task of serving as privacy 'watchdogs', then they must "bark and bite, not balance".⁹⁶

Raab points out that if the concept of balance is to be taken literally, then we are confronted with the task of determining whether or not some degree of parity actually exists between the values or interests that are being weighed. The problem is that this is not often possible, because the weighing of competing interests is a matter of judgement. The judgement however may be contentious and open to dispute over the weights that are distributed to the competing claims or that important considerations were overlooked. As such, the weight given to privacy in the balancing act in the political process is an important factor. Often privacy is not balanced against a competing right, but rather a convenient or desired policy or practice. Because the weighing of interests or values is socially, culturally, and politically constructed, the competing interest to privacy may often be outweighed by a more concrete value or interest in the public policy process. Disturbing the balance of privacy, however, in an attempt to move towards a higher level of privacy, might be possible through a combination of strategy and opportunism, that, as Raab notes, might be more akin to governing or steering.⁹⁷

The balancing process inherently includes a number of different stakeholders who participate in shaping the data protection landscape. This includes data users, regulatory organizations and officials, technology designers, pressure groups, and of course governments. Their different roles and backgrounds bring not only different values and interests, but also different positions of power that they hold in coming to avoid, produce, or resolve a conflict.⁹⁸ Within this balancing framework, different participants will act differently based on their assumptions about what *ought* to happen. Raab suggests that three modes of participation can be constructed as 'ideal types' that are capable of

⁹⁵ *ibid.*

⁹⁶ *ibid.*

⁹⁷ *ibid.* p. 79.

⁹⁸ *ibid.*

producing a conclusion that could be understood as achieving the balance. He terms these 'uncompromised pluralism', 'decentralized balancing', and 'negotiated balances'.

In the uncompromised pluralism mode, each participant seeks to maximize an objective, whether it is in the interest of privacy or in a competing interest. Achieving balance is not necessarily the goal of any of the participants, nor is it subject to decision. Rather, the balance is defined as the outcome. One might have an interest in advancing privacy goals, however they may have little power to exert their influence in the face of countervailing interests.⁹⁹ This mode does not produce a desirable outcome due to the fact that the weight of the interests of those who champion privacy interests would likely be outweighed by competing interests.

The second ideal type, 'decentralized balancing', also involves a collection of disparate actors and opinions, however in this mode, each participant weighs privacy interests against competing interests and internalizes a position that may be different from their original position. Here, for example, the users of data may take privacy concerns into consideration, and likewise, those who have an interest in privacy might consider the merits of the legitimacy and value of the uses of personal information for some end. Unlike in the uncompromised pluralism model, there is an opportunity for actors to exert their influence in exchange for personal trade-offs and compromises. Actors attempt to influence others by shaping the culture and climate of the attitudes of participants who weigh privacy against other values. In this scenario, for example, data regulators may influence database architects to 'build privacy in', or attempt to individually educate others on the consequences of using personal data.¹⁰⁰

In the third mode, 'negotiated balances', the balance amounts to a bargained outcome that takes into consideration the wide range of interests. Here, the resulting balance is based on the negotiation of solution in which the relationships are both interactive and structured and involve consideration of both privacy interests and the other interests. In this mode, pragmatism and flexibility can be extremely valuable in the bargaining process in which the actors are engaged.¹⁰¹ A balance, for example, may be

⁹⁹ *ibid.* pp. 80-81.

¹⁰⁰ *ibid.* p. 81.

¹⁰¹ *ibid.* p. 82.

struck where the conflict between privacy and data processing is achieved by offering privacy protection that facilitates data users rather than hindering them.¹⁰²

Raab suggests that there are a number of dangers in the balancing process. First, values and interests may not in fact be reconcilable, resulting in the inability of the actors to come to an acceptable solution. Second, there is the problem that balances could be 'struck' too easily, where the result is that privacy is traded off as a concession to managing surveillance, instead of restricting it. The outcome here amounts to not enough privacy. Third, there is the possibility that a negotiated balance seemingly offers a viable solution, but it cannot be implemented. Not only do outcomes depend on the attitudes and character of the actors involved, but they also depend on the "governability of highly complex, diverse, and dynamic situations, involving rapid developments in information and communications technologies and on the economic and governmental systems in which they are used."¹⁰³ This of course is highly problematic because regulators, when promoting privacy, are often also managing the task of implementing legislation where a balance between privacy and other objectives has already been struck. Furthermore, simply because a balance has been struck does not mean that there is a solution that can be easily found.¹⁰⁴

To achieve meaningful privacy protection, Raab suggests that regulators must move beyond the balancing paradigm towards a model that emphasizes steering as the essential component of the decision making process, where balancing serves as an instrument, rather than an outcome. Steering, as the metaphor suggests, rests on a conception of movement in a particular direction under the guidance of a privacy regulator who still balances, but balance in this sense connotes "throwing weight against built-in tendencies and moving towards a desired state of affairs".¹⁰⁵ This type of steering requires that there is a desired target or objective to achieve, and "an understanding of the boundaries within which a course must be steered and of what is actually occurring in the system, and ways of moving the latter closer to what is desired."¹⁰⁶ A steering approach, more than balancing, may also lead privacy regulators to more carefully consider the kind

¹⁰² *ibid.* p. 82.

¹⁰³ *ibid.* p. 83.

¹⁰⁴ *ibid.*

¹⁰⁵ *ibid.* p. 84.

of 'tool kit' they need and how to use it. They can also take advantage of the 'whistle blowing' functions that their regulatory position may entail, such as publicizing privacy conflicts and infringements in annual reports and in the media that can serve to send an effective signal to others to control their practices more effectively.¹⁰⁷

Raab's intention is not to reject the idea of 'balance', but rather to employ a more sophisticated conceptualization of the balancing dynamic. Thus, privacy regulators may employ a variety of mechanisms to steer policy, while using balancing language that personifies the limits to authoritative formal intervention.¹⁰⁸ By taking into consideration this enhanced theory of balancing, and by extension, applying the hypothesis to the case studies to be examined in the later chapters, this study of the dynamics of conflict may provide empirical evidence of the various ideal types of balancing. Furthermore, it can be determined whether or not the steering metaphor is accountable to the phenomena analyzed in the respective case studies.

Politicizing Privacy: Lessons from Activists

Although the issue of privacy has not been given much attention by political scientists beyond the analysis of public policy, political activists have been concerned with the issue of privacy for decades. In *"Spanners in the Works: How the Privacy Movement is adapting to Big Brother"*, Simon Davies traces the history of the modern privacy movement from the 1960's. Historically, privacy activism has responded to perceived threats with a number of strategies, ranging from institutionally organized activities to civil-disobedience and non-violent direct action, and embodying tactics ranging from intellectual expression to physical violence against technology.¹⁰⁹

Activism in the 1960's and 1970's shared similar features with activism within the environmental movement, including street marches, industrial sabotage, civil disobedience, etc. In recent years, privacy activism has evolved substantially in parallel with the movement to enact data protection regulations, with greater emphasis on and attention to technical rules governing the handling of information. As the privacy

¹⁰⁶ *ibid.* p. 85.

¹⁰⁷ *ibid.* p. 86.

¹⁰⁸ *ibid.* p. 89, 88.

movement became more mainstreamed in the 1980's, a number of organizations formed to advocate for privacy protections, either to respond to a general need for organization, or to oppose a particular issue of concern.¹¹⁰ In the 1990's with the growth of the Internet and rekindled ideas about sovereignty, state power, and autonomy, the privacy movement has redirected its focus to promote interests such as individual rights, freedom of expression, openness, and equal access. It has also been characterized by activism against encryption restrictions, and the promotion of privacy-enhancing technologies. Although these rights/activist groups encompass a wide range of traditional values, their campaign tactics have been limited, for the most part, to lobbying via electronic media.¹¹¹

A number of online campaigns have proved to be very successful in taking action in the interest of privacy rights. In 1994, a petition opposing the U.S. government's Clipper Chip wire-tapping proposal by Computer Professionals for Social Responsibility and EPIC collected in excess of fifty thousands signatures and significant publicity in a short period of time. Likewise, EPIC was also successful in coordinating an electronic email campaign against the Lotus Corporation for their plan to release a CD-ROM containing financial information on over a hundred million U.S. households. The company chairman received over forty thousands emails of protest in a matter of weeks, and promptly cancelled the product.¹¹² These cases provide clear examples of how privacy issues can attract considerable attention, and consequently how public concern over the issue of privacy can influence decisions to pursue a particular course of action.

Davies suggests that there are three clear trends emerging within the privacy movement. The first, and most significant, is a shift towards direct activism. The second is a trend towards hard-line, high standard lobbying techniques. The third is a trend towards amalgamation, with privacy groups increasingly working with environmental,

¹⁰⁹ Simon Davies, "Spanners in the Works: How the Privacy Movement is adapting to Big Brother", in Bennett and Grant, eds. *Visions of Privacy: Policy Choices for the Digital Age*. University of Toronto Press, 1999. p. 244.

¹¹⁰ *ibid.* p. 246. These groups include the United States Privacy Council, the Australian Privacy Foundation, Stichting Waakzaamheid Persoonregistratie (Netherlands), ArgeDaten (Austria), the Electronic Privacy Information Center, the Canadian Privacy Network, the New Zealand Privacy Foundation, Infophilia (Hungary), and Privacy International. Civil liberties groups such as the American Civil Liberties Union and the National Council for Civil Liberties in the United Kingdom were also active

¹¹¹ *ibid.* p. 251.

¹¹² See Laura J. Gurak, *Persuasion and Privacy in Cyberspace :The Online Protests over Lotus Marketplace and the Clipper Chip*. Yale University Press, 1997.

consumer, anarchist, and civil liberties groups.¹¹³ Davies suggests that these trends, which he conceptualizes as 'old wine in new bottles', reflect a number of tactics and principles of social justice movements of previous decades, and in particular, on strategies of resistance influenced by U.S. rights activist Saul Alinsky. In his final book, *Rules for Radicals*, Alinsky observed that "(t)here are no rules for revolution, any more than there are rules for love or rules for happiness, but there are rules for radicals who want to change their world; there are certain central concepts of action in human politics that operate regardless of the scene or the time. To know these is basic to a pragmatic attack on the system."¹¹⁴ As Davies notes, the rules have strong military parallels as well. These include:

- Information warfare and disinformation: Power is not only what you have, but what the enemy thinks you have.
- Wherever possible, go outside the experience of the enemy.
- Make the enemy live up to their own book of rules.
- A constructive alternative should always accompany a successful attack.
- Identify the target, isolate it, personalize it, and polarize it.¹¹⁵

Davies argues that the Alinsky factor is an indication of how the privacy movement has become more radicalized. Increasingly, focussed campaigns employing astute tactics, historical perspective, good contacts in media and politics, and a broadening knowledge of technology and law are ensuring that privacy concerns and campaigns are having an effect.¹¹⁶

John Westwood also reflects on the issues facing privacy advocates, and considers the extent to which the privacy problem can become more politicized. Westwood analyzes five case studies in which the British Columbia Civil Liberties Association (BCCCLA) played a role. These included the development of PharmaNet, a province wide medical prescription database, the video taping of police investigations for a television program, drug testing in the workplace, mandatory criminal record checks, and the data

¹¹³ Simon Davies, "The Challenge of Big Brother" p. 256.

¹¹⁴ Saul Alinsky, *Rules for Radicals*. New York, Vintage, 1971. As cited in Davies, p. 257.

¹¹⁵ *ibid.*

matching of welfare recipients.¹¹⁷ Although the success of the BCCLA's lobbying was met with varying degrees of success, Westwood shares a number of valuable lessons regarding the conditions under which privacy can be effectively politicized from the 'privacy trenches'. Westwood suggests that the only way that privacy can be preserved is if the costs of the use of surveillance technologies are greater than the benefits. This requires that the misuse of personal information by the public and private sector is illegal, and that an awareness about privacy invasions can be generated and translated into a political force. However, the former is not likely to transpire without evidence of the latter.

Westwood observes that it is difficult to get people motivated enough to protest or take political action over privacy invasions because of three constraining factors. The first is a lack of empathy.¹¹⁸ Few individuals are willing to protest against someone else's privacy being invaded, unless they can imagine themselves in the same predicament. A second constraint is that interests and values other than privacy are often considered more important, pressing, or powerful than the privacy interest. In this sense, as Regan suggests, it is important to present privacy interests as a positive, common good that benefits different aspects of our lives. Finally, the complex and abstract nature of privacy invasions often means that it is difficult to recognize the consequences of the invasion. In this sense, privacy issues that are simple, concrete, and immediate are most likely to influence people to protest.¹¹⁹

Westwood concludes that in order for privacy issues to be understood at a more concrete and immediate level, it is essential that images or icons be created to represent the problem. The use of images or icons, such as the 'Orwellian' concept of 'Big Brother' or 'Nineteen Eighty-Four' can portray the potentially harmful effects of invasions of privacy on individuals. The task for the privacy community is to develop fresh, meaningful images to illustrate the dangers inherent in the misuse of personal data. Although lobbying institutions, educating the media, and using the law to protect privacy

¹¹⁶ *ibid.* p. 259.

¹¹⁷ John Westwood, "Life in the Privacy Trenches: Experiences of the British Columbia Civil Liberties Association". *Visions of Privacy: Policy Choices for the Digital Age*. University of Toronto Press, 1999. pp. 231-243.

¹¹⁸ *ibid.* p. 240-241.

¹¹⁹ *ibid.*

rights are useful strategies for privacy activists, vivid and forceful images are necessary to communicate the more complex and far-reaching threats that challenge our privacy.¹²⁰

In this chapter, I have thus far reviewed the legal and philosophical origins of the concept of privacy. I have attempted to demonstrate that the way that privacy has been defined as a problem has influenced the kind of solution that could address the problem. The emergence of data protection as a legitimate field for policy analysis has been met with relative success over the past thirty years. However, as I have argued, the policy outcomes have reflected the narrow scope to which the problem was defined, though perhaps by necessity. Although the study of privacy issues has been dominated by lawyers, philosophers, sociologists, computer specialists and technocrats, it is clearly a political issue with political implications. While the issue has not been attended to much by political scientists, a number of important contributions to the study of privacy, including the examination of processes, the role of ideas and interests, the social importance of privacy, lessons learned about implementation, a more sophisticated articulation of the important concept of balance, and the role of activism and advocacy have enriched the broader privacy literature.

Many who have studied the privacy issue have noted that conflicts over privacy values can affect how the issue is defined and how interests respond to the conflict. However, there is little, if any, study of the actual dynamics of privacy conflicts. Generally, the literature does point to one conclusion about conflicts over privacy: privacy conflicts, when effectively publicized, can capture the imagination of the public at large. Because the privacy issue is one that holds much personal emotive appeal, the mass media has reported on privacy issues, albeit with a mixed degree of sensationalism. However, despite the public's concern over issues pertaining to privacy (as reflected in public opinion polls), the issue has rarely received much political attention in the past beyond the legislation of data protection statutes. Regan has demonstrated that this is likely attributable to the way the issue has been defined as an idea, and that those in power who have an interest in the problem have been able to influence the 'balance'. Nonetheless, a recent surge in interest about the privacy issue might mean that privacy is

¹²⁰ *ibid.* p. 241.

'an issue whose time has come'. To explore this notion further, I will now turn to a sub-field of policy analysis, namely, the study of agenda-setting.

Policy Analysis and the Dynamics of Agenda-Setting

Broadly speaking, public policy making can be considered to be a set of processes which include the setting of the agenda, the specification of alternatives from which a choice is made, an authoritative choice among the specified alternatives (such as a legislative vote or a decision by the head of state), and the implementation of a decision.¹²¹ According to Kingdon, the 'agenda' is "the list of subjects or problems to which government officials, and people outside of government closely associated with those officials, are paying some serious attention at any given time".¹²² For the purposes of this thesis, it is important to look at how the study of agenda-setting seeks to understand why some subjects are prominent on the agenda and others are not.

Whether or not there is a systematic pattern in which issues can become subjects for political action is of tremendous importance to students of public policy and to a wide range of policy actors inside and outside of government.¹²³ It is crucial for governments to recognize which issues are more likely than others to be successfully elevated from the social to the official agenda. As Cobb and Elder note,

Pre-political, or at least pre-decisional processes often play the most critical role in determining what issues and alternatives are to be considered by the polity and the probable choices that are made. What happens in the decision-making councils of the formal institutions of government may do little more than recognize, document and legalize, if not legitimize the monetary results of a continuing struggle of forces in the larger social matrix. . . . From this perspective, the critical question becomes, how does an issue or demand become or fail to become the focus of concern and interest within a polity?¹²⁴

A great deal of the agenda-setting literature has turned to an analysis of policy cycles to determine how an issue or demand comes to be the focus of concern of the government.

¹²¹ John W. Kingdon, *Agendas, Alternatives, and Public Policies*. (Toronto: Little Brown and Company) 1984. p. 3.

¹²² *ibid.*

¹²³ Michael Howlett, "Predictable and Unpredictable Policy Windows: institutional and Exogenous Correlates of Canadian Federal Agenda-Setting". *Canadian Journal of Political Science* XXXI:3 (September 1998). p. 495.

¹²⁴ Roger W. Cobb and Charles D. Elder, *Participation and American Politics: The Dynamics of Agenda-Building* (Boston: Allyn and Bacon, 1972) p. 12.

It is typical of the literature on the policy dynamics of agenda setting to suggest that policy issues wax and wane in public attention, which results in periodic and coherent patterns of governmental activity in particular policy sectors.¹²⁵ This perspective is representative of the early work on agenda-setting by Anthony Downs.

Downs view is that public policy making in areas of social life tends to revolve around specific issues that momentarily capture the attention of the public. Attention to these issues then results in demand for governmental action. When the complexity and inflexibility of the problems become apparent to the general public, they will fade away. As Downs notes,

American public attention rarely remains sharply focused upon any one domestic issue for very long - even if it involves a continuing problem of crucial importance to society. Instead, a systematic "issue-attention cycle" seems strongly to influence public attitudes and behaviour concerning most key domestic problems. Each of these problems suddenly leaps into prominence, remains there for a short time, and then - though still largely unresolved - gradually fades from the center of public attention.¹²⁶

Downs' work is one of the most often cited works in the agenda-setting literature, and the issue-attention cycle has garnered a great deal of scholarly attention. Despite this, the original hypothesis forwarded by Downs is vague. Downs argued that the problems that were most likely to be affected by the issue-attention syndrome shared three basic characteristics. First, they were problems that adversely affected a minority of the population. Second, they were problems that developed as side-effects of arrangements that benefited the majority of the public. Third, they were capable of creating dramatic moments of attention in the mass media, but these dramatic moments would not last for sustained periods.¹²⁷ These three characteristics combined would ensure that "most people will not be continually reminded of the problem by their own suffering from it; . . . solving the problem requires sustained attention and effort, plus fundamental changes in

¹²⁵ Michael Howlett, "Issue-Attention and Punctuated Equilibria Models Reconsidered: An Empirical Examination of the Dynamics of Agenda-Setting in Canada" *Canadian Journal of Political Science*, XXX:1 (March 1997) p. 4.

¹²⁶ Anthony Downs, "Up and Down with Ecology: the issue attention cycle". *Public Interest*, vol. 28, no. 1, 1972. p. 38.

¹²⁷ ¹²⁷ Michael Howlett, "Issue-Attention and Punctuated Equilibria Models Reconsidered: An Empirical Examination of the Dynamics of Agenda-Setting in Canada". p. 9.

social institutions and behaviour; . . . [and] the media's sustained focus on this problem soon bores a majority of the public."¹²⁸

When issues shared the three issue-attention characteristics in Downs' model, other key elements were clear. The key actors were the government and the public, and the relationship between them was one in which the government responded to the concern of the public. Both sets of actors were driven by self-interest: re-election for the politicians, and rational calculation by the public over what could be accomplished with limited political resources to address particular problems.¹²⁹

Given Downs' assumptions and issue characteristics, the expected result was that policy outcomes could be measured by a periodic, cyclical pattern of issue-attention, where public interest in an issue would peak and be followed by government attention. After the government attended to the problem, public interest would diminish, and so would government activity, until the next wave of public interest in the cycle would result in further government action. Arguably, Downs' theory of the issue-attention cycle is representative of the politics of privacy and data protection in North America. In the 1960's, the problems were identified, which was followed by renewed academic interest and public concern. This concern was then addressed by the development and implementation of data protection. Renewed concern in the 1990's over the increasing complexity of the issue also attracted renewed academic attention, and a new wave of public concern has drawn attention to the issue. Whereas government uses of information was the prime motivator in the past, this phase of the issue-attention cycle is predominantly concerned with the information practices of the private sector. However, Downs' theory is not particularly complex, and it does not speak to how specific issues capture the attention of the public. Furthermore, the issue of privacy, and in particular the phenomena that I will examine in the next two chapters is arguably of concern to a large sector of the public.¹³⁰

¹²⁸ *ibid.* Quote by Downs, as cited in Howlett.

¹²⁹ *ibid.*

¹³⁰ This appears to be the case in the conflict over the Longitudinal Labour Force File insofar as most Canadians were listed in the database. With regard to the DoubleClick case, it is true that the vast majority of Americans may not be concerned, as a large percentage of the population does not use the Internet. However, the reach of the case extends beyond the American border.

Baumgartner and Jones have developed a different model of agenda-setting that focuses on the significance of policy subsystem change for understanding policy dynamics. The underlying premise is that the process of agenda-setting involves discussion, debate, and persuasion among policy actors who present evidence to support their position and argument. The key element in the process of agenda-setting involves the creation of "policy monopolies" in which specific subsystems gain the ability to control the interpretation of a problem and consequently the way in which it is conceived and discussed.¹³¹ Governmental actors and the public are located in policy subsystems. The key relationship for analysis of US agenda-setting is between individuals and groups who are represented in subsystems or those who desire to be represented.

The "image" of a policy problem is significant because it will influence subsystem membership. "When they are portrayed as technical problems rather than as social questions, experts can dominate the decision-making process. When the ethical, social or political implications of such policies assume center stage, a much broader range of participants can suddenly become involved."¹³²

In this model, subsystem members attempt to alter policy images to undermine the stability of the policy subsystem. This can be done by changing the venue in which the policy debate occurs, or by altering other aspects of the policy discourse. The strategies adopted by groups generally fall into two types. In the Downsian strategy, groups publicize a problem in order to alter its venue by encouraging the public to demand the government to resolve the problem or take advantage of a new technology. In a second approach, which Baumgartner and Jones categorize as a "Schattschneider" mobilization, groups involved in the policy subsystem who do not agree with the policies developed or discussed by governments seek to change the institutional arrangements in which the subsystem operates to attempt to expand or contract its membership.¹³³

This behavior tends to result in a different pattern of policy outputs or results, however it is not cyclical like Downs' model. Instead, the outputs result in an irregular, stepped function that involves a "punctuated equilibrium" process where relatively long

¹³¹ Frank Baumgartner and Bryan Jones. *Agendas and Instability in American Politics*. Chicago: University of Chicago Press. 1993. p. 10.

¹³² *ibid.*

¹³³ *ibid.* p.11.

periods of policy stability are interspersed with infrequent periods of rapid change as issue images and venues, institutions and subsystems, are changed. As Baumgartner and Jones note,

When shocks or changes are introduced in this system, they may lead not just to a momentary deviation from normal, with a more or less rapid return to the status quo, but rather to new points of stability, as the system settles down at a point radically different from the original. If policy and politics can be said to follow such a dynamic, then we expect stability during certain periods, but with the possibility of rapid, dramatic and non-incremental change.¹³⁴

Although the Downsian 'Issue-Attention Cycle' and Baumgartner and Jones' work on 'Punctuated Equilibrium' contain a number of conceptual elements that are widely accepted in the policy literature, there has been little convincing empirical evidence to support their claims. I will now turn to examine John Kingdon's work on agenda-setting which is considered the standard in the policy studies literature.¹³⁵

One of the most pre-dominant theories of agenda setting in the public policy literature is John Kingdon's work on 'policy windows'. This model deals with the question of state and non-state influences on agenda-setting by examining the role of policy entrepreneurs inside and outside of government in taking advantage of agenda-setting opportunities. These opportunities are made possible when policy windows open and move items onto the formal government agenda. As Kingdon notes, "the policy window is an opportunity for advocates to push their pet solutions, or to push attention to their special problems."¹³⁶ Kingdon's windows are windows of opportunity that open when three separate 'streams come together' and are 'coupled.' The three streams are the 'problem stream', the 'policy stream', and the 'political stream'. I will return to the idea of the 'coupling' process after an examination of these streams.

Characteristics of the issues are identified as the 'problem stream'. Various mechanisms within this stream bring problems to the attention of governmental officials. These mechanisms include indicators, focussing events, and feedback. Indicators are used to assess the magnitude and change in a problem. Focussing events, such as disasters,

¹³⁴ *ibid.* Quote by Baumgartner and Jones, as cited in Howlett. p. 11.

¹³⁵ *Op Cit.* Howlett, "Predictable and Unpredictable policy Windows". p. 497.

¹³⁶ John W. Kingdon, *Agendas, Alternatives, and Public Policies*. (Toronto: Little Brown and Company) 1984. p. 173.

crises, personal experience, and symbols can play an important role in the setting of the agenda, however for this to happen a focussing event must be accompanied by a pre-existing perception that is reinforced, it must serve as a more influential indicator, or a combination of the two. Feedback provides important information including an assessment of current performance, an indication of a failure to meet a goal, or the suggestion of an unintended consequence.¹³⁷

Also of importance to the problem stream is problem definition. Kingdon makes the distinction between a 'condition' and a 'problem'. We deal with conditions every day. Conditions become defined as problems when it is believed that something should be done about them.¹³⁸ There is a great deal at stake in problem definition, as a problem's status may be helped or hindered depending on how it is defined. The process of fixing attention on one problem rather than another is a central component of the agenda-setting process.¹³⁹

Within the policy stream, proposals are generated, debated, redrafted, and accepted for consideration. Much of this proposal process takes place within a community of specialists. Communities are most effective when they are tightly knit. If a community is fragmented, the consequence might be the creation of disjointed policy, a lack of a common orientation, and/or agenda instability.¹⁴⁰

Ideas and proposals go through a process in which a wide number of potential initiatives are narrowed to a 'short list of ideas'. Reception to new ideas or proposals must go through a process of 'softening up'. Policy entrepreneurs are individuals who invest various resources in return for a policy in which they favor. To enhance their chance of survival, proposals must be technically feasible, meet the standards of the values of the members of the policy community including equity and efficiency, and be able to anticipate future constraints. Thus, the community produces a short list of ideas that meets the criteria of the community. Having a viable alternative facilitates the high placement of a subject on the governmental agenda, and it likewise dramatically

¹³⁷ *ibid.* pp. 95-108.

¹³⁸ *ibid.* p. 113.

¹³⁹ *ibid.* p. 121.

¹⁴⁰ *ibid.* pp. 121-126.

increases the chances for placement on the decision agenda.¹⁴¹ Consensus building often operates on persuasion.

The political stream operates independently of the problem and policy streams, and according to its own dynamics. The political stream is composed of factors such as the national mood, election results, changes of administration, changes of ideology or partisanship, and pressure by interest groups.¹⁴² Consensus building in the political stream relies less on persuasion than it does on bargaining.

When the problem stream, the political stream, and the policy stream combine at once in time, a policy window opens up and policy entrepreneurs may seize the opportunity to take advantage of the agenda-setting opportunity. Kingdon argues that the process of agenda-setting could best be conceived as a process in which more or less fleeting opportunities arose for issues to enter governmental debate. At the right place and time, policy windows could be seized upon by key players in the political process to provide an opportunity for particular issues to gain entrance to the agenda. Policy entrepreneurs assume a key role in that they are charged with the task of linking or 'coupling' policy solutions and policy problems with political opportunities. Although linking these streams is a necessary condition for issue entrance, more is required to get an issue to the agenda. Kingdon notes that although window openings are sometimes governed by accidental or incidental circumstances, such as a seemingly unrelated external "focussing event", crisis, or accident, other times they are affected by institutionalized events, like budgetary cycles or elections:

Sometimes windows open quite predictably. Legislation comes up for renewal on schedule, for instance, creating opportunities to change, expand or abolish certain programs. At other times, windows open quite unpredictably, as when an airliner crashes or a fluky election produces unexpected turnover in key decision-makers. Predictable or unpredictable, open windows are small and scarce. Opportunities come, but they also pass. Windows do not stay open long. If a chance is missed, another must be awaited.¹⁴³

¹⁴¹ *ibid.* p. 150. Kingdon distinguishes between the government and decision agendas as follows: the government agenda is the list of subjects that are getting attention, and the decision agenda is the list of subjects within the government agenda that are up for active decision.

¹⁴² *ibid.* p.153-163.

¹⁴³ *ibid.* p. 213.

Thus, windows are opened by events in either the problem stream or the political stream. When a new problem appears, there is a new opportunity to attach a solution to it. A well thought out and viable proposal developed in the policy stream increases the chances that a problem will rise to the decision agenda.

From a pluralist perspective, the definition of problems and the setting of the agenda is the outcome of a process of competition between different groups. Schattschneider argued that politics, as a conflict of values, interests, and beliefs was displaced by the management of conflict: "All forms of political organization have a bias in favor of the exploitation of some kinds of conflict and the suppression of others because *organization is the mobilization of bias*."¹⁴⁴ In this model, bias is mobilized to ensure that conflict is managed and contained. However, insofar as conflict can be contained, it can also be expanded. Cobb and Elder have suggested that the dynamics of issue expansion depend on five general characteristics:

- *The degree of specificity*- the more ambiguous an issue is defined, the greater the chance it will reach an expanded public
- *The scope of social significance*- the more socially significant the issue, the greater likelihood that it will be expanded
- *Temporal relevance*- the more that the issue is relevant over a long period of time, the greater chance it will be exposed to a larger audience
- *Degree of complexity*- the more that an issue is defined as non-technical, the greater chance it will be expanded to a larger public
- *Categorical precedence*- The more an issue is defined as lacking a clear precedent, the greater chance it will be expanded to a larger public.¹⁴⁵

Similarly, Cobb and Elder argue that issue expansion is confronted by strategies of issue containment. Strategies of containment involve two aspects that deal with groups and issues. These are:

- Group strategies focus on discrediting the contesting group, appeal above the heads of the leadership, and co-option of leaders

¹⁴⁴ Elmer E. Schattschneider. *The Semi-Sovereign People*. New York: Holt, Rinehart, and Winston. 1960, p. 71.

¹⁴⁵ Wayne Parsons. *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*. Aldershot, U.K.: Edward Elgar, 1995. p.128-129.

- Issue strategies focus on symbolic rewards and reassurance, showcasing or tokenism, creation of new organizational units, symbols of co-option, and feigned constraint.¹⁴⁶

Like the laws of physics, conflict in politics often follows a pattern of action, succeeded by an equal and opposite reaction. Like the forces of nature, there are also sources of resistance and acceleration that can affect the outcome of an action. The policy literature on agenda-setting acknowledges that focussing events, or events that are sudden, relatively uncommon, defined as harmful or revealing the possibility of harm, concentrated in a particular community of interest, and known to policy makers and the public simultaneously, can have a tremendous impact on the agenda-setting process. However without a critical event to inspire policy change, access to the agenda-setting process is rendered all the more difficult. It is thus a worthy venture to turn our attention to the focussing event, and consider how focussing events can be used to politicize privacy issues.

Focussing on Focussing Events

Although the issue of information privacy has never been a particularly salient political issue, people's concern over how their data is collected, used, and manipulated by governments and corporate interests has renewed interest in the topic.¹⁴⁷ Nonetheless, privacy remains an issue that receives little attention unless attention is directed to it. As Kingdon notes, there are a number of factors that contribute to an issue being considered a 'problem' that requires resolution rather than the issue being defined as a 'condition', and why government officials fix their attention on one problem rather than another. Privacy issues often capture the attention of a wide audience when there is a publicized conflict of values or a 'horror story' to attract attention. In the absence of a mechanism to draw attention to the privacy issue, individuals may be emotional about what privacy means to them, but they will not likely be so concerned as to pursue the issue to any great extent. The same can be said for the public officials who conduct the day to day operations of government. However, recent events involving conflicts over privacy values suggests that

¹⁴⁶ *ibid.* p. 129.

¹⁴⁷ This contention is based on results of a number of public opinion surveys regarding issues of privacy. See for example: Pew Internet & American Life Project. *Trust and Privacy Online: Why Americans Want*

when the problem is accompanied by an event that focuses attention on the problem, the issue has a significantly better chance of being politicized. A better understanding of the agenda-setting characteristics of focussing events and their dynamics in the policy process may serve as an invaluable tool to politicize issues concerned with information privacy. I will now turn to briefly consider the dynamics of focussing events.

The policy literature often makes mention of the agenda-setting influence of focussing events, however few policy studies systematically examine the dynamics of these events.¹⁴⁸ It is widely accepted that focussing events can be used as valuable tools to advance issues in the agenda and serve as 'triggers' for policy change.¹⁴⁹ Moreover, they are particularly interesting because focussing events are not politically neutral. They can represent tremendously important opportunities for politically disadvantaged groups¹⁵⁰ to articulate a message that has been suppressed by a dominant group or advocacy coalition. Thus, focussing events can be an important tool for groups seeking to influence of change policy.¹⁵¹

Because a focussing event is an event that is sudden, relatively uncommon, can be defined as harmful or revealing the possibility of harm, and attracts the attention of both policy makers and the public simultaneously, they can immediately highlight problems to which the government or other institutions might respond. Although the 'harms' are most often caused in a particular geographical area (such as a region or a nation), communities of interest are as important as geographically defined communities.¹⁵²

The increasing technical sophistication of the privacy community and the diligence of advocates have in many ways transformed the 'balance of power' with regard to privacy concerns. By investigating data architectures and producing technical audits of information systems, software applications, and data-use practices, a number of

to Rewrite the Rules. <http://www.pewinternet.org/reports/toc.asp?Report=19> ; Business Week / Harris Poll. *A growing Threat*. http://www.businessweek.com/2000/00_12/b3673010.htm

¹⁴⁸ Thomas A. Birkland, "Focusing Events, Mobilization, and Agenda Setting", *Journal of Public Policy*, vol. 18, no. 1. 1997. p. 53.

¹⁴⁹ Triggering mechanisms and focussing events have been examined by Baumgartner and Jones (1993), Cobb and Elder (1983), Kingdon (1984) and Walker (1977). Bennett examines the 'triggering mechanism' of the Watergate scandal to explain how an extrinsic set of circumstances served to precipitate policy action. *Regulating Privacy*, p. 237.

¹⁵⁰ By this I mean groups who normally would not have access to the political agenda.

¹⁵¹ Op cit. Birkland. p. 54.

¹⁵² *ibid*.

problematic privacy conflicts have become increasingly publicized in recent years. I have already mentioned the conflicts over Lotus Marketplace and the Clipper Chip, and other conflicts involving large technology corporations such as Real Networks and Microsoft have also garnered attention. These conflicts have generally been resolved quickly and quietly through the cancellation of the respective projects, policy change, or by modifying the ways in which the applications handle and manipulate personal information.

While political scientists have acknowledged the importance of studying the dramatic utility and impact of focussing events, privacy scholars generally have not. As such, this thesis attempts to fill this void. In the following two chapters, I will examine the dynamics of two recent focussing events that provided a means for the privacy issue to be elevated to the political agenda. But first, I will outline the organization of the chapters, and establish the parameters of the respective case studies.

Organization of the Case Studies

Two high profile privacy conflicts have recently attracted the attention of the public, the media, and a diverse range of interests, and made their way onto the political agenda. The first case concerns a privacy conflict in the public sector of Canada. The second case concerns a private sector Internet conflict. Both privacy conflicts are representative of the types of privacy problems faced by similar organizations in their respective sectors, and are paradigmatic of the threats that they pose to privacy. For each of the case studies, I will review the relevant policy landscape that establishes the rules for data processing in each jurisdiction, and explore the broader origins of the respective policy problems. I will then take a 'closer look' at the conflict, and highlight the privacy problematic. After the background conditions of the particular problem is explained, I will analyze the dynamics of the focussing events from the time of their first publicity to the time of the resolution of the conflict. I will then provide a brief summary of the immediate aftermath of the privacy crisis.

After examining the respective cases separately, I will compare the different processes or dynamics of politicization against one another, to highlight any relevant similarities and differences, and their conceptual convergences and divergences. Although the conflicts involve different sectors, states, regulatory environments, policy instruments,

and political cultures, they are fundamentally representative of larger privacy concerns. Thus a thorough examination of these cases might provide some interesting insights into the dynamics of conflict, and in particular, into the emergence of a new politics of privacy.

Chapter Two: The Politicization of the Longitudinal Labour Force File

Introduction

Perhaps the greatest perceived threat to privacy in the twentieth century has been the ability of nations to amass a considerable amount of sensitive personal information on its citizenry. Max Weber argued that the surveillance tendencies of the state have evolved out of the inherent tendencies of bureaucratic organizations to collect, organize, manipulate and control information in the form of files and in the quest to achieve efficiency. These files contain personal information on the subjects of the state to ensure that organizations, and in particular the government, can keep tabs on the citizenry. For Weber, modern organizations are characterized above all by their *rationality*.¹⁵³ Within the bureaucracy, all activity is geared towards making carefully calculated decisions. The result is the accumulation of specialized knowledge that increases the power of the agency. The more that the organizations can claim a monopoly on the specialization of knowledge, the greater their opportunity to compose a clearer portrait of individuals private lives. Furthermore, the more that certain categories and classifications are imposed on individuals (for example classifications of health or economic risks) the greater the distinctions that are made between what is considered acceptable and unacceptable behaviour. This in turn serves to define what is meant by 'normal' or 'average', 'citizen' or 'dissident'. Rationalization involves the application of method for the pursuit of identifiable goals. In this sense, the rationalization of the bureaucratic system defines rules and standards as rational, fair, or impartial, and as such acts as a social control. One of the ironies of this rationalization is the production of the 'subject', which actually creates an object to be further objectified by the bureaucratic organizations of the state.

In this Weberian sense, the loss of privacy is representative of the modern state's insatiable desire to collect any information that will improve upon the bureaucracy's ability to operate efficiently. But what are the limits of bureaucratic efficiency, and at what point does the individual's right to privacy trump the government's requirement of

¹⁵³ Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press, Boulder, 1993. p. 38.

information? In this chapter, I will examine a privacy conflict in the Canadian public sector that is concerned with this problem. I will begin by setting the context of the conflict, examining the regulatory environment, the origins of the policy problem, and the inherent privacy problematic. Following this, I will examine the specific conflict over the Longitudinal Labour Force File, identifying the key arguments and perspectives, the public debate, the political debate, the role of the media, and the role of the various interests throughout the conflict. I will now turn to explore the policy landscape in Canada.

The Policy Landscape and the Privacy Problem

The Policy Landscape in Canada

Canada was among the handful of advanced industrial nations that enacted privacy legislation in the 1970's to address the increased capabilities of organizations to collect, store, manipulate, and disseminate large volumes of personal data. The first privacy legislation enacted at the federal level was contained within Part IV of the 1977 Canadian Human Rights Act.¹⁵⁴ This legislation established the office of the Privacy Commissioner as a member of the Canadian Human Rights Commission, and institutionalized the responsibilities of the Commissioner to receive complaints from the general public, to conduct investigations, and to make recommendations to parliament.

Part IV of the Human Rights Act also codified a set of fair information principles in Canadian legislation for the first time. These principles were established to ensure the following: that the existence of record-keeping systems for personal information should be publicly known; that individuals should have rights of access and correction to their own information; that personal information should only be collected for legitimate and openly stated purposes; that personal data should only be used (internally) in ways that are consistent with those purposes; that personal data should only be disclosed to other organizations in ways that are consistent with those purposes - unless the individual consents; and that there should be adequate and appropriate security safeguards to

¹⁵⁴ Previous legislation, notably the Privacy Act of 1974, was concerned with addressing issues of privacy pertaining to communications, and in particular wiretapping.

prevent unauthorized access or disclosure.¹⁵⁵ Unlike many industrialized countries with modern constitutions, there is no right to privacy in the Canadian Constitution and Charter of Rights and Freedoms. However, section 8 of the Charter which codifies the right to be secure against unreasonable search and seizure has been interpreted by Canada's courts as recognizing an individual's right to a reasonable expectation of privacy.¹⁵⁶

In the early 1980's, the importance and significance of personal privacy protection was thought to be misplaced and overshadowed within the Human Rights Act, an act that was concerned with and devoted to questions of discrimination.¹⁵⁷ At the same time, there was an increase in political pressure to develop a set of standards that would govern access to information held by federal agencies.¹⁵⁸ Canada sought to develop a more comprehensive privacy policy that would govern the use of information by the federal government. The 1982 *Privacy Act* flows from the contention that the protection of personal information should be a corollary to freedom of information and that the various exemptions in both pieces of legislation should be consistent. The introduction of Bill C-43 (*An Act to enact the Access to Information Act and the Privacy Act*) incorporated the Access to Information Act and a Privacy Act, and consequently institutionalized the Canadian innovation of legislating access to information and the protection of privacy within the same statutory framework.¹⁵⁹

¹⁵⁵ Colin J. Bennett and David J. Todd. "Data Protection Policy in Canada". *Mathew Bender's International Computer Law*. 1999.

¹⁵⁶ David Banisar and Simon Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments". *The John Marshall Journal of Computer & Information Law*, Volume XVIII, Number 1. Fall 1999. p. 27.

¹⁵⁷ Bennett, Colin J. "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing." *Canadian Public Administration*, vol. 33, 1990. p. 559.

¹⁵⁸ These debates raised questions about the inherent compatibility between Freedom of Information legislation and the privacy standards enacted within Part IV of the *Human Rights Act*. The Progressive Conservative government of Joe Clark put "considerable pressure" on the Department of Justice and the Privy Council Office to produce access to information legislation, and this initiative provided an opportunity to revise Part IV of the Human Rights Act. See Flaherty, *Protecting Privacy in Surveillance Societies*, p. 245.

¹⁵⁹ The practice of legislating both policy areas within one statute was later copied by the provinces: by Quebec in 1982, by Ontario in 1988, by British Columbia in 1993, by Alberta in 1995, and by Manitoba in 1997. Each of these information privacy statutes have converged based on a common set of fair information principles. All provinces now have privacy legislation governing the public sector. Quebec is the only province that has enacted legislation governing the use of information by the private sector. The development of Bill 68 in 1993 (the *Act Respecting the Protection of Personal Information in the Private Sector*) put into effect information privacy rights that are incorporated into the Quebec Civil Code and

The Privacy Act is overseen by an independent Privacy Commissioner of Canada, and the Office of the Privacy Commissioner is the primary supervisory mechanism for the protection of personal data.¹⁶⁰ The Commissioner has two primary sets of powers. These include the power of disclosure, which is the right to make information public, and the power to take matters to the Federal Court of Canada, which can in turn order organizations to stop a particular practice, and can award substantial damages for contravention of the law.

The privacy work however is on the whole more advisory. All privacy commissioners are primarily "Ombudsmen" whose principal duty is to receive and investigate complaints. The federal Privacy Act, for example, specifies in considerable detail the procedures and powers for receiving, investigating, and reporting the results of complaints. Much of the work is therefore reactive, and commands a significant amount of the office's often-limited personnel and resources.

Privacy commissioners also conduct investigations and audits of government departments. These may be part of a formal audit program, or based on more ad hoc "site visits" to public bodies. In this capacity, commissioners and their staff serve more as "consultants" than "investigators". These activities can often lead to special reports on practices and technologies that have privacy implications. For example, reports on AIDS¹⁶¹, drug testing¹⁶², and genetic testing¹⁶³ have been prominent at the federal level. Other shorter fact sheets are often released from time to time, to provide guidance to agencies about their responsibilities and education to the general public about their rights. Information and Privacy Commissioners are also obliged to file an annual report on their activities.

Commissioners are also authorized to comment on the privacy implications of pending legislation and other initiatives. The privacy commissioners constantly try to

made Quebec the first North American jurisdiction to produce and adopt a set of comprehensive data protection rules for the private sector.

¹⁶⁰ The Privacy Commissioner has a website at www.privcomm.gc.ca

¹⁶¹ Privacy Commissioner of Canada, *AIDS and the Privacy Act* (Ottawa: Minister of Supply and Services, 1989).

¹⁶² Privacy Commissioner of Canada, *Drug Testing and Privacy* (Ottawa: Minister of Supply and Services, 1990).

¹⁶³ Privacy Commissioner of Canada, *Genetic Testing and Privacy* (Ottawa: Minister of Supply and Services, 1992).

inject a privacy perspective at the earliest stages of the legislative process, technology development, or service delivery. High-profile legislative changes that involve radical implications for the processing of personal information are often the circumstances under which consultation is the most serious; examples would be the proposed DNA data bank¹⁶⁴ or the permanent voters' register.¹⁶⁵ Developments such as these have been typically attended by significant media interest. On other occasions, however, privacy commissioners complain that privacy protection is a last minute "add-on" and that their staff are not consulted early enough in the policy development process.

The Privacy Commissioner is also responsible for developing and conducting information programs to foster public understanding of the powers of the office, the duties of the Commissioner, and the rights of data subjects. In this capacity, the Commissioner may undertake and publish research that is related to the protection of personal information, encourage organizations to develop detailed policies and practices (including organizational codes of practice), and to promote by any means the Office of the Privacy Commissioner and the purposes of the Act that fall under the powers of the Office. The Commissioner may also make public any information relating to the personal information practices of an organization if the Commissioner considers the matter to be of public interest. In difficult cases concerning governmental surveillance, the balancing of competing interests returns to the political arena.¹⁶⁶

On January 1, 2001, privacy legislation concerning the private sector came into effect. The *Personal Information and Electronic Documents Act* establishes rules that govern the collection, use and disclosure of personal information in the private sector.¹⁶⁷ The legislation adopts a phased in approach¹⁶⁸ and establishes rules for the management

¹⁶⁴ Privacy Commissioner of Canada, *Annual Report 1994-95* (Ottawa: Canada Communications Group, 1995). p. 19.

¹⁶⁵ Privacy Commissioner of Canada, *Annual Report 1995-96*. (Ottawa: Canada Communications Group, 1996). p. 47.

¹⁶⁶ Flaherty, *Protecting Privacy in Surveillance Societies*. p. 243.

¹⁶⁷ The *Personal Information Protection and Electronic Documents Act* was first introduced in the House of Commons in October 1998 as Bill C-54. It was re-introduced as Bill C-6 in October 1999 at the opening of the Parliamentary session. The Senate later passed the bill with two amendments pertaining to personal health information. Parliament approved the amendments, and the Act received Royal Assent on April 13, 2000.

¹⁶⁸ Beginning January 1, 2001, the law applies to Federal works, undertakings or businesses, such as banks, telecommunications companies, airlines, railways and inter-provincial trucking companies, and to the employee records in those organizations. It also includes personal information disclosed across borders for

of personal information by organizations involved in commercial activities. The *Act* attempts to strike a balance between an individual's right to the protection of personal information and the needs of organizations to obtain and use information for legitimate business purposes. Perhaps the most significant achievement of the private sector privacy legislation is that it contains a set of fair information principles that are rooted in international data protection standards and are based on the Canadian Standards Association's Model Privacy Code for the Protection of Personal Information. The CSA Model Code was developed with input from businesses, governments, consumer associations and other privacy stakeholders.¹⁶⁹

Now that I have reviewed the regulatory environment in Canada, I will turn to explore the origins of the policy problem. But first, I will begin with the Privacy Commissioner's initial public announcement of the privacy problem at hand.

The Privacy Alarm

On May 16, 2000, the Privacy Commissioner of Canada issued a News Release announcing the publication of the Privacy Commissioner's Annual Report for 1999-2000. The Release, entitled "Looking back, moving forward" boldly asserted that "Canadians should be concerned about the existence of a *de facto* citizen profile containing as many as 2,000 pieces of information about each of more than 30 million Canadians".¹⁷⁰ This "extraordinarily detailed database", called the 'Longitudinal Labour Force File' is operated by Human Resources Development Canada and is used for research purposes. However, the scope and magnitude of the database is a cause for concern and represents a potential threat to the privacy of the Canadian public. As Commissioner Phillips noted, "Successive Privacy Commissioners have assured Canadians that there was no single

consideration (e.g., the sale or lease of lists). On January 1, 2002, the law will apply to personal health information collected, used or disclosed by organizations described under phase one of the law. On January 1, 2004, the law will apply to the collection, use and disclosure of personal information by any organization in the course of commercial activity within a province. It will also include all personal information in all inter-provincial and international transactions by all organizations subject to the Act in the course of commercial activities.

¹⁶⁹ See the Canadian Standards Association's *Model Privacy Code for the Protection of Personal Information* at http://www.csa-international.org/english/product_services/ps_privacy.html

¹⁷⁰ Privacy Commissioner of Canada, *News Release*: "Looking back, moving forward: the Privacy Commissioner releases his 1999-2000 annual report". OTTAWA, May 16, 2000.

federal government file, or profile about them. We were wrong - or not right enough for comfort."¹⁷¹

Origins of the Policy Problem: The Creation of HRDC

In 1998, the Privacy Commissioner's Office dedicated the bulk of its available compliance resources toward a comprehensive audit of the information handling practices of the Department of Human Resources Development Canada (HRDC). The decision to audit the Department of HRDC had its roots in a previous government reorganization, in which HRDC assumed a number of responsibilities and integrated an array of new programs. HRDC was officially created by Bill C-11- *The Department of Human Resources Development Act*, which came into force on July 12, 1996.¹⁷² From November 1993 to the enactment of Bill C-11, HRDC had been operating under a series of Memoranda of Understanding involving various components of the founding departments, including Employment and Immigration Canada, Health and Welfare Canada, Labour Canada, Secretary of State and the Department of Multiculturalism and Citizenship. When C-11 took full force, HRDC assumed the duty and mandate to deliver a wide range of programs and services. This included the absorption of market adjustment programs in response to the phasing out of Labour Canada, the transfer of social and income security programs from the defunct Health and Welfare Canada, a number of social development and education programs from the Secretary of State Department, as well as Unemployment Insurance and labour market programs from Employment and Immigration Canada and the Canada Employment Insurance Commission.¹⁷³ In the process of this re-structuring, HRDC became the federal government's largest repository of personal information on Canadian Citizens. As such, the decision to audit HRDC on their compliance to the Privacy Act, given the amalgamation of departments, programs, and services, was thus both sensible and obvious.

HRDC's primary objectives are to help Canadians prepare for, find and keep work, to assist Canadians in their efforts to provide financial security for themselves and

¹⁷¹ *ibid.*

¹⁷² <http://www.hrdc-drhc.gc.ca/menu/profile-hrdc.shtml>

¹⁷³ *ibid.*

their families, and to promote a fair, safe, healthy, stable, cooperative, and productive work environment. In meeting these objectives, HRDC is responsible for maintaining and delivering Employment Insurance Programs (such as Employment Insurance), Human Resources Investment Programs (such as Canada Student Loans), Income Security Programs (such as Canada Pension Plan and Old Age Security), as well as National Labour-related activities (such as the Canada Labour Code).¹⁷⁴ The end result has been the adoption of an enormous clientele, an equally massive budget for operations, and a vast and comprehensive collection of personal data on virtually every Canadian citizen.

The magnitude of the tasks and responsibilities bestowed upon the Department of HRDC has unsurprisingly exerted pressures on the department to deliver a wide range of programs, to improve any problems with existing programs, and to eliminate fraudulent activity by the users of the services. To deliver and administrate the departments programs, HRDC relies heavily on information technology to deliver, monitor, and assess their programs and services.¹⁷⁵

Although the development of advanced information technologies can increase bureaucratic efficiency in the administration and delivery of services, often issues relating to the privacy of information are not taken into consideration, or the benefits of the efficiency are perceived to outweigh the costs of protecting privacy. HRDC, with massive databases containing personal information, a powerful configuration of computer systems and network infrastructure, combined with increasing communication and data sharing between the federal government, provincial social programs, and private sector organizations who subcontract service delivery, make it among the most information intensive departments in all of government. Thus, in 1998, the Office of the Privacy Commissioner conducted an audit into the information handling practices of HRDC. The Commissioner's audit began with an informal, but systematic review of HRDC from which it assembled a profile of the department.¹⁷⁶ They identified the Department's information handling practices, including the information collected by HRDC and the purpose for its collection, how the information 'flowed' through HRDC, and examined

¹⁷⁴ www.hrdc-drhc.gc.ca/menu/profile-hrdc.shtml

¹⁷⁵ Privacy Commissioner. "ANNUAL REPORT 1999-2000". <http://www.hrdc-drhc.gc.ca/menu/profile-hrdc.shtml>

¹⁷⁶ *ibid.*

and identified the subsidiary uses of the information, how it was shared, and how the data was retained. Once the review of HRDC's practices was completed, the Privacy Commissioner's Office concentrated their efforts at further investigating HRDC activities and practices that put the privacy of the departments clients most at risk. The privacy-invasive characteristics of two particular projects by HRDC justified further investigation. These were the Common Client Identifier Project and the Longitudinal Labour Force File.¹⁷⁷

The Audit of the Longitudinal Labour Force File

The Longitudinal Labour Force File (LLFF) is a database that was created by HRDC's Strategic Policy Branch for research purposes, evaluation, policy and program analysis to support services and programs operated by the department. It is an extremely comprehensive database, containing information on more than 33.7 million individuals. The data on individuals in the LLFF is drawn from a wide range of separate and dispersed internal and external government files from varying time periods. Furthermore, the information that is inputted into the LLFF is never purged. As such, there are more records in the tables and fields of the LLFF than there are citizens in Canada. The Privacy Commissioners Office views the Longitudinal Labour Force File as "the next thing to a citizen profile".¹⁷⁸

The Longitudinal Labour Force file is operated by the Data Development & Technical Services group in the Strategic Policy Branch of HRDC.¹⁷⁹ Using personal identifiers, data on individuals is extracted from federal departments and from other levels of government. To ensure that the information in the LLFF is as current as possible, it is updated frequently by the Data Development & Technical Services group. The data integrated into the LLFF is drawn from files in a number of federally administered programs, including:

- T1- Income Tax Returns and T4-S and T4-F forms issued for income tax purposes;

¹⁷⁷ *ibid.*

¹⁷⁸ *ibid.*

¹⁷⁹ The Data Development and Technical Services Group develops and manages data systems and frameworks to support HRDC policy and program analysis, research and evaluation, and provides informatic services to Evaluation and Data Development Branch. See http://www11.hrdc-drhc.gc.ca/edd/vweb_medd.info?subs=DDTS

- Child Tax Benefits
- Immigration and Visitor files (from EIC - 1993 or earlier)
- Provincial and Municipal Welfare Files
- National Training Program
- Canadian Job Strategy
- National Employment Services
- Employment Insurance Administrative
- Record of Employment
- Social Insurance Master File¹⁸⁰

In addition, there have been proposals by the Strategic Policy Branch to expand the database to also include information on social assistance recipients from additional provinces and territories, and to use data from the Canada Student Loan Program, the Canada Pension Plan, and the Old Age Security Program.¹⁸¹

Upon the completion of the informal audit process conducted by the Privacy Commissioner's Office, the Privacy Commissioner Bruce Phillips wrote to HRDC to address his concerns about the Longitudinal Labour Force File. The Commissioner acknowledged that the Longitudinal Labour Force File amounted to a permanent and comprehensive invisible citizen profile. This began a steady exchange of letters and telephone calls between HRDC and the Privacy Commissioner's Office.¹⁸² Over the course of this correspondence, the Commissioner outlined the problems inherent in the Longitudinal Labour Force File.

The Privacy Problem

The problems with the LLFF database are extensive. The first concerned the comprehensiveness of the database. The LLFF is extraordinarily detailed, as it contained up to as many as 2000 'elements' or bits of data. This includes information on individuals such as their education, marital/family status, language, citizenship and landed immigration status, ethnic origin, mobility, disabilities, income tax data, employment histories, labour market activities, use of social assistance programs and Employment

¹⁸⁰ See Info Source, Human Resources Development Canada Personal Information Banks: Sources of Federal Government Information 1999-2000. http://dsp-psd.pwgsc.gc.ca/InfoSource/Info_1/HRDC-PB-e.html

¹⁸¹ Op cit. Privacy Commissioner's *Annual Report, 1999- 2000*.

¹⁸² The Privacy Commissioner's Office first sent a letter in July of 1998. The correspondence continued through until Feb. 9, 2000, when the Privacy Commissioner first threatened to publish his findings in the Annual Report.

Insurance. The centralization of such sensitive and detailed personal information and the continued integration of updated personal data on almost every living citizen (and a large number who are deceased) is certainly problematic and poses significant risks to the privacy of Canadian citizens.

The second significant problem with the Longitudinal Labour Force File is its relative invisibility. Although HRDC describes the database in InfoSource¹⁸³ and on its website, the descriptions of the LLFF are not widely read or publicized, it is not easily understandable, and the description of the database is not especially detailed. Individuals do not know the frequency or amount of information that is collected about them, nor are they aware of the extent to which it is integrated with other information and shared with others. For example, the vast majority of individuals would likely be concerned that their financial and tax information is stored in an HRDC database. Furthermore, HRDC can supply this information to research firms in the private sector under contract for program planning, statistics, research, and the evaluation of programs.¹⁸⁴ The data in the LLFF can also be given to researchers and academics at non-governmental organizations such as Universities who conduct research on the labour force, the labour market, or similar research in a related field.

A third problem with the LLFF is its permanence. HRDC's data retention policy is to never purge the database. The Longitudinal Labour Force File consists of roughly 33.7 million files, which amounts to roughly 3.3 million more files than the 30.4 million estimated population of Canada. This practice of retaining all of the information in the database without pre-defining the parameters for the length of time that the data will be stored goes against privacy 'best practices'.

The fourth significant problem with the LLFF is that there is no legal protective framework to legislate standards or provide penalties for misuse beyond the Privacy Act. Statistics Canada, Canada's foremost statistical agency, operates under additional stringent legislation that governs a number of information practices within its department.¹⁸⁵ The Statistics Act includes penalties against misuses of personal data that

¹⁸³ See Government of Canada Info Source, http://dsp-psd.pwgsc.gc.ca/InfoSource/Info_1/HRDC-PB-e.html

¹⁸⁴ Op cit. Privacy Commissioner's *Annual Report, 1999-2000*.

¹⁸⁵ See Section 17 of the Statistics Act, <http://www.statcan.ca/english/about/statact.htm>

is used for research and statistics. There is no legislative protection for the HRDC research databases.

The Privacy Commissioner's Audit of the Longitudinal Labour Force File concluded that HRDC's compilation of longitudinal records by linking records or matching data poses a serious hazard to information privacy "because of the temptation for government to use the information for data mining and individual profiling"¹⁸⁶. The use of such a research database could lead to other purposes for using the information, and fears that the government might use this information to make decisions or predictions about individuals are not far outside the realm of possibility. A further potential privacy threat is that information could be retrieved and used for purposes that were unanticipated, such as accessing particular information by disability or by ethnic origin. In fact, in the recent past, HRDC launched the Service Outcome Measurement System project that was to use research data from the Longitudinal Labour Force File for program investigation and evaluation.¹⁸⁷

The Internal Debate Between HRDC and the PCO

The concerns of the Privacy Commissioner's Office (PCO) over the Longitudinal Labour Force File were first addressed to HRDC in September of 1998. The Privacy Commissioner made repeated attempts to address the problems. In particular, the Commissioner made a number of recommendations to HRDC, including: that HRDC establish a fixed retention span for the data in the LLFF; that penalties are introduced and sanctions established for the misuse of information; to ensure that research data is not used for program administration; that HRDC establish strict controls and data protection safeguards on its collection, use and retention of any personal information used for research and evaluation; and that they incorporate a clear purpose-specific research mandate in its enabling legislation.¹⁸⁸

After the Privacy Commissioner released the audit findings, HRDC conducted its own review of the Longitudinal Labour Force File. The internal review focussed on the size of the database and examined the indirect method in which information is gathered

¹⁸⁶ Op cit. Privacy Commissioner's *Annual Report, 1999-2000*.

¹⁸⁷ *ibid.*

¹⁸⁸ *ibid.*

for the long file. They also investigated if or how individuals were notified about secondary uses of information held in the database, and considered the department's policy regarding the retention of data.¹⁸⁹

HRDC continued to defend the Longitudinal Labour Force File and concluded that their department's policies and procedures were adequate. With regard to the size of the database, HRDC suggested that all of the data that it uses and collects is imperative to develop their policies, manage the effectiveness of its "interventions", and to improve programs and the delivery of services. In responding to the Privacy Commissioner's accusation that the collection of information is 'speculative', HRDC argued that "from a pure business perspective, it would not be effective for HRDC to collect and maintain information that is not useful".¹⁹⁰ They argued that any effective and credible evaluation of the "labour market and social policy analysis must take account of a daunting array of factors" and that the information needed to be "disaggregated" to target specific groups and areas to assess the impact of their programs on groups and individuals.¹⁹¹ Furthermore, in responding to the concerns of the Privacy Commissioner's Office over the lack of a legal protective framework, HRDC argued that all of the information that they use is either related to their operating programs or else it can be disclosed by other departments under their own legislation, and as such it is permissible under the Privacy Act.

In responding to the Privacy Commissioner's claim that HRDC should establish strict controls on the collection, use, and retention of information, HRDC argued that they are required to collect information directly from the individual only when they intend to use it for an administrative purpose, as in the case when they make a decision that directly affects a person. Because the LLFF is not used for that purpose, they concluded that the direct collection of information is not required.¹⁹² Furthermore, HRDC insisted that because the Privacy Act only requires that information be collected directly "whenever possible", Parliament has authorized indirect collection when "it would not be possible to obtain the information directly from the individual". In addition, HRDC

¹⁸⁹ *ibid.*

¹⁹⁰ *ibid.*

¹⁹¹ *ibid.*

¹⁹² *ibid.*

points to section 8(2) of the Privacy Act that states that departments may disclose information if the disclosure is for research.¹⁹³ HRDC also states that they do not need to inform individuals about the collection of information because the Privacy Act requires federal institutions to "inform the person from whom they collect personal information".¹⁹⁴ Because HRDC uses information that is collected from another organization and they do not use the information to make decisions about an individual, they insisted that they do not need to notify individuals. HRDC also observed that the Privacy Act does not address retention limits on research databases. The department rejected the criticism that there should be strict controls on the retention of data, arguing that they need to analyze the data through different market cycles and have a mechanism to assess the impact of variables such as free trade, technological change, and market globalization.¹⁹⁵

Finally, in responding to the Privacy Commissioner's recommendation to incorporate a clear purpose-specific mandate in its enabling legislation, HRDC argued that a combination of the existing legislation and HRDC's internal policies provided adequate protection for the personal information held in the LLFF.¹⁹⁶ HRDC noted that information in the database is masked and that access to the unmasked data is limited. They did concede however that there are fewer penalties in place for the misuse of data than under the Statistics Act and the Income Tax Act, but staff professionalism and internal policies were sufficient to guard against any potential misuses.

In the time since HRDC originally responded to the Privacy Commissioner's recommendations, they agreed to limit the retention time of data to 25 years, tighten access to the data in the LLFF, and introduce measures to prevent administrative uses of the data.¹⁹⁷ HRDC also announced that they are considering the introduction of amendments to its legislation with penalties and sanctions for the misuse of information. Although the Commissioner commended HRDC for these moves, he noted that HRDC's actions focus more on aspects of security than on the protection of privacy. As Phillips noted, "it is very difficult for me to accept, for example, on the basis of your review, that

¹⁹³ See the *Privacy Act*, Section 8 (2) <http://canada.justice.gc.ca/en/laws/P-21/text.html>

¹⁹⁴ *ibid.*

¹⁹⁵ *Op Cit. Privacy Commissioner's Annual Report, 1999, 2000.*

¹⁹⁶ *ibid.*

all of the information contained in the Longitudinal Labour Force File is indeed directly relevant and necessary to HRDC's operating program and policy activities".¹⁹⁸ In a later letter, the Commissioner stood by his previous assessment of the LLFF, noting "I still view the Longitudinal Labour Force File as something tantamount to a citizen profile". The Commissioner also took exception to the HRDC claim that the department is in compliance with the Privacy Act. Phillips noted that "one does not have to be a privacy expert to see that this assertion rests on a restrictive and literal interpretation of . . . the fundamental rights that are at the heart of the Privacy Act . . . I do not find it satisfactory that the federal government's largest department defends the creation, maintenance and expansion of dossiers on vast numbers of Canadians by saying that it meets minimum legal provisions. Surely a higher duty than that is imposed."¹⁹⁹ Achieving compliance to the law and accountability to Canadians would require complete transparency in how research is conducted and how decisions are made by HRDC. The Privacy Commissioner's Office thus concluded that HRDC's response was inadequate. To be truly compliant and accountable, HRDC must communicate to Canadians why their information is used, how it is used, how long the information will be kept, and to whom it will be disclosed.

To this point, I have attempted to explain the origins of HRDC and the background history of the Longitudinal Labour Force File. As well, I have identified the primary participants in the conflict and their arguments. Implicit in the positions presented by the Privacy Commissioner's Office and HRDC is a prototypical example of the competing interests and values that are pervasive in attempts to restrict the uses of information for the sake of privacy. In the next section, I will examine how the privacy conflict was publicized by the media, politicized in the House of Commons, and responded to by citizens across Canada. I have sub-divided the dynamics of the conflict into different stages to emphasize the temporal and conceptual progressions of the conflict. These stages are, respectively, Initial Publicity, Escalation, Intensification, Denial, Reaction, Fall-out, and Aftermath.

¹⁹⁷ The letter was dated Sept. 3, 1999.

¹⁹⁸ *ibid.*

The Dynamics of Conflict

Initial Publicity

On Wednesday, May 17, 2000, Canadians across the country woke up to the news that the Government of Canada had a secret, massive database that contained the intimate details of their personal lives. News stories on the morning radio played sound bites of Canada's Privacy Commissioner revealing the unexpected: "This is an enormous database with enormous amounts of information about each one of us," the commissioner explained. "Every one of us is covered in this file in one way or another. They have a complete record of you if you've had any contact anywhere with any (of a number of government departments and programs) . . . which tells them how your life is progressing."

News of the giant database also made the front page of most of the major papers across the country. The headlines were suggestive and ominous. The lead story on the front page of the *National Post* declared 'Ottawa defends 'big brother' database',²⁰⁰. The front of the *Montreal Gazette* announced that 'Ottawa has files on us all Cradle-to-grave database open to abuse',²⁰¹. The *Edmonton Journal* led with a story proclaiming 'Canadians tracked by huge gov't database: 'Every one of us is covered' in millions of individual files',²⁰². The story in the *Calgary Herald* reported 'Feds database filled with our intimate details',²⁰³. On the west coast of Canada, the *Vancouver Sun's* front page declared 'Ottawa keeps secret files on all Canadians- The privacy watchdog reveals the existence of a huge database on individual citizens',²⁰⁴. Likewise in Victoria, the front page of the *Times Colonist* featured an article stating 'Federal computers keep tabs on us',²⁰⁵. The Human Resource Department's 'secret database' was no longer a secret.

This letter from the Privacy Commissioner was dated Sept. 28, 1999¹⁹⁹ *ibid*.

²⁰⁰ *National Post*. "Ottawa defends 'big brother' database: Ministry kept public in the dark about data collection: Files contain up to 2,000 different details about lives of 33 million Canadians". May 17, 2000, National Edition, p.A1 / FRONT.

²⁰¹ *Gazette, The (Montreal)*. "Ottawa has files on us all: Cradle-to-grave database open to abuse". May 17, 2000. Page A1.

²⁰² *Edmonton Journal*, "Canadians tracked by huge gov't database: 'Every one of us is covered' in millions of individual files -- commissioner". May 17, 2000, Final Edition, p.A1 / FRONT

²⁰³ *Calgary Herald*, "Feds database filled with our intimate details". May 17, 2000, Final Edition, p.A1.

²⁰⁴ *Vancouver Sun*. "Ottawa keeps secret files on all Canadians: The privacy watchdog reveals the existence of a huge database on individual citizens." May 17, 2000. Final Edition, p.A1 / FRONT.

²⁰⁵ "Federal Computers Keep Tabs on us." May 17, 2000. p. A1.

The contents of the articles were for the most part similar in substance. The newspapers concentrated on the size and scope of HRDC's database, reporting quotes and facts from the Privacy Commissioner's Annual Report. Particular attention was paid to the types of information catalogued into the single file. One of the notable features of the initial coverage of the privacy conflict was the evocation of dystopic images, and in particular the image of 'big brother' from George Orwell's famous work on totalitarianism presented in 1984. The *Vancouver Sun* quoted excerpts uttered by the Privacy Commissioner: "I said years ago the fear is not Big Brother, it's thousands of little brothers, all of whom have an increasing technological ability to monitor the personal lives of Canadians." "But there is a Big Brother factor as well and I think the Longitudinal Labour Force File is an example of the kind of thing that modern technology makes possible. We should know about it. We should know they're doing it and they should have to do it under very tightly written legal restraints about the usage of that information."²⁰⁶ The *National Post* also focused on imagery to communicate the potential consequences of HRDC's "Orwellian computer database".²⁰⁷

The *National Post* also included comments from critics of the Liberal government. "This is scary stuff," said Maurice Vellacott, a Canadian Alliance MP and Human Resources critic. "It sounds like the future, like the Big Brother described in the science fiction books, but none of us realized it was occurring right now." Jean Dube, the Conservative Party Human Resources critic, proclaimed her surprise to here that the intimate details of Canadian citizens were held in a giant database, noting "It's wrong and not acceptable".²⁰⁸

The *Montreal Gazette*, among others, cited the Privacy Commissioner's Report warning of the problems with the database. "Canadians don't know how much information is being collected about them and the extent to which it is being integrated and shared with others. How many Canadians know their tax information is in an HRDC profile? Continually centralizing and integrating so much personal data on almost every

²⁰⁶ *Vancouver Sun*, "Ottawa keeps secret files on all Canadians: The privacy watchdog reveals the existence of a huge database on individual citizens." May 17, 2000. Final Edition, p.A1 / FRONT.

²⁰⁷ *National Post*, "Ottawa defends 'big brother' database: Ministry kept public in the dark about data collection: Files contain up to 2,000 different details about lives of 33 million Canadians". May 17, 2000, National Edition, p.A1 / FRONT.

person in Canada poses significant risks to our privacy."²⁰⁹ The *National Post* reported that HRDC is proposing to expand the database to include more data on social assistance recipients from provinces and new territories, as well as information about student loans, retirement pensions and old age security benefits. The *Post* also reported the privacy commissioner's comment that HRDC is emphasizing that its data are stored securely and coded in such a way that nobody could be identified when they are shared with private research firms and other governments for research purposes. The article highlighted HRDC's defense that its practices meet "minimum legal provisions."²¹⁰

A voice from the policy community outside of government was also heard in the lead story in the *Montreal Gazette*. Pippa Lawson of the Public Interest Advocacy Centre admitted that she is worried that personal information could be sold. "History has shown governments can go off the rails," Lawson said in an interview. "There's a huge market out there for personal information, for marketing purposes in particular. We've already seen municipal and provincial governments selling databases."²¹¹

The Department of Human Resources had the opportunity to respond to the conflict in a number of newspapers across the country in the initial phase of publicity. The *Edmonton Journal* published comments by Bob Wilson, HRDC's director-general of evaluation and data development. "We have taken his concerns seriously", Wilson suggested in response to the concerns raised by the Privacy Commissioner.²¹² He noted the database is "always open to misuse or abuse unless there are legislated, legal restraints on its use." However, he continued to defend the intent of the Longitudinal Labour Force File. "On the other hand, it's really important to Canadians that we do policy research and evaluation so that we can get programs that meet their needs."²¹³ Wilson assured that specific information in the database is electronically masked to hide an individual's identity and that only a handful of HRDC officials have access to the

²⁰⁸ *ibid.*

²⁰⁹ *The Gazette (Montreal)*, "Ottawa has files on us all: Cradle-to-grave database open to abuse". May 17, 2000. Page A1.

²¹⁰ *Op cit. National Post*, "Ottawa defends 'big brother' database: Ministry kept public in the dark about data collection: Files contain up to 2,000 different details about lives of 33 million Canadians".

²¹¹ *Op cit. The Gazette (Montreal)*, "Ottawa has files on us all: Cradle-to-grave database open to abuse".

²¹² *Edmonton Journal*, "Canadians tracked by huge gov't database: 'Every one of us is covered' in millions of individual files -- commissioner". May 17, 2000, Final Edition, p.A1 / FRONT.

²¹³ *ibid.*

technological hardware needed to unmask the data. However, he also acknowledged that the masked data is sometimes given to private firms for research and analysis. "We, perhaps not wisely but nevertheless, have relied on the fact that we've been doing this for 15 years and never had a problem with it, never had even a hint of a (security) breach."²¹⁴

Escalation

On the day after the Speaker of the House tabled the 1999-2000 report of the Privacy Commissioner and permanently referred it to the Standing Committee on Justice and Human Rights, the conflict over the LLFF continued to escalate. On May 17, the privacy implications of the Longitudinal Labour Force File were first debated in the 2nd Session, 36th Parliamentary session of the House of Commons. Deborah Gray, Canadian Alliance Member of Commons and Leader of the Opposition began the attacks on Jane Stewart, the Minister of Human Resources Development Canada by accusing her of continuing in the mismanagement of the federal government's largest department. HRDC had previously been assaulted by the Opposition, the media, and the Canadian public for the mismanagement of a Job Creation Fund. "Canadians have borne witness to the HRD minister's mismanagement of over a billion dollars," said Tory House leader Peter MacKay. "With this record of bungling, how can Canadians trust this minister to protect their most personal of information?"²¹⁵ The revelation that HRDC was compromising the privacy of Canadian citizens put the Opposition on the offensive. "What the Privacy Commissioner did was to ring some very loud alarm bells and Canadians are listening. I hope the Minister is," Canadian Alliance MP Diane Ablonczy told the Commons. "In the hands of private business, such information could keep someone from getting insurance or a job. And imagine this information in the hands of criminals because of lax security," she added.²¹⁶

In addition to the criticism of irresponsible management, the Leader of the Opposition challenged HRDC's commitment to security. Grey accused the department of lacking in expertise and knowledge of proper security procedures. She based this assessment on an internal audit that her staff had uncovered on the assessment of

²¹⁴ *ibid.*

²¹⁵ Edited Hansard, 36th Parliament, 2nd Session. (Number 099). Wednesday, May 17, 2000.
http://www.parl.gc.ca/cgi-bin/36/pb_chb_hou_deb_ind.pl?36:2:e:099_2000-05-17

²¹⁶ *ibid.*

information technology security conducted in September of 1999. The audit stated that “(s)ince few people know of the existence of the IT security policies and procedures, personnel knowledge of IT security standards and practises needs improvement.”²¹⁷ Jane Stewart defended HRDC noting that “it is a department that is continuously looking at itself, using audits to identify areas where we can make improvements and it is a department that makes changes to improve the services that we provide to Canadians.”²¹⁸

The Opposition continued to focus on the security aspect of the privacy problem. Their criticisms were continually met with the same general response, that suggested that the information is encrypted and secure, and that the deputy minister of HRDC had requested the consultation of the Privacy Commissioner to participate on a working group on privacy. In response to the onslaught of questions about the security measures in place at HRDC, the Honourable Minister Stewart continued to accuse the Opposition of “doing nothing but trying to scare Canadians”.²¹⁹

In addition to questions about the security of HRDC’s Information Technology (IT) practises, the Liberal Government was questioned as to why the database was constructed in the first place, and the Minister for HRDC was asked to justify her refusal of the Privacy Commissioner’s recommendations.²²⁰ Again, Stewart’s response focussed on assurances of the security of the data rather than on the threat to privacy inherent in such a database. Stewart also noted that the Department had considered the Privacy Commissioner’s recommendations, and that they introduced a time frame that would set limits on the duration in which information would be held in the database.

Stewart was also questioned about her department’s “interpretation” of the Privacy Act. The Opposition’s criticisms were based on the Commissioner’s comment in the Annual report that “one does not have to be a privacy expert to see that (HRDC’s) assertion rests on a restrictive and literal interpretation of . . . the fundamental rights that are at the heart of the Privacy Act”. Stewart responded that the Commissioner made it clear that HRDC was working within the law. However, NDP MP Bill Blaikie noted that the Privacy Commissioner confirmed that they were operating within the law, but noted

²¹⁷ *ibid.*

²¹⁸ *ibid.*

²¹⁹ *ibid.*

²²⁰ *ibid.*

that that might say something about the law as well.²²¹ In response to questions about the effectiveness of the Privacy Act, Anne McLellan, the Minister of Justice and Attorney General of Canada later noted that the government "will review the existing privacy legislation in a timely fashion".²²²

On May 18, the privacy concerns facing HRDC continued to escalate. In a *Canadian Press Newswire* release, the federal government's "tracking of the lives of Canadians" continued to attract attention.²²³ Again, the focus on security issues was a main theme. The article explained that the system was set up so that even if the code is broken, the resulting data would not allow the matching of a person's name with the person's data. Daniel Lavoie, a spokesman for the Department of Human Resources, explained that "the personal information is masked to ensure that somebody using the data bank cannot link the personal information with the raw data. So even if somebody was able to break the code, they would face a massive set of masked data ... just computer codes."²²⁴ Lavoie continued to explain the anonymous character of the information that is used for research, noting "when we do research, we look at one series of data, but we don't have the names because it's masked. To clarify the types of purposes that the LLFF serves, Lavoie provided a scenario for how the data might be used. "If the government wanted to increase benefits under the Employment Insurance program by \$5 a week, for example, it could pull data from the database to gauge the impact on the economy of a given community."²²⁵

The newspapers also provided comments from representatives of the provinces to comment on the Longitudinal Labour Force File. "I would be very concerned if we were sharing information of a personal nature - outside of criminal activity and areas like maintenance enforcement - that could jeopardize the privacy of an individual" said Alberta Premier Ralph Klein.²²⁶ The Quebec minister responsible for citizen relations was vocal as well, calling on the federal government to destroy all information on Quebec citizens. In British Columbia, Attorney General Andrew Petter stated "I intend to

²²¹ *ibid.*

²²² *ibid.*

²²³ *Canadian Press Newswire*. "Opposition slams ``Big Brother`` database. No worries, officials say". May 18, 2000

²²⁴ *ibid.*

²²⁵ *ibid.*

communicate to the federal minister of justice my very serious concerns".²²⁷ In the *Vancouver Sun*, it was also reported that British Columbia may refuse to share personal information on British Columbians unless the federal government would agree to stringent and restrictive rules regarding the use of the records. "What we should do is satisfy ourselves that the information being provided to the federal government is being limited to specific purposes", said Petter.²²⁸ B.C.'s Information and Privacy Commissioner, David Loukidelis agreed with the Attorney General, stating "B.C. has to come up with a really effective stance that makes it plain to the feds that personal information will only be shared under stringent criteria. The feds really have to be called to account on this." He also suggested that the B.C. government should "disclose information only for purposes that it thinks are legitimate and pressing."²²⁹

Privacy coverage continued to dominate the headlines in the *National Post*. In addition to the *Canadian Newswire* story, there were three stories covering the conflict surrounding the Longitudinal Labour Force File. One of the articles was concerned with a review of the federal Privacy Act, and reported on the call for a review of the current privacy legislation that governs the public sector.²³⁰ Another article focussed attention on other recent privacy issues, including Ontario's ministry of transport selling personal information to private companies earlier this year. The article also reported on an incident from last year when Elections Canada "misplaced" a Manitoba Highway Department file containing the name, address, sex, date of birth, and license registration number of almost all of the 675,000 drivers in the province. It is believed that the file (stored on a single magnetic tape) ended up in the garbage, but no one is sure.²³¹

The fourth article in the *National Post* was in the *Financial Post* section and it considered the possibility that the Longitudinal Labour Force File represents a sign of things to come. The article suggests that government is a "coercive monopoly", and that

²²⁶ *ibid.*

²²⁷ *The Province* (Vancouver), "Petter fears federal files open to abuse". May 18, 2000, Final Edition, p.A23.

²²⁸ *Vancouver Sun*, "B.C. threatens to withhold personal data from Ottawa: Provincial officials react angrily to news Ottawa has secret files on all Canadians". May 18, 2000, Final Edition, p.A1 / FRONT.

²²⁹ *ibid.*

²³⁰ *National Post*, "'Time to review' Privacy Act, says Justice Minister- Outrage over database- Opposition attacks focus on Stewart". May 18, 2000, National Edition, p.A6.

²³¹ *National Post*, "Keeping secrets". May 18, 2000, National Edition, p.A19.

its access to information represents a source of monopoly profit.²³² The article argues that "In an information economy, where technology can digitize and compartmentalize information into taxable bits and bytes, information may eventually form an explicit part of the tax base."²³³ The combination of an Information Technology infrastructure with the wealth of information collected to provide and administer programs combine to serve as a potential form of government revenue. "Government becomes an info-predator, stalking its citizens for information it can then sell to the highest bidder. Vehicle records, tax records, hospital and medical records, business records -- all become potential sources of revenue." The article argues that privacy legislation alone is not enough to protect individuals from the 'predatory state'. "To keep the info-predatory tendencies of the state in check, we need some form of property rights assigned to citizens regarding the disposition and uses of current information."²³⁴

Intensification

The LLFF privacy conflict intensified in the second day of debate in Question Period. The dispute over the Longitudinal Labour Force File began with MP Maud Debien of the Bloc Quebecois (BQ) inviting everyone to check the contents of their file by filing a written application under the Access to Information Act to HRDC.²³⁵ Progressive Conservative MP Bill Casey wanted to avoid the hassle of going through the Freedom of Information process altogether: "I should like to ask the minister if she will provide me with my file, complete with the names of all government agencies that have accessed my file. I would like her to do it without going through the delay process of the access to information process."²³⁶ Another BQ member asked why it was so difficult for ordinary citizen's to obtain information about themselves when the department can get it without the consent of the individual.²³⁷

The issue of consent continued to be a common theme in a number of questions directed at the Human Resources Minister. The Minister was asked why consent was

²³² *Financial Post* (National Post), "Will mining our information be governments' new profit centre? Federal database raises disturbing possibilities". May 18, 2000 p. C19.

²³³ *ibid.*

²³⁴ *ibid.*

²³⁵ Edited Hansard, 36th Parliament, 2nd Session. (Number 100). Thursday, May 18, 2000
http://www.parl.gc.ca/cgi-bin/36/pb_chb_hou_deb_ind.pl?36:2:e:100_2000-05-18

²³⁶ *ibid.*

required to be put on the Permanent Voters Registry on Income Tax forms, but it was not required for information held in the Longitudinal Labour Force File. Invoking the OECD principles, Paul Crete of the BQ also asked how the files are "cleaned up", referring to the principle of accuracy.²³⁸ In response to these questions, the Minister suggested that she "would like my department to sit with him (the Privacy Commissioner) and his department in a working group to determine how we can ensure that Canadians do know how their information is being used." When asked "why . . . does the minister violate Canadians' privacy without their consent", Stewart again acknowledged the importance of privacy and quoted the Privacy Commissioner saying that "we are not aware, nor has it been brought to our attention, that the database has ever been compromised or access inappropriately obtained by virtue of deficiencies in security safeguards."²³⁹ Again the Minister defended the *security* of the database when asked a question about *privacy*. Throughout question period, the Liberal Government continued to defend the database and HRDC's policies, suggesting that the Opposition must not "cry wolf".²⁴⁰

The debate in the House continued to focus on the security theme. In response to comments and questions about the internal audit of IT security by HRDC, it was revealed that the audit was of HRDC's Local Area Network (LAN) and not all of HRDC's IT practices.²⁴¹ The security of the LLFF involves a completely separate system. The Minister of HRDC continued to assure members of the House that access to the database is limited (only six HRDC staff have access to unmasked data), the information is encrypted, and the database is secure. The Opposition continued to focus attention on the security audit, and shifted attention to the way in which HRDC disposes of computer hardware. Canadian Alliance members noted that the security audit warned "(t)here is no assurance that all hard drives are erased of potentially sensitive data prior to disposal." They continued to focus on the conclusions of the internal security audit, quoting that "(w)hen asked to define and describe their interpretation of an IT security breach people did not know exactly what this term meant or how to report it."²⁴²

²³⁷ *ibid.*

²³⁸ *ibid.*

²³⁹ *ibid.*

²⁴⁰ *ibid.*

²⁴¹ *ibid.*

²⁴² *ibid.*

For the second consecutive day, debate over the Longitudinal Labour Force File focussed attention on other governmental privacy conflicts. The HRDC Minister attacked the privacy practices of the Canadian Alliance, noting that "one of the leadership candidates for that member's party has been inappropriately collecting and using lists".²⁴³ A Canadian Alliance MP also highlighted a case from the Privacy Commissioner's Annual Report that documented a complaint in which an RCMP officer was giving insurance companies in Alberta the names of motorists who were ticketed for being in violation of mandatory seatbelt laws.²⁴⁴

Denial

The HRDC privacy conflict continued to be a hot topic of debate on Friday, May 19, 2000 in the House of Commons. The Opposition continued to focus on the security of the database. Minister Stewart also continued to assure the Opposition that the Longitudinal Labour Force File was secure, and that they wanted to work with the Privacy Commissioner "to ensure that the system that is secure today will be secure tomorrow".²⁴⁵ Canadian Alliance members continued to ridicule the Human Resource Department for trying to hide the existence of the database and shrouding it in secrecy, despite the fact that they were quoting information that was available on the Government of Canada's *InfoSource* website.

Again, the privacy debate drew attention to other privacy issues. When Canadian Alliance MP and HRDC critic Diane Ablonczy asked why the government and minister are "so brazen to keep violating the privacy rights of Canadians", the Deputy Prime Minister Herb Grey ignored the familiar accusation and instead questioned a Canadian Alliance proposal to implement a DNA database to store information on *suspected* criminals.²⁴⁶ Grey quoted the Canadian Alliance justice critic, who had previously stated that "(e)ven those who are found not guilty or have the charges dropped should have their DNA recorded on file because police only arrest people for good reasons". Grey, pointing at the Opposition side of the House, declared "(t)here are big brother and big sister, and

²⁴³ *ibid.*

²⁴⁴ *ibid.*

²⁴⁵ Edited Hansard, 36th Parliament, 2nd Session. (Number 101). Friday, May 19, 2000.
http://www.parl.gc.ca/cgi-bin/36/pb_chb_hou_deb_ind.pl?36:2:e:101_2000-05-19

²⁴⁶ *ibid.*

that is not what Canadians want".²⁴⁷ After the Minister of HRDC was questioned as to why "they want this information from innocent, law-abiding citizens", Stewart deflected criticism by drawing attention to another privacy problem involving the "extreme right". As the Minister noted, "(i)t is interesting that the Harris government, particularly the ministry of transportation, is selling confidential driver data including home addresses to private companies, the companies that the hon. member said should not have them. Do members know what hurts? They are making money from it and are refusing to tell us in this province how much it is worth."²⁴⁸

Another concern raised over the course of the debate was whether or not the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS) have access to the LLFF database. The Minister of HRDC responded that CSIS and the RCMP do not have direct access to the longitudinal file, and that if they were to request information they would have to have a court order. The Minister reminded the Members of the House of Commons that the Privacy Commissioner had already concluded that there has never been a disclosure of information for administrative or law enforcement purposes.

Criticism of the Longitudinal Labour Force File continued in the media on Friday, May 19. It was clearly evident that there was a tone of skepticism in response to the HRDC denial. This sentiment was perhaps most clear in the *National Post*: "The existence of a Big Brother file is a handy addition to the government's many other tools for making sure your private life remains state business. Tools like audit and census bureaus with power to sanction non-co-operation with criminal penalties. So if the government takes an interest in you, that interest will be satisfied."²⁴⁹ A number of stories suggested that HRDC was missing the point over serious concerns about its massive databank tracking the lives of Canadians. For example, the Privacy Commissioner was cited as acknowledging the legality of the database, but noting that HRDC's position does "not reflect the spirit of the Privacy Act, the principles of the Privacy Act or the objective of the Privacy Act." Although HRDC complied with the strict letter of the law in

²⁴⁷ *ibid.*

²⁴⁸ *ibid.*

²⁴⁹ *National Post*, "Ottawa's policy: Do ask, don't tell- They have massive files on us, but keep their doings secret". May 19, 2000, National Edition, p.A1 / FRONT.

constructing the database, Phillips reflected on the limits of the law: “in my opinion, there are issues that get beyond law here. There are basic ethical and philosophical issues.”²⁵⁰ Phillips was also critical of the fact that the database was created before its research uses and purposes were spelled out, noting that “(t)hat's a reversal of the customary approach”. The Privacy Commissioner was also critical of the fact that “there is absolutely no element of consent anywhere in the database ... No effort has been made to obtain personal consent.”²⁵¹

Reaction

In ‘letters to the editor’ across the country, Canadians were expressing their anger over and disgust with the HRDC “big brother database”. A letter to the *Toronto Star* suggested that “(t)o merely rely on HRDC staff professionalism to always do the right thing for the right reasons is the height of folly.”²⁵² In the *Halifax Herald*, one respondent called for stricter measures governing HRDC’s data practises, noting “(u)ltimately, the only way the Canadian public will be reassured is if limits are put on Ottawa’s information gluttony. HRDC’s database should be governed by the same rules as Statistics Canada, where misuse of information carries penalties.”²⁵³ Another frustrated writer to the *Ottawa Citizen* encouraged Canadians to make a Freedom of Information request, after noting “I was shocked, but not surprised, that our Liberal government keeps these files on every Canadian. What self-respecting police-state-in-waiting would not keep these Stasi-like files?”²⁵⁴

House of Commons Opposition members who had asked the Liberal Government if CSIS and the RCMP had access to the Longitudinal Labour Force File got their answer in a *Canadian Press Newswire* article, and it was different from the one given by HRDC previously. Both Canada’s spy service and the RCMP have the right to obtain sensitive personal and financial information about Canadians, without their consent, from the LLFF. Martin Nantel, the legal adviser to Privacy Commissioner, confirmed that “the

²⁵⁰ *ibid.*

²⁵¹ *ibid.*

²⁵² *The Toronto Star*, ‘Letters to the Editor’ May 19, 2000, First Edition.

²⁵³ *The Halifax Herald*, ‘Letters to the Editor’ May 19, 2000, First Edition.

²⁵⁴ *The Ottawa Citizen*, ‘Letters to the Editor’ May 19, 2000.

option is there for an investigative body to request (the information)".²⁵⁵ Under the existing privacy law, CSIS and the RCMP can legally obtain sensitive information from the computer database without consent. The article reported that RCMP and CSIS would not require a search warrant to obtain any information contained in the Longitudinal Labour Force File. All that CSIS and the RCMP would have to do, noted Montreal privacy lawyer Raymond Doray, is "write a letter to the Human Resources Department saying that they are doing an inquiry right now about Mr. X and they would like to obtain the information concerning this person for investigative purposes. That's it. It would be totally legal."²⁵⁶ The Department of Human Resources would not be compelled under the Privacy Act to disclose information contained in the computer database to the RCMP or CSIS, however the decision to release the material would be at the discretion of an official within Human Resources. *Montreal La Presse* also reported that a request was made by the United States Federal Bureau of Investigation to the RCMP to access files in the LLFF. The RCMP denied the FBI's request.

On Saturday May 20, the *Calgary Herald* reported that in three days, over 500 individuals had made a request to the Department of Human Resources to access their information in the Longitudinal Labour Force File.²⁵⁷ Daniel Lavoie, spokesman for Human Resources Development Canada, confirmed the requests and announced that HRDC was working with the Privacy Commissioner on the most efficient way to release the information. HRDC anticipated difficulty in retrieving and distributing information in the LLFF because the database was not designed to retrieve information on a particular individual, but rather on a group of individuals.²⁵⁸

In the *Montreal Gazette*, the Public Interest Advocacy Centre, a non-profit group that monitors privacy issues, called for the modernization of laws protecting individual privacy. Andrew Reddick, research director for the Centre, noted that "(t)he government

²⁵⁵ *Canadian Press Newswire*, "RCMP, CSIS can access computer files on citizens without consent: report". May 19, 2000.

²⁵⁶ *ibid.* Section 8.2 (e) of the Privacy Act stipulates that personal information under the "control of a government institution" can be released "without the consent of the individual to whom it relates ... (to) an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada."

²⁵⁷ *Calgary Herald*, "Privacy concerns mount over 'invisible citizen profile'". May 20, 2000, Final Edition, p. A5.

²⁵⁸ *ibid.*

has gone from lawnmower technology to Cadillac-style computers in terms of storage and data matching.”²⁵⁹ “How the information is used is generally beneficial to Canadians, but there is real potential for abuse. There is always the risk of a real Big Brother if you have information put together.”²⁶⁰ Although HRDC claims that “existing legislation and internal policies provide adequate protection of personal information”, nonetheless, the possibility of data mining or profiling individuals may encourage the temptation for abuse.

The *Toronto Star* published an editorial entitled a “warning worth heeding” that heavily criticized the Human Resources Department. The *Star*, skeptical of HRDC’s ability to protect citizen information, declared that they “fail to see the need for an electronic profile of every citizen. If the federal government wants facts and figures for research purposes, it can use the information that Statistics Canada gathers, under strict confidentiality rules.”²⁶¹ Echoing the government Opposition, the *Star* called on HRDC to “wipe out” the database containing intimate details on the nation’s population, and encouraged readers to make a request for their information.

The publicity surrounding the Longitudinal Labour Force File in the country’s newspapers faded in the week following the intense coverage that it received. Concern over the database however continued to be on the minds of Canadians, and a number of stories and information on the database were posted on the Internet.²⁶² Hack Canada, a website dedicated to providing information and resources to Canadian Hackers, posted information on the conflict and instructions on how to access records from HRDC.²⁶³ The government speculated by the end of the week that over 18,000 requests for information had been filed under the Freedom of Information Act.

Fallout

On Monday, May 29, 2000, 13 days after the release of the Privacy Commissioner’s Annual Report documenting the existence of problems with the

²⁵⁹ *The Gazette (Montreal)*, “Canadians are requesting their HRDC files” May 20, 2000, Final Edition, p. A14.

²⁶⁰ *ibid.*

²⁶¹ *The Toronto Star*, “A warning worth heeding” May 20, 2000, First Edition.

²⁶² For the most part, these were mostly postings and clips of news articles that were originally published in the print media.

²⁶³ <http://www.hackcanada.com/canadian/freedom/canadasbigbrother2000.html>

Longitudinal Labour Force File, HRDC issued a press release confirming that the giant database would be dismantled. In dismantling the LLFF, HRDC eliminated the computer program that was used to link its information with information from Canada Customs and Revenue Agency and data on social assistance from provincial/territorial governments.

In addition to the 'unlinking' of the databases, the information in the LLFF from the Canada Customs and Revenue Agency (CCRA) was returned.²⁶⁴ HRDC announced that they would review the information-sharing arrangements that they have with provincial and territorial governments for research purposes. They also announced that the department's policy analysis and research data relating to its own programs will be kept as separate, secure and unlinked files, and that all personal information identifying individuals will remain encrypted.²⁶⁵

In the HRDC press release, Stewart commented that "given public concerns about privacy issues in this era of advanced and constantly changing technology, I have chosen an approach that addresses future threats to privacy."²⁶⁶ Stewart acknowledged that "the Privacy Commissioner fully supports this decision, and the other measures we are taking to protect privacy." In a letter HRDC dated May 27, Bruce Phillips, the Privacy Commissioner responded to Claire Morris, the Deputy Minister of Human Resources Development Canada, noting that he accepts and supports these measures, and that they satisfy all the recommendations and observations outlined in his 1999-2000 Annual Report. The Commissioner also commended "the spirit of which our discussions have taken place and the clear demonstration of your determination to improve the supervision and management of your information systems in ways that strengthen the privacy rights of Canadians."²⁶⁷

In addition to the removal of the computer program that linked the files in the LLFF and returning the information to the CCRA, HRDC announced that they would also remove personal identifiers on the Social Assistance Recipients databank that is used by researchers, and that a review of the database would be conducted with the

²⁶⁴ Human Resources Development Canada, *News Release*: "HRDC Dismantles Longitudinal Labour Force File Databank". May 29, 2000.

²⁶⁵ *ibid.*

²⁶⁶ *ibid.*

²⁶⁷ *ibid.*

consultation of the provinces and the territories.²⁶⁸ HRDC assured that Human Resources databases (such as the employment insurance database) will be maintained separately and securely, and that personal identifiers would be encrypted. The Privacy Commissioner agreed to monitor the implementation of these measures.

HRDC also announced " a new governance structure for future social and labour market policy research" that would be modeled on Statistics Canada's practices.²⁶⁹ This new governance structure will be guided by principles relating to the public interest, including confidentiality, transparency (uses and linkages), an assessment of the public good, avoidance of potential harm to particular groups, appropriate sample size, etc. This will require that research that uses linkages of separate databases meet a number of criteria. Under this structure, research must be:

- consistent with the public interest principles above;
- based on detailed project proposals reviewed by a senior-level committee (including senior officials responsible for research and privacy);
- approved by the Deputy Minister;
- include consultations with specific groups that may be the focus of a particular study; and,
- receive the advice of the Privacy Commissioner.

In addition, future linkages between individual government databases required for approved projects would be done only on the following basis:

- Linked files would contain no personal identifiers;
- Linked files would be constructed only with the specific information required for the project (e.g. elements, length of time, number of people etc.);
- Linked files would only be approved for a fixed time and would be returned and destroyed after research use; and,
- Intrinsically long studies would require built-in reviews at fixed intervals.²⁷⁰

²⁶⁸ *ibid.*

²⁶⁹ Human Resources Development Canada, "BACKGROUND: HRDC's Measures to Strengthen Privacy of Information". May 29, 2000.

²⁷⁰ *ibid.*

The revamping of HRDC's policies regarding the structure of social and labour market policy also took into consideration the issue of transparency. HRDC announced that they would create an external research advisory committee that will include a representative from the Office of the Privacy Commissioner. The department is also instituting a process of annual public reporting on its social and labour market policy operations to better inform Canadians of their activities and the importance of their research.²⁷¹

To ensure that the research activities of HRDC are held accountable in the future, the department recommended a legal protective framework, including penalties for the misuse of information, to govern the collection and uses of data and information obtained from Canadians by HRDC. HRDC also announced that they will continue to seek advice from the Privacy Commissioner's Office, and the Commissioner will monitor the dismantling of the Longitudinal Labour Force File.

Human Resources Development Canada also announced that they are working with the Privacy Commissioner's Office to respond to Freedom of Information requests regarding information held in the LLFF. Requests for information on LLFF data require the individual's full name, address, postal code, telephone number, social insurance number (SIN), and a citation that the information is requested with reference to the Privacy Act.²⁷² HRDC announced that they will send a letter to all individuals who have made a request, informing them of the process and timelines for responding to it. The Department asked individuals who did not provide their SIN to supply it, because the SIN is the universal identifier and the only means to identify the right file associated with the requestor. HRDC also asked individuals to confirm their desire to receive the LLFF information held about them, in consideration of the fact that database was going to be dismantled. HRDC announced that for requests received up until June 30, 2000, arrangements would be made with CCRA to provide information from the database returned to them. After that date, however, privacy requests would need to be made separately to HRDC and CCRA.²⁷³

²⁷¹ *ibid.*

²⁷² *ibid.*

²⁷³ *ibid.*

The Aftermath

In the immediate aftermath of the conflict, a number of commentators in the print media remained skeptical of the government's sudden commitment to privacy.

Nonetheless, the database was dismantled with little fanfare.

Inside the federal government, the privacy issue remained salient. On June 16, 2000, the Privacy Commissioner's Office released a 174 page report on *Privacy Act Reform*, outlining a proposal to modernize the Privacy Act and bring its language up to the level of the private sector privacy legislation.²⁷⁴ Furthermore, a number of government departments began working more closely with the Privacy Commissioner's Office, and a number of PCO staff now meet regularly with departmental representatives to discuss privacy issues and introduce privacy considerations at a much earlier stage in the policy development process.

Considering the short duration of the public dimension of the conflict, the response to the privacy issue was striking. Not only did the conflict receive much more attention by the political realm and the print media than most conflicts over privacy values, it also captured the attention of the Canadian citizenry. At the June 30, 2000 deadline for Freedom of Information requests to access data from the LLFF, in excess of 70,000 Canadians had applied for access to their file.

However, it is important to note that the actual duration of the conflict was significantly longer than it appeared. The first letter regarding the conflict was originally sent in July of 1998, and it was not resolved until the end of May in 2000. That the conflict was resolved in a relatively short period of time points to the significant implications that a 'focussing event' can have on a policy problem. Without the sudden, dramatic events that followed the Privacy Commissioner's tabling of the Annual Report in Parliament, the conflict surely would not have been resolved as quickly or with the same measures enacted. That the Annual Report and the consequent press release could attract such attention is a testament to the power that the Privacy Commissioner can manifest through the 'whistle blowing' functions of the office. It also demonstrates the effectiveness of the 'tool kit' that provides for the publication of Annual Reports and the

²⁷⁴ *Privacy Act Reform: Issue Identification and Review. A Report by the Privacy Commissioner of Canada on Proposed Amendments to the Federal Privacy Act. June 16, 2000.*

opportunity to open a dialog with the Canadian public to send a signal to others to control their practices.

Now that I have examined how a privacy issue was politicized by way of a focussing event in the public sector of Canada, I will now turn to examine a private sector violation in the political jurisdiction of the United States. The same manner in which I explored the conflict in Canada will be replicated in the second case study. In this regard, I will review the policy landscape in the United States, explore the origins of the policy problem, define the privacy implications, and take a closer look at the problem of online profiling. This will then be followed by an extensive examination of the dynamics of conflict.

Chapter Three: The DoubleClick Conflict

Introduction

One of the greatest perceived threats to the privacy of individuals in the twenty-first century is the ability of organizations in the private sector to amass detailed and extensive sensitive personal information on consumers. Businesses and corporations have long had a vested interest in the everyday lives of individuals. "Know your customer" has also been a mantra for success in the world of business and marketing. To know your customer is to be able to meet the needs and demands of individuals in the marketplace.

Since the National Science Foundation transitioned the Internet to a competitive and commercially managed network in April of 1995²⁷⁵, a new economy has emerged with unparalleled opportunities for service delivery and commerce. Businesses have been restructured to facilitate greater demands for the transfer of information, and evolving business practices and revenue models have redefined the relationship between the 'marketed' and the 'marketer'. The Internet, providing a framework to deliver 'one to one' or 'one to many' communication by design with unprecedented precision, has challenged conceptions of anonymity and privacy in the digital sphere.

In many ways, the threats posed to privacy by the private sector can be conceptualized in terms of Oscar Gandy's 'panoptic sort'. The process of the panoptic sort is represented by the "all seeing eye of the difference machine that guides the global capitalist system."²⁷⁶ Other commentators have referred to this process as 'cybernetic capitalism', the emergence of a totalizing system of social control that depends on the ability of corporate interests to collect, store, process, and share massive amounts of information in order to track, command, coordinate, and control each one of us in ways we might not have thought possible.²⁷⁷ The panoptic sort operates to increase the ability

²⁷⁵ An NSF report entitled "Realizing The Information Future: The Internet and Beyond" was released in 1994 and provided a blueprint for the evolution of the information superhighway. It anticipated the critical issues of intellectual property rights, ethics, pricing, education, architecture and regulation for the Internet. This policy, embracing privatization, culminated in the defunding of the NSFNET Backbone in April, 1995. Funds were then redistributed on a competitive basis to regional networks to buy national-scale Internet connectivity. *A Brief History of the Internet*: <http://www.isoc.org/internet/history/brief.html>

²⁷⁶ Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press: Boulder. 1993. p. 1.

²⁷⁷ *ibid.*

of organized interests to identify, isolate, and communicate with individuals. It provides an opportunity to influence how consumers get to choose among a wide array of options. While the panoptic sort operates to improve upon the precision in which individuals are classified according to their perceived value in the marketplace, it also drains power from opportunities that are denied. In this chapter, I will examine how the issue of online profiling became publicized and politicized amidst much debate, as privacy advocates and industry advocates battled it out in a war of interests. But first, I will turn to examine the policy landscape in the United States, and explore the origins of the policy problem.

The Policy Landscape and the Privacy Problem

The Policy Landscape in the United States

As in the Canadian case, there is no explicit right to privacy in the U.S. Constitution. However, as I have already discussed, legal challenges and interpretations of the constitution have played a central role in establishing privacy protections. The Supreme Court has ruled that there are limited constitutional rights to privacy within the provisions of the Bill of Rights. These provisions grant a right of privacy from government surveillance where an individual has a "reasonable expectation of privacy"²⁷⁸, as well as in matters concerning marriage, procreation, contraception, family relationships, child rearing, and education.²⁷⁹

Unlike Canada, there is no comprehensive legislation that governs the private sector in the United States. The primary locus of privacy legislation is the Privacy Act of 1974 which protects information records by requiring agencies to apply four fair information principles to the uses of information. In addition to the Privacy Act, there is a patchwork of federal laws that regulate specific types or categories of personal information. These laws concern financial records, credit reports, video rentals, cable television, educational records, motor vehicle registration, and telephone records.²⁸⁰ However, a number of activities that concern personal information are not protected by law, such as the selling of bank and medical records, and workplace surveillance such as keystroke monitoring. A number of states have state level sectoral legislation, and almost

²⁷⁸ Katz v. U.S., 386 U.S. 954 (1967) <http://laws.findlaw.com/US/386/954.html>.

²⁷⁹ Banisar and Davies, "Global Trends in Privacy Protection". p. 108.

²⁸⁰ *ibid.* p. 109.

all states have recognized the tort of privacy that provides a civil right of action for invasion of privacy.²⁸¹

Where there is regulation of personal information in the private sector in the United States, it is often concerned with particular types of information use, such as video rental information or the credit reporting industry. In this sense, the U.S. approach differs from many other advanced industrial nations, in that they have avoided any comprehensive 'omnibus laws' to establish the rights and responsibilities pursuant to the processing of personal information.

U.S. common law has developed a set of tort rights that are designed to protect against four types of privacy invasion. These are: 1) intrusion upon one's seclusion; 2) misappropriation of one's name or likeness without permission; 3) public disclosure of private facts; and 4) publicity that faces one in a false light.²⁸² However, the establishment of limitations on each of the torts over time has eliminated their usefulness to respond to privacy conflicts or violations on the Internet. As such, most of the data processing on the Internet is not subject to the scope of the four branches of tort, or for that matter, anything at all.

One of the perceived weaknesses of U.S. privacy policy is the absence of an oversight agency to address privacy concerns and monitor compliance. Where there are oversight and enforcement mechanisms, they lie within the Federal Trade Commission's powers to protect consumer credit information and fair trade practices. However, the FTC has no formal authority to enforce privacy rights, unless the conflict is concerned with fraudulent or deceptive trade practices. The FTC has been monitoring the privacy issue, and they have organized a number of workshops and surveys on issues related to consumer privacy. The workshops and surveys have almost always yielded the same conclusions: privacy protection on the Internet is poor, and if self-regulation is to work, then it is going to take time and require greater industry support.²⁸³

Whether or not self-regulation is an effective mechanism to safeguard individual privacy has been a matter of significant debate recently in the United States. Although the

²⁸¹ *ibid.*

²⁸² Paul M. Schwartz, "Privacy and Democracy in Cyberspace". *Vanderbilt Law Review*, Vol. 52, 1998. p. 1634.

self-regulatory regime has been the preferred method of regulating privacy in the private sector by both the White House and industry in general, there is increasing pressure by rights activists, consumer groups, and Internet savvy individuals to enact a legislated privacy solution. There are two major objections to the self-regulatory model in the United States. The first is that it generally does not offer individuals strong privacy protections, and secondly, despite experimentation with the industry favored approach, there is little evidence that self-regulation is working.

The current self-regulatory regime requires businesses to develop and post a privacy policy in a prominent place on their website that explains the company's policy based on the fair information principles of *notice*, *choice*, *access* and *security*. Industry participants then register to a third party privacy 'seal of approval' program, such as Truste or BBBOnline.²⁸⁴ Once the company has agreed to 'tell the truth' in their privacy policies and pay a fee to the registration agency, they receive a graphic seal that alerts web surfers that they abide by the 'seals' principles. However, critics of the self-regulatory regime point out that there are serious shortcomings of this type of privacy protection. First, the privacy seal programs are awarded based on the existence and publication of a privacy policy, not on the content of the policy or assurances of best practices. A company whose practices may be considered problematic can easily be awarded a seal providing that their practices are properly disclosed. Under this system, there is much room to blur the familiar line between the spirit of privacy protection and compliance to it.

A second way in which the self-regulatory model is problematic is that it fails to regulate 'bad actors'. That is, even if the majority of businesses in the information industry adopted the self-regulatory model, the lack of restrictions would not prevent a company from misusing and abusing information. It may however force them to the cyber-metaphorical 'underground' where they can prey on the insecure and uninformed.

A third reason why the self-regulatory system is failing is that it has not proven to demonstrate any semblance of enforcement or accountability. A number of high profile privacy violations highlighted the shortcomings of the self-regulatory model. Both Intel,

²⁸³ The FTC's investigations, workshops, and surveys are well documented at <http://www.ftc.gov/privacy/index.html>.

the manufacturer of the popular Pentium processor, and Microsoft, a monopolistic software and Windows operating system developer had introduced products that used globally unique identifiers to track the activities of users on the Internet without their consent or knowledge. In the Microsoft case, Truste ruled that Microsoft was not in violation of their Truste certified privacy policy because the information was collected via software, and not from the actual Microsoft website.

The problem that advocates of self-regulation have confronted, and likewise, the advocates of federal legislation, is that the policy problem at hand is as complex and multi-faceted as the structure and functioning of the Internet itself. In the next section, I will turn to explore the origins of the Internet, its technological structure, and the problems of privacy in this revolutionary new medium.

Origins of the Policy Problem: The Commercialization of the Internet

If the mere emergence of databases in the 1960's and 1970's were representative of a new threat to privacy, then technological advances in networking capabilities have further enhanced these threats exponentially. The centerpiece of the information revolution to date has most certainly been the Internet. The Internet is an outgrowth of ARPANET, a government project launched in the early 1960's by the Advanced Research Projects Agency.²⁸⁵ ARPANET was created to enable transfers of data between computers operated by the military, defense contractors, and universities in the United States. The project was established in the aftermath of the launch of Sputnik by the U.S.S.R. in 1957, and the task of ARPA was to develop a network that would both take advantage of the new computing ability of Command and Control, and assure that the network could sustain a nuclear attack.²⁸⁶

The Internet functions based on a complex set of rules, or protocols, that define how a computer can communicate with another computer. The communication is facilitated via high-speed data connections between nodes, or host computers that route data across the Internet. In 1991, Tim Berners-Lee developed the "World Wide Web", which was a web of inter-linked documents residing on Hypertext Transfer Protocol

²⁸⁴ See www.truste.com and www.bbbonline.com

²⁸⁵ Michael Hauben, "Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet". <http://www.dei.isep.ipp.pt/docs/arpa--1.html>

²⁸⁶ *ibid.*

(HTTP) servers located throughout the world, written in Hypertext Markup Language (HTML), and identified by Uniform Resource Locators (URL's). The technical specifications for the World Wide Web made it an extremely useful means of presenting visual and multimedia information and providing access through hypertext links to different documents. In 1991, the backbone of the Internet, the National Science Foundation's NSFNET, lifted its ban on commercial network traffic, and in 1995, NSFNET reverted back to a research project, leaving the Internet in the hands of commercial interests.²⁸⁷

The Internet's technical qualities have revolutionized how data can be stored and accessed, and it has facilitated the development of a number of revolutionary communications technologies. However, the technical qualities that have revolutionized the information age also have a negative dimension, in that they facilitate a tremendous capability for surveillance. The negative consequences of information collection on the Internet results from what Paul Schwartz identifies as the "privacy horror show". The "privacy horror show" includes information collected on personal computers, information collected by Internet Service Providers (ISP's), and information collected by web sites.

One's personal computer can contain an extraordinary amount of privacy sensitive information that most computer users are unaware of. First of all, a personal computer can betray one's confidences by failing to destroy documents that users sought to remove through deletion.²⁸⁸ Information that is deleted from computers can generally be recovered easily, because deleting a file does not destroy the information, it only hides it from view unless the hard drive is formatted. Not only can information be recovered from the personal computer, but it can also be recovered from any other part of the network system where the data has resided, regardless if it was deleted. Secondly, web browsers contain software protocols that create files that store information detailing which web sites have been visited by the browser. These can be easily accessed by accessing the "history" menu in the browser or by looking at "drop down files" on the browser's location bar. Although these functions have value for computing use, they can also reveal exactly which websites have been visited, on which day, and in which order. Thirdly,

²⁸⁷ PBS Internet Timeline. <http://www.pbs.org/internet/timeline/timeline-txt.html>

²⁸⁸ Paul M. Schwartz, "Privacy and Democracy in Cyberspace". *Vanderbilt Law Review*. Vol. 52, p. 1623.

personal computers can reveal confidences by accepting cookies, also known as "persistent client-side hypertext transfer protocol files".²⁸⁹ Cookies are the digital equivalent of an identification tag, which website operators place on the hard drive of web users to identify the user as a previous visitor and allow the site to match the details of the previous visit. Most web browsers are configured to automatically accept cookies, and consequently the placing of cookies goes unnoticed in the background, and without consent. I will further explore how the use of cookies can be problematic in a later section on online profiling.

The second dimension of the privacy horror show is the collection of information by Internet Service Providers (ISP's). ISP's are the onramp to the proverbial 'information super highway' and the supplier of connectivity. They have access to detailed and potentially sensitive information ranging from consumer behaviour on the Internet, to clickstream data that can reveal detailed information about what sites one visits, what kind of information they access, and with whom they communicate. Consumer information can be compiled, matched with direct marketing information, and shared with strategic partners. The consequences however can be far more severe than a matter of a direct marketing nuisance, as one high profile case has demonstrated. In the U.S. federal case *McVeigh v. Cohen*, Timothy McVeigh, a nuclear submariner with the navy, had sent an email to a colleague's wife regarding a charity, but he inadvertently sent it from his private email userid 'boysrch', an email alias that he received as an American Online Customer.²⁹⁰ The colleague's wife searched the AOL member's directory and found an anonymous profile that specified 'boysrch' was in the military, worked in Honolulu, and his marital status was listed as gay. When this was brought to the attention of the navy, an investigator contacted AOL to ask for the identity of 'boysrch', without revealing that he was a government official. Despite their established policy, AOL promptly handed over the information.²⁹¹

The third dimension of the online privacy horror show concerns the collection of information at websites. A number of web sites on the Internet collect a great deal of

²⁸⁹ *ibid.* p. 1624.

²⁹⁰ *ibid.* p. 1629.

²⁹¹ See also "AOL Admits Error in Gay Sailor Case", Jan. 21, 1998. www.nytimes.com/aponline/w/AP-Navy-Gay-Dismissal.html

personal and sensitive information from consumers. In fact, the Federal Trade Commission suggests that up to eighty-five percent of web sites collect personal information.²⁹² This information is typically collected using a variety of techniques, including through the use of cookies, through filling in information in online application and registration forms, and via sweepstake and contest schemes. In addition to personally identifiable information, other information is collected through transaction logging. Most commercial web sites keep detailed logs of the transactions they perform. These logs are used to provide statistics on service use, track peak usage times, and provide data to assist in troubleshooting problems. In both its aggregate and identifiable forms, these are the typical means in which information is collected. Other techniques are more sophisticated and problematic, and I will turn now to examine these techniques of surveillance.

The Privacy Problem

Computers do not inherently invade privacy. The process by which information is collected about individuals through technologies is based on conscious decisions by system designers, software developers, and business owners, and often with unintended consequences. It is no more complex to build a system that is considerate of privacy than it is to build one that is privacy invasive. However, information is fast becoming a type of currency on the Internet. To offset the cost of delivering services, entertainment, or information, many websites generate revenue through advertising, and they want to know as much about their market as possible to maximize potential revenue. Many Internet users are happy to participate in the information-for-services barter. However, while many companies are open and transparent about their information practices, others are not. Techniques of surveillance are becoming increasingly more sophisticated, clandestine, and prevalent. The use of 'spyware', or advertising supported software (adware) is a case in point.

One way in which shareware²⁹³ authors can make money from a developed product, other than selling it to their users, is to offer a version of software that is supported by advertising. While many users will consider this a fair trade off, the cost to

²⁹² Op cit. Schwartz. p. 1629.

²⁹³ Shareware is software that is distributed free of charge. Often times shareware is a scaled back version of an enhanced product that users can purchase if they are satisfied with the product and would like to pay for improved functionality.

privacy is that often times advertising companies install tracking software on the user's system that is continuously "calling home" and reporting statistical data to the adware servers.²⁹⁴ Often times adware is installed without the knowledge or consent of the user. The software communicates in complete secrecy, sending information about the surfing habits to a remote, often undisclosed location, and in some cases the software establishes a 'server' on the user's machine to solicit advertising from foreign servers. Furthermore, many adware programs are designed so that they cannot be deleted from the user's machine, even if the shareware program that the advertising supported is uninstalled.²⁹⁵ It continues to operate in the background, reporting the users every movement across the Internet.

Millions of Internet users are using advertising supported 'spyware', and it is likely that many users are unconcerned about the privacy costs. However, many more are uninformed of the techniques of surveillance that proliferate across the Internet. Although the issue of 'spyware' has not yet been examined by regulators or received much public attention outside the privacy community, the issue of 'online profiling' by network advertisers has been a particularly politically salient issue of late. I will now turn to analyze the practice of online profiling and examine how the issue achieved agenda-setting status by way of attention to a 'focussing event'.

A Closer Look: Online Profiling

Advertising on the World Wide Web has grown exponentially with the explosion of the Internet. So too have online advertising revenues. Since 1996, it is estimated that revenue generated from the online advertising industry has grown from \$301 million to approximately \$4.62 billion in 1999. This massive growth is estimated to accumulate to \$11.5 billion by 2003.²⁹⁶ Most of this advertising revenue is generated through the delivery of "banner ads" by ad serving companies that are displayed on various web pages. Typically, banner ads are graphic advertisements that appear in designated locations on web pages, and these ads are generally located strategically above or to the side of the primary content that is displayed on the page. A tremendous number of

²⁹⁴ See Steve Gibson's "Privacy and Spyware Info on the Net". <http://grc.com/oo/news.htm>

²⁹⁵ See www.spychecker.com/spyware.html

²⁹⁶ See Jupiter Communications, <http://www.jup.com/sps/research/service2.jsp?service=ADV>

advertisements are served by advertising agencies, and the number of ads that are displayed each month are in the billions. DoubleClick, the largest of the network advertising companies, estimates a delivery rate of roughly 1.5 billion advertisements each day, for a total of approximately 45 billion ads per month.²⁹⁷ Typically, these ads are not selected by the particular website that is visited by the consumer, but by a network advertising company that specializes in the management and delivery of electronic advertisements.

The delivery of an advertisement is often not a 'one way' transaction. Most network advertising agencies do not only supply and deliver the ads, but they also collect data about the individuals who receive advertising on the web page that is visited. To collect information on the consumers who view the advertisements, network advertising agencies employ techniques that track the individual's activity on the Web. One of the most prevalent techniques to accommodate this is through the utilization of 'cookies'. There are two types of cookies: session cookies and persistent cookies. Session cookies are used to communicate to the web server that a particular individual is engaged in a session with the web server.²⁹⁸ Session cookies expire once the browser is closed. Persistent cookies, on the other hand, do not necessarily expire, and may be used to identify an individual when they return to the site that placed the cookie.

"Web bugs" are also used to collect information on individuals. Also known as clear gifs or 1x1 gifs, web bugs are tiny one pixel by one pixel image files that are embedded into a web page and which are usually the same colour as the background colour in which it is embedded. Because of the size of the image and its colour coordination with the background, they are invisible to web viewers. Web bugs are used to send information back to the home server, including the IP address of the computer that loaded the 'bugged' page, the URL of the page on which the web bug appears, the URL of the web bug image, the time that the bugged page was accessed, the type of browser that the individual is using, and the identification number of any cookie on the individual's computer that was placed by the web server. The existence of a web bug can

²⁹⁷ See DoubleClick's ad serving solutions at http://www.doubleclick.net/us/advertisers/adserving/default.asp?asp_object_1=&

²⁹⁸ For example, a session cookie might be used to confirm that an individual has certain permissions to access pages that might not be accessible by others, as in the case of using a web-based email program.

only be detected by searching through the actual source code of the page that contains the web bug. In some circumstances, web bugs can be used to place a cookie on a computer to synchronize an email address with a cookie i.d., rendering an anonymous profile personally identifiable.²⁹⁹

Cookies and web bugs are limited in the types of information that they can collect. This includes the type of information that is on the website visited by consumers, the time and duration of the visit, query terms that individuals use at search engines, a history of past purchases, whether an individual "clicked" on an advertisement on a page (click-throughs), and the website address from which the individual came from (the referring page). Cookies can collect this information without the consumer ever even clicking on an advertisement banner.

Typically, the information that is collected by network advertisers is anonymous. Rather than identifying individuals by name, profiles are often linked to the identification number of the cookie that is placed on the individual's computer by the advertisers web server. However, a number of network advertisers derive their profiles by merging the non-identifiable information in cookies with personally identifiable information. There are two common and prevalent methods of identifying an individual to merge personally and non-personally identifiable information to complete the profile. The first method requires the cooperation of a website that collects personal information and the network advertiser. In this scenario, a cooperating website collects personally identifiable information, such as their name, email address, gender, age, mailing address, phone number, level of education, profession, and often a survey of the individual's consumer interests. It is not unusual for websites to require individuals to register their information in exchange for access to information or the use of services such as free email. This information is then provided to the network advertiser. In this case, a previously anonymous profile consisting of information retrieved from cookies could be linked to an individual by a different identification number provided by a cookie containing the personal information. A second way that a profile can be made personally identifiable is if a website incorporates personally identifiable information into a URL (uniform resource locator) string that is transmitted to a network advertiser through its cookie. For

²⁹⁹ See Richard M. Smith's "The Web Bug FAQ". <http://www.tiac.net/users/smiths/privacy/wbfaq.htm>

example, if a user inputted personal data on a page and then navigated to a different page on the same site, the URL string could incorporate the users name, in the string so that they could continue to be identified by the web site.³⁰⁰

Once consumer information is collected, it can be automatically sorted, analyzed, and combined with demographic and psychographic information from third party sources, including an individual's online and offline purchases, their inferred interests and preferences, and other information that was collected from surveys and registration forms. The end result is a potentially extremely detailed profile that can be used to predict the individual's tastes, needs, and purchasing preferences. This profile can then be used to make split second computer automated decisions regarding which advertisements are delivered to a particular individual and targetted to their specific consumer interests.

Due to the enormous scope and magnitude of consumer profiling practices on the Internet, these consumer profiles can be extremely detailed. Some network advertisers claim that their profiles contain as many as 800 different "interest categories".³⁰¹ Cookies placed by network advertising companies can track individuals on any website that is served by the network advertiser, allowing data to be collected by the same source across unconnected, disparate, and unrelated sites on the Internet.³⁰² When this "clickstream" data is combined with other third party information, the profiles can include hundreds of distinct data fields.

The profiling of individuals on the Internet is an omnipresent and ubiquitous practice. It is also often invisible to consumers. The advertising banners that are placed by network advertisers appear seamless on the web pages in which they are displayed. Furthermore, the visitor to the website has no knowledge that a cookie is being placed on his or her machine unless the default setting in the web browser being used to view the page has been changed to provide notification of cookie placement. Unless a website

³⁰⁰ In this regard, the URL string might be composed something like this:

http://www.privacyinvasivesite.com/newuser/david_todd/bd08091974g=male.htm

In this hypothetical example, [privacyinvasivesite.com](http://www.privacyinvasivesite.com) lists the users name, date of birth, and gender in the URL string. If the site serves banner advertisements, then the advertising company would receive this URL string because they record all referrer URLs.

³⁰¹ See <http://www.engage.com/press/releases/2qfiscal.htm>

³⁰² It is not uncommon for network advertisers to deliver advertising to 1000 or more sites on the Internet, making their advertising network large and capable of collecting an immense amount of consumer information.

provides notification of the advertising networks presence in a privacy policy, individuals may be totally unaware of the fact that their online activities are being monitored.³⁰³

One particular "focussing event" involving the Internet advertising company DoubleClick Inc. captured the essence of the debate over Online Profiling. The conflict between privacy advocates and corporate interests around the proposed merger of online and offline databases captured the attention of both the print and electronic media, privacy and consumer advocates, the government, the courts, Wall Street, and corporate boardrooms throughout the world. In the shadows of pending legislation, this particular conflict personified the issue at stake and epitomized the balancing of interests to resolve the dispute over online profiling.

The Privacy Alarm

On June 14, 1999, DoubleClick Inc., the Internet's largest network advertising company and the "leading provider of comprehensive global Internet advertising solutions for marketers and web publishers", announced that it had signed a definitive merger agreement with Abacus Direct Corporation in a \$1 billion stock for stock transaction. Abacus Direct is the leading provider of information and research to the direct marketing industry in the United States, and they operate and manage the largest proprietary database of consumer catalog buying behavior. Abacus collects purchase data from over 1,100 consumer catalogs. The information that Abacus collects grows quickly, and it has compiled comprehensive five-year buying profiles on over 88 million U.S. households. Abacus then sells the profiles that it has compiled to catalog companies who want to pinpoint their target audience. In merging the two companies, Abacus Direct and DoubleClick could combine their resources of consumer information and Internet target advertising technology to provide their clients with "comprehensive, full service marketing and advertising solutions".³⁰⁴

³⁰³ Even if a privacy policy does mention the use of a network advertiser, it is often worded in vague language that does not communicate the implications of profiling. For example, network advertisers encourage their partner websites to post that "third parties" may use cookies to assist in the personalization of the surfing experience and to provide content relevant to your preferences.

³⁰⁴ DoubleClick, Inc. *Press Release*. DOUBLECLICK, INC. AND ABACUS DIRECT CORPORATION TO MERGE IN A \$1 BILLION STOCK TRANSACTION - Merger Creates The World's Leading Online Advertising And Database Marketing Company. NEW YORK, NY, 6/14/99.
http://www.doubleclick.net/us/corporate/presskit/pressreleases.asp?asp_object_1=&press%5Frelease%5Fid=2327

The justification for the merger was clear in press release statements by the Chief Executives of the two companies. Kevin O'Connor, Chairman and CEO of DoubleClick suggested that the most important aspect of the merger would be that the combination of the two companies "further enhances our (DoubleClick's) ability to deliver the right advertising message, to the right consumer, at the right time." Similarly, Tony White, Founder, Chairman, and CEO of Abacus said "this merger combines two high growth, industry leading companies to create a powerful and unique online advertising and marketing entity. DoubleClick's online ad serving technologies and media expertise, will enable consumers to receive the most relevant and effective messages at the right time."³⁰⁵

Other comments were more candid and suggestive. Referring to DoubleClick's current DART (Dynamic Advertising Reporting and Targeting) technology that is only able to target advertisements based on general information that is collected from web surfer's online behaviour, Kevin O'Connor suggested that "the final piece of the [targeting] puzzle is data . . . no one knows more about the data business than Abacus Direct."³⁰⁶ The combination of this data with DoubleClick's profiles of online clickstream data provides the companies with an opportunity to deliver potentially perfectly targeted advertisements. By using cookie technology to positively identify a web browser by an identification number and matching that information with identifying information, DoubleClick would know exactly who the person is.³⁰⁷ Abacus CEO Tony White announced that they would "be relating everything to a name and address . . . we'll hang additional information on that." The profile data that DoubleClick has collected and accumulated would be inputted into the Abacus Database to be matched with the offline data.

³⁰⁵ *ibid.*

³⁰⁶ Craig Bicknell, "DoubleClick's Single Focus: You". wired news: www.wired.com June 14, 1999, 2:30 p.m. PDT.

³⁰⁷ The Cookie that DoubleClick places identifies the web browser, not the individual. For example, if a number of people used the same web browser for using the Internet, DoubleClick's Cookie records the navigational and transactional information of all the users from the same Cookie(s).

The Dynamics of Conflict

Initial Publicity

DoubleClick's decision to merge with Abacus Direct came at a time when privacy abuses in the private sector were gradually becoming a politically salient issue. Growing concerns over Internet privacy and an expanding debate on the ability of the private industry to self regulate its privacy practises has drawn increased attention from the Internet media, public interest groups, the Federal Government, and individuals on the Internet. Jason Catlett, president of Junkbusters Corp, a privacy clearinghouse and consulting firm for Internet companies and outspoken privacy advocate immediately attacked the proposal to merge the two companies and their massive databases. Catlett commented that "(t)his is potentially the end of anonymity on the Internet", and suggested that it represented "a degree of surveillance that is totally unacceptable".³⁰⁸ Likewise, Marc Rotenberg, the Executive Director of the Electronic Privacy Information Center (EPIC) suggested that the merger "is a red flag for privacy advocates. What they are doing is simply wrong".³⁰⁹ Rotenberg attempted to demonstrate that this represents how and why self-regulation is not a viable solution, noting "that is why we've been trying to make the case against self regulation: These policies quickly collapse when an opportunity presents itself, and that is what we are seeing here."³¹⁰ DoubleClick and Abacus contended however that the interests of consumers had been put first by providing them with the option to remove themselves of the databases by "opting-out" and to deliver personalized advertising content to surfers and relevant marketing information to their customers.

Privacy advocates also noted immediately following the announcement that the business plan proposed by the companies contradicted the "spirit" of DoubleClick's privacy policy, which promised not to collect "any personally identifiable information about you, such as your name, address, phone number, or email address".³¹¹ Although

³⁰⁸ op cit. "DoubleClick's Single Focus: You".

³⁰⁹ Macavinta, Courtney. "Consumer group to fight DoubleClick deal". June 14, 1999. *CNET News.com*.
<http://www.news.cnet.com/news/0-1007-200-343608.html>

³¹⁰ *ibid*.

³¹¹ see <http://www.doubleclick.net/us/corporate/privacy/> DoubleClick has since updated its privacy policy, and changes to the policy are not dated or archived for public access. DoubleClick's privacy policy states

DoubleClick claims not to collect personal data through the cookies that are placed when an advertising banner is displayed, they do facilitate the exchange of data in its network of more than 1300 websites and 1100 merchandise catalog companies.³¹² O'Connor noted at the press conference that participants in the DoubleClick network would have the ability to make the match by name and address.

Despite outrage by privacy advocates and news that consumer groups were planning to file a complaint with the Federal Trade Commission (FTC) on the grounds that the merger could create an unprecedented database of personal information without obtaining prior consent, DoubleClick's President Kevin Ryan refused to acknowledge any problematic privacy implications, noting "(w)e don't think it's an issue." "We spent a lot of time on this in discussing the merger-- if consumers are not happy, neither one of us has a business."³¹³ Both DoubleClick and Abacus Direct are leading members of the Online Privacy Alliance and the Direct Marketing Association. The mission of the Online Privacy Alliance is "to lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce".³¹⁴ Similarly, the Direct Marketing Association acts on behalf of its members to encourage the growth and profitability of companies in the direct marketing industry and encourage adherence to high ethical standards.³¹⁵ Despite their claims to act in the best interests of consumer privacy, privacy advocates were critical of DoubleClick's opt-out model and their focus on the principle of notice rather than on informed consent. When asked if DoubleClick would get consent from web surfers and profiled consumers about the merging of offline and on line data, Kevin Ryan announced that "we're not in a position to do that" adding "we would encourage everyone to have a full disclosure, and we are going to absolutely stick to the opt-out policy." ³¹⁶ DoubleClick argued that there was no demand from the public for prior consent, suggesting as evidence the fact that only ten people per day opt-out of the DoubleClick

that they may update the policy at any time without notice, suggesting that individuals should check for changes periodically as it changes "from time to time".

³¹² Op cit. "Consumer group to fight DoubleClick deal".

³¹³ Macavinta, Courtney. "DoubleClick not worried about privacy charges". CNET News.com. June 15, 1999. <http://www.news.cnet.com/news/0-1007-200-343680.html>

³¹⁴ <http://www.privacyalliance.org/mission/>

³¹⁵ <http://www.the-dma.org/aboutdma/whatisthedma.shtml>

³¹⁶ "DoubleClick not worried about privacy charges". ibid.

network out of 75 million people per month who view DoubleClick ads and receive their cookies.

Escalation

To protest the proposed merger of DoubleClick and Abacus, privacy advocates and consumer groups planned to launch a relentless campaign reminiscent of campaigns against Intel's Pentium II processor, and the online protests against Lotus Marketplace and the Clipper Chip. Fearing that the merged company would facilitate the exchange of a wide range of highly detailed and potentially sensitive information, the coalition against DoubleClick targeted action towards their adversaries where it was potentially most vulnerable - on Wall Street.

On June 21, 1999, a coalition of privacy advocates³¹⁷ wrote an open letter to Kevin O'Connor and Tony White urging them to abandon the proposed merger of the companies on the grounds that "it would severely undermine the privacy of Internet users." The letter suggested that the merger would only make economic sense if their intention was to link the 88 million household files in the Abacus database with the 30 million cookies in the DoubleClick DART database. The letter also described how the DoubleClick and Abacus network would combine information resources to profile consumers both on the Internet and off. The privacy advocates suggested that the most important damage that would be caused by the DoubleClick/Abacus merger would be a fundamental change in the nature of the Internet: "from one where people are usually anonymous as they move around the Web, to one where they are usually silently identified unless they consistently work to protect their anonymity."³¹⁸

The privacy advocacy coalition also criticized the opt-out policy and highlighted its insufficiency. Their argument was that opt-out mechanisms are meaningless if an individual is not aware that they are being profiled, or the extent to which their information is collected, used, and disseminated. Furthermore, they suggested that the

³¹⁷ The letter was signed by Jason Catlett of Junkbusters Corp., Marc Rotenberg of EPIC, David Banisar of Privacy International, Ed Mierzwinski of US Public Interest Research Group, Jeff Chester, Center for Media Education, and Beth Givens of Privacy Right Clearinghouse. The letter was copied to John McCain and Ernest Hollings of the Senate Commerce Committee, John Ashcroft and Richard Bryan of the Subcommittee on Consumer Affairs, Thomas Bliley and John D. Dingell of the House Commerce committee, and Billy Tauzin and Ed Markey of the Subcommittee on Telecommunication, Trade and Consumer Protection.

opt-out mechanism that DoubleClick uses is particularly problematic. When one opts-out of the DoubleClick network, a cookie is placed on the machine that tells the DoubleClick server not to place a cookie. If someone deletes his or her cookie file, the opt-out cookie is also deleted and the individual will no longer be opted-out of the system. The coalition against DoubleClick noted the inadequacy of the cookie technique suggesting it was analogous to "an inn keeper offering do-not-disturb signs instead of locks on guest room doors."³¹⁹

DoubleClick opponents also wanted assurances that the DART system, which delivers targeted ads to consumers with the use of cookies, would live up to the company's privacy policy. The policy promises not to collect "any personally identifiable information about you, such as your name, address, phone number, or email address."³²⁰ The advocate's letter went on to state that "if you are willing to issue a guarantee that the merged entity and successors will never associate a name and address with a cookie without the affirmative informed consent of the individual concerned, please state this in public."³²¹

In addition to formally objecting to the DoubleClick and Abacus merger and explaining the privacy implications of it, the coalition announced that a campaign would be undertaken in a similar fashion as the campaigns against Intel over their Processor Serial Number and Microsoft over their Global User Identifier. The Campaign would include the following measures:

- An appeal to shareholders of DoubleClick and Abacus to disapprove the merger
- An appeal to the Federal Trade Commission or Department of Justice to disapprove the merger under the Hart Scott Rodino Act
- An appeal to the FTC to enjoin business practices by the merged entity as unfair or deceptive under the Federal Trade Commission Act
- A call to socially responsible mutual funds to divest their holdings in the company

³¹⁸ Open Letter 6/21 asking the companies to abandon their merger. <http://www.junkbusters.com>

³¹⁹ *ibid.*

³²⁰ Marinaccio, Wendy. "Privacy advocates blast DoubleClick merger", *CNET News.com*. June 21, 1999. <http://news.cnet.com/news/0-1005-200-343915.html>

³²¹ *Op. Cit* Open Letter 6/21/99.

- A public education campaign on the privacy risks of online advertising and catalog buying, and the benefits of ad blocking software and opting out of list sales
- A call for Congressional oversight of hearings on the proposed merger as well as possibly an evaluation of the entire enterprise of industry self-regulation to protect privacy. (They noted that the Online Privacy Alliance, which is a coalition of large companies that oppose laws to protect privacy, has not expressed any opposition to the merger.)

DoubleClick did not respond to the concerns of the privacy advocates, or acknowledge their request for a meeting.

On June 29, 1999, the coalition of privacy advocates addressed an open letter to the Stockholders of Abacus Direct. The letter explained why the advocates believed that the disapproval of the merger is the right choice both on public policy grounds and in terms of the Stockholders economic interests.³²² It also raised the question of whether or not the Stockholders had been misled or inadequately informed about the privacy-related risks of the two companies' past behavior and their proposed merger. For example, the letter pointed to DoubleClick's statements in its SEC filings that suggests that its officers are either unaware of the legal and political environment with regards to privacy and their business in Europe, or they deliberately concealed important information regarding difficulties and risks from investors. The only mention of privacy in the SEC filing (July 17, 1999) was the following:

(q) Company has conducted its business and has collected, maintained and used its data at all times in accordance with (i) accepted industry practice standards promulgated by the Direct Marketing Association, and (ii) all applicable Laws, including but not limited to those affecting privacy issues.³²³

This contention is disputed by the privacy advocates. They concluded that DoubleClick's privacy practices are "more likely than not" in violation of laws in many European countries that limit non-consensual data collection including countries in which

³²² They suggested that the merger would be disadvantageous to Abacus on purely economic grounds, noting the disparity of Abacus' record of profitability and DoubleClick's history of huge expenditures and lack of profitability. They also suggested that the Internet banner ad model is "broken" and that click rates are declining.

³²³ DoubleClick's 8-K SEC filing, conformed June 13 1999. Available at:
<http://www.sec.gov/Archives/edgar/data/1049480/0001005477-99-002865-index.html>

DoubleClick is established. They also contended that in an earlier SEC filing (May 20, 1999), DoubleClick provided "a very inaccurate picture" of the 1995 European Union Directive.³²⁴ They were also critical of DoubleClick's silence regarding the potential for legislated privacy laws in the United States and a failure to address the Safe Harbor negotiations undertaken between the U.S. and the European union. Finally, the letter warned that because of these privacy concerns, the merged company may not be able to engage in the practices that provided the rationale for the proposed merger of the company.

In the summer of 1999, concern over privacy on the Internet continued to garner considerable attention. The Federal Trade Commission provided a Report to Congress in July 1999 entitled "Self-Regulation and Privacy Online". The report examined the role and effectiveness of industry attempts to self regulate privacy practises. The report acknowledged what privacy advocates had suggested; that individual's were concerned about their privacy online and that these privacy concerns were a barrier to entry into participation in electronic commerce. The report also noted that eighty-seven percent of recent survey respondents are somewhat or very concerned to threats to their privacy online.³²⁵ Seventy percent of respondents in a different survey reported that they were uncomfortable with providing information to businesses online.³²⁶ The report also found that only 1/4 of Internet users felt comfortable enough to engage in electronic commerce.

The Report to Congress also addressed the adoption of self-regulatory measures by industry. The FTC commended the industry for its success in implementing fair information practices and the emergence of private sector seal programs that require its licensees to abide by fair information practices. The FTC report concluded that no new

³²⁴ The filing, located at <http://www.sec.gov/archives/edgar/data/1049480/0001047469-99-021740.txt> contained the following paragraph: "The European Union recently enacted its own privacy regulations that may result in limits on the collection and use of certain user information. The laws governing the Internet, however, remain largely unsettled, even in areas where there has been some legislative action." The coalition against DoubleClick suggested that the DoubleClick ignores the EU regulator's statements that the medium of dataflows, whether through the Internet or other means, is irrelevant to the Directive's application. *See Recommendation 1/99 on Invisible and Automatic Processing of Personal Data Performed by Software and Hardware* at

<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp16en.htm>

³²⁵ See Lorrie Faith Cranor et al., "Beyond Concern: Understanding Net Users Attitudes about Online Privacy". <http://www.research.att.com/projects/privacystudy>

³²⁶ Federal Trade Commission, "Self-Regulation and Privacy Online: A Report to Congress". July 1999. <http://www.ftc.gov/os/1999/9907/privacy99.pdf>

laws are needed at this time. Although the FTC suggested that "the implementation of fair information practices is not widespread among commercial web sites" they concluded that "legislation to address online privacy is not appropriate at this time."³²⁷

The Federal Trade Commission's Report to Congress also put the issue of consumer "online profiling" on the political agenda. A workshop on Online Profiling would be jointly sponsored by the FTC and the U.S. Department of Commerce to examine online advertising firms use of cookies and use of tracking technologies to develop targeted, user-profile based advertising campaigns.

On the eve of the FTC Online Profiling workshop, a number of rights groups and consumer advocates asked the government to ban the practice of online profiling. These groups declared that the tendency towards industry consolidation in the marketing business poses a tremendous threat to consumer privacy. The advocates used the example of the DoubleClick and Abacus merger as a focussing event to communicate the techniques of network advertisers and the consequent privacy implications of engaging in such practices.

The Online Profiling workshop brought together members of industry, consumer and privacy advocates and the government.³²⁸ The task at hand was to assess the costs and benefits of online profiling and to gauge the scope of the industry, understand the activities and technological capabilities of network advertisers, and address any privacy concerns. Various industry representatives defined their business models, explained the basic design architectures of their information systems, and presented their public policy positions.

The first session explored information technologies - both those that are currently in use and those in development - that facilitate profiling of consumers online. This session focussed on the extent to which these technologies permit the integration of information that identifies consumers as individuals with non-identifying information.³²⁹

³²⁷ *ibid.*

³²⁸ The transcript of the workshop can be found at <http://www.ftc.gov/bcp/profiling/online.pdf>.

³²⁹ Presenters included Michael Griffiths, Chief Technology Officer and Vice President of MatchLogic, Inc. and Daniel Jaye, Chief Technology Officer of Engage Technologies, Inc. Panelists included Jason Catlett, President of Junkbusters Corporation, Lori Feena of Electronic Frontier Foundation, Kunwar Chandrajeet Singh, President of Cyberknowhow, Inc. Richard M. Smith, Internet Consultant, Daniel Weitzner, Director of Technology and Society and Domain Leader of the World Wide Web Consortium, and Eric Wenger, New York State Attorney General's Office

The second session examined the extent to which online profiling technologies impinge upon consumer privacy, and discussions considered the costs and benefits of online profiling for both consumers and businesses.³³⁰ The final panel examined the potential of self-regulation as a means of addressing the privacy concerns raised by online profiling. This session also examined ways in which profiling technology can be deployed to promote adherence to fair information practices.³³¹

Intensification

Perhaps the most significant outcome of the workshop was the emergence of a new coalition of industry advocates. The Network Advertising Initiative (N.A.I) is composed of 90% of the leading providers of advertising solutions to web publishers and advertisers on the Internet, and includes 24/7 Media, AdKnowledge, Adsmart, AdForce, DoubleClick, Engage, Flycast, MatchLogic, NetGravity and Real Media.³³² The purpose of the N.A.I. is to promote the development of a self-regulatory framework to govern the practices of network advertisers, to increase consumer confidence in the medium, and to contribute to the growth of electronic commerce.

The workshop provided the industry with the opportunity to establish the three key tenets of the Network Advertising Initiative. First, the N.A.I. announced that each company would continue to provide consumers with a clear explanation of the information it collects, how that information is used, and the benefit to consumers of such use. Second, the N.A.I. assured that for consumers who choose not to receive tailored

³³⁰ Participants included Bradley Aronson, President of i-frontier, Fred H. Cate, Professor of Law and Director of the Information Law and Commerce Institute, Indiana University School of Law, Jason Catlett, President of Junkbusters Corporation, Jeffrey Chester, Executive Director of the Center for Media Education, Austin Hill, President of Zero-Knowledge Systems, Inc., Deirdre Mulligan, Staff Counsel for the Center for Democracy and Technology, Daniel Jaffe, Executive Vice President of the Association of National Advertisers, Michael Rowsom, Senior Vice President of 24/7 Media, Jonathan Shapiro, Senior Vice President of Business Development, DoubleClick, Inc., Solveig Singleton, Director of Information Studies at the Cato Institute, Robert Ellis Smith, Publisher of Privacy Journal, and Shari Steele, Director of Legal Studies, Electronic Frontier Foundation.

³³¹ This panel included Paula Bruening, Director of Compliance and Policy for TRUSTe, Fred H. Cate, Professor of Law and Director of the Information Law and Commerce Institute at the Indiana University School of Law, Michael Griffiths, Chief Technology Officer and Vice President of MatchLogic, Evan Hendricks, Editor and Publisher of Privacy Times, Daniel Jaye, Chief Technology Officer of Engage Technologies, Inc., John Kamp, Senior Vice President of the American Association of Advertising Agencies, Dr. Steve Lucas, Chief Information Officer and Vice President of Government Affairs for PrivaSeek, Inc., Tim Lordan, Manager of the Online Privacy Alliance, Andrew Shen of the Electronic Privacy Information Center, Robert Ellis Smith, Publisher of Privacy Journal, Elizabeth Wang, General Counsel for DoubleClick, Inc. and David Zinman, Vice President of Marketing for AdKnowledge.

messages, each N.A.I. company either currently provides or will soon provide an easy-to-use method to opt out from such tailoring. Third, the companies committed to participate in consumer outreach and education programs and to let consumers know about the role that network advertisers play in the delivery of tailored messages over the Internet.³³³

The initiative website at www.networkadvertising.org was developed to promote consumer awareness about the industry and provide an easily accessible and convenient place for consumers to exercise choice regarding the use of their data.

The N.A.I. adheres to the fair information practices developed by the Online Privacy Alliance. Thus, Internet advertising websites owned or controlled by one of the participating companies are required to disclose their data collection and use practices on their websites in a clear, concise and conspicuous manner, and in language that consumers can understand. These disclosures would include:

- what data are collected and what data are not collected,
- how the data are used, including whether they will be combined with personally identifiable data from any other source,
- what other data are collected and how they are used, including the use of data for ad management, and
- what opt-out procedures are available for consumers who decline to have data used to create a profile.

With regard to personally identifiable data, the NAI also formulated a self-regulatory policy. First, companies that collect these data will notify consumers about the collection and use of their data, and at a minimum, will let consumers opt-out of unrelated or secondary uses at the time these data are collected. Second, if the data is linked to other personally identifiable information, the companies will give consumers the opportunity to opt-out. Third, in accordance with fair information practices, the companies that collect personally identifiable information will make reasonable efforts to provide timely and

³³² Information on the Network Advertising Initiative can be found at <http://www.networkadvertising.org>

³³³ Transcript of workshop, <http://www.ftc.gov/bcp/profiling/online.pdf>

See also the NAI press release at <http://www.networkadvertising.org/press/11-9-99-testimony.shtml>

appropriate access to that information under policies that each of the participating network advertisers will post on their websites.

The network advertisers explained that there is some information that network advertisers collect that consumers will not be able to opt out of. This includes the transmission of data for basic ad management and statistical reporting purposes. This information is necessary to deliver the ads, and also to provide advertisers with information about how many users saw the campaign.³³⁴

To address the issue of oversight and supervision, the N.A.I. companies committed to not only complying with these principles but also to join or retain a third party organization that provides for periodic audits of compliance with their privacy policy. This includes organizations such as TRUSTe, BBB Online, Webtrust, and other nationally recognized accounting firms that provide these services.

Privacy advocates and consumer groups were critical of the Networking Advertising Initiative's insistence of a strictly opt-out policy, and in particular in situations where the information that is collected is personally identifiable. Furthermore, because the information contained within online profiles can be connected to offline individuals, consumer advocates argued that the full array of Fair Information Practices should apply to the situation.³³⁵

Because consumers may not know that they are being profiled, N.A.I. opponents suggested that their activities were potentially unfair and deceptive. Critics argued that online profiling results in a diminution of our autonomy, and thus, represents a violation of privacy. They suggested that autonomy is challenged because the consumer is manipulated in the marketplace, and often when vulnerable and without knowledge of profiling practices.³³⁶ Advocates pointed out that the Supreme Court ruled in 1995 that as a tort matter, targeted advertising at a vulnerable population is an invasion of privacy. Based on recent experiences in related areas³³⁷, consumer advocates concluded that there

³³⁴ The Network advertisers noted that it would be almost impossible for a website to sell advertising space without being able to tell the advertiser how many users will see their ads.

³³⁵ See additional Comments by Andrew Shen of EPIC.

<http://www.ftc.gov/bcp/profiling/comments/shen.htm>

³³⁶ <http://www.ftc.gov/bcp/profiling/online.pdf> Comments by Jeff Chester, Center for Media Education.

³³⁷ The self-regulatory model drew heavy criticism after Truste investigated privacy violations involving Microsoft and RealNetworks and the organization had no jurisdiction to penalize their actions. Microsoft was accused of using a Globally Unique Identifier in its Windows 98 Operating System Software.

is little reason to believe that self-regulation will provide sufficient protections from the potential privacy risks of online profiling. Consumer advocates continued to contend that strong privacy protections enforced by independent agencies were necessary.

On November 19, 1999, the same privacy advocates that participated in the previous open letter campaigns against the DoubleClick and Abacus merger released a third open letter. This time the 'target audience' was the managers of socially responsible mutual funds.³³⁸ The letter addressed the "harmful social effects of the imminent merger" and explained the current practices of the online advertising industry that are "severely damaging the fundamental human right of privacy."³³⁹ The privacy coalition also proposed a strategy to socially responsible investors:

- Divest any holdings of DoubleClick and Abacus Direct as soon as possible
- Add DoubleClick and Abacus to "screening" lists of companies that are to be excluded from investment based on socially criteria, specifically a disregard for human rights
- Dialog with the publicly-traded online advertising networks to persuade them to limit their data collection and not to associate profiles with offline identity
- Support programs of shareholder activism towards these ends by means such as submitting and voting proxy resolutions

The letter closed by stating that they believe that "privacy will be as important to socially responsible investing in the 21st century as health and pollution have been in the late 20th century".

On November 22, 1999, the eve of the vote to approve the DoubleClick/Abacus proposal, news stories on the Internet covered the privacy advocates battle against the information industry giants. The plan to merge net surfing habits obtained from 5 billion

RealNetworks was also using a unique identifier that was collecting the playlists of individuals using their RealJukebox software application. Both cases were ruled not to be in violation of their web seal because the information was not being collected from a website, but rather from software using the Internet. Incidentally, Maria Cantwell, Senate candidate in Washington State in the 2000 election was previously Senior Vice President of Consumer and e-commerce and Vice President of Marketing for RealNetworks, and one of the first ten employees of the company. She played a critical role in marketing the RealJukebox application, and ran a campaign championing privacy issues.

³³⁸ This included the managers of : Calvert Social Equity Fund, Citizens emerging growth fund, Domini Social Equity Fund, Dreyfus Third Century Fund, Parnassus Fund, Smith Barney Concert Social Awareness Fund.

³³⁹ "Open Letter sent to managers of socially responsible mutual funds", 11/19/1999.

cookies served per week with 2 billion personally identifiable consumer catalog transaction records was described by Jason Catlett as "a full frontal attack, funded by Wall Street, on anonymity on the Net".³⁴⁰ The privacy groups continued to call on the FTC to put a stop to the merger until there was a suitable development of a regulatory framework. The groups met with FTC Commissioners Sheila Anthony and Mozelle Thompson to persuade them to use its jurisdiction over unfair business practices, but to no avail. Requests to Abacus for a statement by *CNET* staff on the rally against the merger were referred to DoubleClick, however DoubleClick refused to comment.³⁴¹

DoubleClick's privacy policy, already under the microscope by its critics, was reviewed and under scrutiny by the press. Their policy stated that "in the course of delivering an ad to you, DoubleClick does not collect any personally identifiable information about you, such as your name, address, or email address." But DoubleClick does collect personal information such as those mentioned through surveys, registration, and purchase forms on sites that are operated by DoubleClick, such as NetDeals.com. The NetDeals.com privacy policy states that they combine personal information³⁴² with other information available about individuals, noting "this includes other personally identifiable information and certain non-personally identifiable information, such as browser type."³⁴³ In addition, The NetDeals.com site states that "we participate in the DoubleClick Information Alliance and share the information we have about you with that Alliance." DoubleClick's privacy policy however stated nothing of the Alliance, and there was no mention of it anywhere on the DoubleClick sites. Despite the anti-DoubleClick rhetoric reported by the press, the stock value of the two companies fared very favorably on Wall Street, with DoubleClick's shares closing with a 8.31 gain to \$158 per share and Abacus shares closing up 10.5 to \$167.31 per share.

On November 23, 1999, DoubleClick announced in a brief Press Release that it had completed the merger with Abacus following approval from the respective companies shareholders. Based on the previous day's stock value closing, the transaction was valued at approximately \$1.8 billion, with a combined market capitalization of the

³⁴⁰ Courtney Macavinta, "Privacy advocates rally against DoubleClick-Abacus merger". *CNET News.com*, November 22, 1999. <http://news.cnet.com/new/0-1005-200-1461826.html>

³⁴¹ *ibid.*

³⁴² In this case name, home and email address, and birth dates.

two companies at \$8.8 billion. Kevin O'Connor offered only a brief statement: "the merger with Abacus Direct, along with the recent closing of the NetGravity merger, will allow us to offer publishers and advertisers the most effective means of advertising online and offline."³⁴⁴

Privacy fears over the merger again made headlines when the *USA Today* reported that DoubleClick had begun to sign up sites to create a network tying web surfer's travels with their personal information and both online and offline shopping habits.³⁴⁵ Over 11,500 sites that belong to the DoubleClick Network could have access to the database, which would be correlated with the Abacus Database. DoubleClick noted that not all of the sites in the network would have the opportunity to join the Alliance - "they have to somehow have something to give to be a member of this," said DoubleClick Spokeswoman Jennifer Blum. "The goal here is to match up information."³⁴⁶ Jason Catlett, one of the leaders of the privacy coalition against DoubleClick was again in the press. "Privacy advocates have been saying for years that marketers will turn the Net into a gigantic data-gathering machine for junk mail, telemarketing, and advertising; now that machine is working."³⁴⁷

The next day, the mobilization of interests against DoubleClick continued to mount. The Electronic Privacy Information Center announced it was preparing to file a complaint with the Federal Trade Commission following the news that DoubleClick was merging their data profiles. *Privacyplace.com*, an online magazine dedicated to personal privacy issues warned and encouraged web users to boycott websites that share information with DoubleClick, if the names of those sites are ever made public.³⁴⁸

On January 27, 2000, a Californian woman filed a suit in Marin County Superior Court against DoubleClick, accusing the Web advertising firm of unlawfully collecting and selling consumers' private information.³⁴⁹ The lawsuit, *Judnick vs. DoubleClick Inc.*,

³⁴³ This indicates that this type of information is cookie information.

³⁴⁴ DoubleClick Press Release: "DoubleClick Completes Merger with Abacus Direct". November 23, 1999. http://ir.doubleclick.net/ireye/ir_site.zhtml?ticker=DCLK&script=410&layout=-6&item_id=66808

³⁴⁵ USA Today, January 25, 2000.

³⁴⁶ Courtney Macavinta, "Privacy fears raised by DoubleClick database plans". *CNET News.com*. January 25, 2000. <http://news.cnet.com/news/0-1005-200-1531929.html>

³⁴⁷ *ibid.*

³⁴⁸ www.privacyplace.com

³⁴⁹ The suit was filed by Hariett Judnick.

accused the New York-based company of using sophisticated technology to identify Internet users, track and record their Internet use and the Internet Web sites they visit, and obtain confidential and personal information about them without their consent. The suit asked the court to bar DoubleClick from using technology to collect personal information without the prior written consent of the Internet user.³⁵⁰ The suit also asked for a clear and simple method by which collected private information could be destroyed. It also asked that DoubleClick be required to destroy all records obtained without a customer's knowing consent.³⁵¹

Within days, lawsuits against the beleaguered company continued to mount. On January 28, 2000, four more cases were filed against DoubleClick in the courts. In a similar case to the previous days filing, *Bruce v. DoubleClick, Inc.* was filed in the U.S. District Court for the Northern District of California. *Healy v. DoubleClick Inc.* was also filed in the U.S. District Court for the Southern District of New York. This complaint alleged that DoubleClick improperly collected and used information concerning Internet users in violation of certain federal electronics privacy statutes, as well as common law trespass and invasion of privacy. The complaint also sought damages and injunctive relief on behalf of a defined class of Internet users. *DeCorse v. DoubleClick, Inc.* was filed in the Superior Court of the State of California, Marin County, on similar grounds. *Steinbeck v. DoubleClick, Inc.* was filed in the United States District Court for the Central District of California, and the claims were consistent with the previous filings. *Donaldson v. DoubleClick Inc.* was also filed in the U.S. District Court for the Southern District of New York on the first day of February, 2000. DoubleClick maintained that these lawsuits were without merit.³⁵²

Privacy advocates continued speaking out against DoubleClick and challenging the company's practices.³⁵³ "Who appointed them the Big Brother of cyberspace?" asked

³⁵⁰ *Reuters*, "DoubleClick sued over privacy: Internet advertising company accused of unlawfully obtaining and selling consumers' private personal information." January 28, 2000. www.zdnet.com/zdnn/stories/news/0,4586,2429053,00.html?chkpt=zdnurla

³⁵¹ Sandheep Junnarkar, "DoubleClick accused of unlawful consumer data use". *CNET News.com*, January 28, 2000. <http://www.cnet.com/news/0-1005-200-1534533.html>

³⁵² <http://www.sec.gov/Archives/edgar/data/1049480/0000950117-00-000281-index.html>

³⁵³ Pamela Parker, "DoubleClick Documents Reveal More Legal, Regulatory Troubles". http://www.internetnews.com/bus-news/article/0,,3_305521,00.html

Jason Catlett in the *Industry Standard*, another of the online and offline electronic industry magazines covering the escalation of the conflict.³⁵⁴

Within a week, the Center for Democracy and Technology organized a campaign against DoubleClick that encouraged the public to email complaints to DoubleClick and 60 of its clients to protest their privacy policies.³⁵⁵ The campaign called for a stop to the sharing of information by prominent Internet companies in the DoubleClick network which tracks individuals and ties that information with offline activities. In an email response to the CDT, DoubleClick denied that it collects information on personally identifiable individuals, noting that "DoubleClick does not and cannot know the identity of a user online unless that user has provided that information to an Abacus Online participant who has provided the user with the appropriate notice and choice."³⁵⁶ Within hours, a number of companies contacted DoubleClick about the protest,³⁵⁷ and the companies were informed that the protest was legal. *Thestreet.com*, a financial news and analysis site and DoubleClick customer, received in excess of 2,200 email messages within the first morning of the campaign alone. Although the CDT did not know which of the 60 companies shared personal information with DoubleClick, Ari Schwartz, a spokesman for the organization, acknowledged that they wanted the public to put pressure on all of 11,500 DoubleClick clients to protect consumer privacy, noting "we want these companies to be aware that their customers are concerned about this issue."³⁵⁸ The Center for Democracy and Technology confirmed that the protest was well under way, with a reported 6,000 e-mails forwarded to DoubleClick and 4,400 e-mails forwarded to DoubleClick's clients in the first four days of the campaign alone.³⁵⁹

³⁵⁴ Diane Anderson, "The Trouble with DoubleClick". *The Industry Standard Online*, January 28, 2000. <http://www.thestandard.com/article/display/0.1151.9261.00.html>

³⁵⁵ See <http://www.cdt.org/action/doubleclick.shtml>

³⁵⁶ Evan Hansen, "DoubleClick under email attack for consumer profiling plans". *CNET News.com*, February 2, 2000. <http://www.news.cnet.com/news/0-1005-200-1539478.html>

³⁵⁷ Among the companies included in the campaign were Alta Vista, Ask Jeeves, AuctionWatch, Blue Mountain Arts, Drkoop.com, Hewlett-Packard, Kozmo.com, Network Solutions, and the New York Times.

³⁵⁸ Op cit. Hansen.

³⁵⁹ Keith Perin, "Privacy Activists File DoubleClick Complaint: Watchdog group EPIC alleges ad firm violated federal law, merits investigation." *The Industry Standard*, February 10, 2000. <http://www.thestandard.com/article/display/0.1151.9694.00.html?nl=mg>

Denial

Despite the increased pressure by privacy advocates and what appeared to be the development of a consumer backlash against the company, DoubleClick persisted with its assertions that they were doing nothing improper and that consumers will benefit by getting more precisely targeted advertisements. "We are good actors", said Jonathan Shapiro, a senior vice president for DoubleClick. "We've been leaders in protecting consumer privacy for the past four years, and we think our commitment to providing notice and choice to consumers puts us ahead of the curve."³⁶⁰ David Sobel, the general counsel for the Electronic Privacy Information Center, disagreed with the DoubleClick spin. "This poses a much more widespread privacy threat than any situation we have seen before. All of this is happening invisibly to most consumers."³⁶¹

DoubleClick's Abacus Online division continued with their profiling plans despite the pending legal challenges and organized protests by consumer groups. The Abacus Online Alliance promised that it could help deliver far more effective ads and thus a correspondingly higher rate to the advertisers, providing they provide the names of users who fill out registration forms, make purchases, or conduct other transactions that would reveal the consumer's identity. "We want to make advertising work on the web" said Shapiro, though he continued to decline to say which sites, or even how many sites were participating in the Abacus Alliance.³⁶²

On Thursday, February 10, EPIC filed a complaint with the Federal Trade Commission regarding DoubleClick's information collection practices. EPIC alleged that DoubleClick was unlawfully tracking the online activities of Internet users and combining surfing records with detailed personal profiles contained in a national marketing database. EPIC asked the FTC to investigate the practices of the company, to destroy all records that were wrongfully obtained, to invoke civil penalties³⁶³, and to

³⁶⁰ Greg Miller, "Ad Firm's Practice Seen as Threat to Net Anonymity". *Los Angeles Times*. February 3, 2000.

³⁶¹ *ibid.*

³⁶² *ibid.*

³⁶³ EPIC requested that the Commission level civil penalties on DoubleClick in an amount equal to 50 percent of the company's revenue. See Patricia Jacobus, "FTC investigates DoubleClick's data-collection practices". CNET News.com, February 16, 2000. <http://www.news.cnet.com/news/0-1005-200-1551521.html>

enjoin the firm from violating the Federal Trade Commission Act.³⁶⁴ EPIC's complaint further alleged that the DoubleClick merger of the two databases violated previous assurances that the information collected on Internet users would remain anonymous, and that the data collection was therefore unfair and deceptive.³⁶⁵ EPIC also charged that the company failed to follow its revised privacy policy, which they deemed was also unfair. DoubleClick responded by calling the complaint "meritless".

In a press release, Marc Rotenberg, Executive Director of EPIC, said "This complaint against DoubleClick is a critical test of the current state of privacy protection in the United States. We are looking to the Federal Trade Commission to see whether companies that break their promises and collect personal information in an unfair and deceptive manner will be held accountable."³⁶⁶

On February 14, 2000, DoubleClick announced a "major five-point consumer on-line privacy initiative" in an attempt to deflect the tremendous criticism that it has received over its privacy policies. DoubleClick promised to "launch one of the largest public service campaigns in Web history to help individuals understand that they have the power to protect their privacy online" with the "Internet Privacy Education Campaign".³⁶⁷ They also announced a series of initiatives that DoubleClick claimed would "build on DoubleClick's position as having the most advanced privacy policies and practices in the online advertising industry." To initiate the Internet Privacy Education Campaign, DoubleClick would sponsor 50 million banner advertisements³⁶⁸ that would link consumers to www.privacychoices.org, a site that DoubleClick created to educate consumers about online privacy and provide an opportunity to opt-out of the DoubleClick

³⁶⁴ See "Complaint and Request for Injunction filed to the Federal Trade Commission in the manner of DoubleClick". http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf

³⁶⁵ *ibid.* p. 4-5.

³⁶⁶ EPIC Press Release: 'EPIC FILES FTC COMPLAINT AGAINST DOUBLECLICK, ALLEGES "DECEPTIVE AND UNFAIR TRADE PRACTICES" IN ONLINE DATA COLLECTION' February 10, 2000. http://www.epic.org/privacy/internet/ftc/DCLK_comp_pr.html

³⁶⁷ DoubleClick Press Release, "DoubleClick Announces Major Five-Point Initiative: 'Internet Privacy Education Campaign' to be one of the largest public service advertising campaign in Web history". New York, February 14, 2000. http://www.doubleclick.net/us/corporate/presskit/press-releases.asp?asp_object_1=&press%5Frelease%5Fid=2400

³⁶⁸ Interestingly, DoubleClick announced that they would only place advertisements on Websites that notify consumers of DoubleClick's data-collection practices and offer an opportunity to opt-out.

cookie with "two clicks".³⁶⁹ DoubleClick also announced that it would provide full page advertisements in the *New York Times* and other papers across the country.

DoubleClick President Kevin Ryan also announced the measures that they would take to provide consumers with more information about their privacy. This included the following:

- In the United States, DoubleClick will only do business with Web sites that have a clear and effective privacy policy on their sites. All of DoubleClick's new contracts will be affected immediately and, over a short period of time, the company will work with all existing customers to integrate this new policy.
- DoubleClick has engaged PricewaterhouseCoopers LLP to perform periodic privacy audits so that consumers can remain confident that they are living up to their commitment to protect consumer privacy.
- DoubleClick is establishing an impartial Consumer Privacy Advisory Board consisting of consumer advocates, security experts and authorities in the field of online privacy. The Board will advise DoubleClick and their partners on how to improve the clarity of their privacy policies.
- DoubleClick is hiring a Chief Privacy Officer (CPO), reporting directly to the company's Board of Directors. The CPO will ensure that DoubleClick is effectively implementing its privacy policies and procedures, act as a resource for Internet users, work with advertisers to institute and police their privacy procedures, and educate the public about DoubleClick's leadership role with regards to privacy.

After the press conference announcing the initiative, Kevin Ryan told reporters that the company had already created approximately 50,000 to 100,000 individual profiles from combined information, but the company had not yet sold any advertising based on the merged database data. Ryan also said that consumers will not be able to view and edit their Abacus profiles, citing the difficulty in maintaining the security of the files. "We think that with notice and with choice, the merging of these databases will be a great thing," Ryan said. "What's important to remember is that, individual by individual, this will only happen as users on the Internet give their OK."³⁷⁰

³⁶⁹ *ibid.*

³⁷⁰ Ben Hammer and Diane Anderson, "DoubleClick Strikes Back: Online ad firm attempts to counter privacy advocates' accusations with new site, two-click "opt-out" ability." *TheStandard.com*, February 14, 2000. <http://www.thestandard.com/article/display/0,1151,10331,00.html>

Reaction

DoubleClick opponents immediately responded to the company's "privacy initiative". That day, consumer groups conducted an audio conference that heavily criticized DoubleClick's actions, and concluded that their measures did not go far enough. "DoubleClick is launching an advertising campaign because they're trying desperately to avoid legislation", said Marc Rotenberg of EPIC.³⁷¹ Jeff Chester of the Center for Media Education called on the FTC and Congress to "crack down on this deceptive kind of advertising". Other advocates for privacy continued to communicate the privacy problems inherent in such a scheme. Richard Smith, an independent and well-known security expert and outspoken advocate for consumer privacy explained why it was important to opt-out of the DoubleClick system. After conducting analysis of the information that DoubleClick was collecting on consumers with a packet sniffer, he announced that the company had access to many more personal details than consumers might imagine, noting "they are getting a lot of data there that they shouldn't be getting."³⁷² Other advocates, such as Evan Hendricks of *Privacy Times*, continued to focus on the inadequacy of the opt-out model, suggesting "our goal is to make sure that privacy is protected based on informed consent."³⁷³

In a Security and Exchange Commission filing issued by DoubleClick that same day, it was revealed that the FTC had launched an informal inquiry into DoubleClick's business practices.³⁷⁴ The FTC was investigating to determine whether the company had engaged in unfair and deceptive practices in violation of section five of the Federal Trade Commission Act. In the filing, DoubleClick stated that "if, as a result of any of these proceedings, a judgment is rendered or a decree is entered against us, it may materially and adversely affect our business, financial condition and results of operation." The news caught the attention of Wall Street, and the DoubleClick conflict continued to make the news throughout the Internet industry. Two days later, the DoubleClick stock dropped

³⁷¹ Patricia Jacobus, Courtney Macavinta, and Evan Hansen, "Is DoubleClick privacy plan adequate?". CNET News.com, February 14, 2000. <http://www.news.cnet.com/news/0-1005-200-1549770.html>

³⁷² *ibid.*

³⁷³ Chris Oakes, "DoubleClick Plan Falls Short". Wired News. February 14, 2000. <http://www.wired.com>

³⁷⁴ <http://www.sec.gov/Archives/edgar/data/1049480/0000950117-00-000281-index.html>

roughly five points to 106.50, and in after hours trading the stock continued to decline to 96.50 on 636,000 shares.³⁷⁵

The legal challenges against DoubleClick continued to mount on February 16 when Michigan Attorney General Jennifer Granholm accused DoubleClick of violating Michigan's Consumer Protection Act, an offense punishable by a fine of \$25,000. In a statement, Granholm said "Forget Big Brother, truly, Big Browser appears to have arrived in the form of an Internet corporate giant. Companies like DoubleClick take advantage of the technology to rob people of their privacy."³⁷⁶ The Michigan action stated that DoubleClick does not give consumers "meaningful notice and choice" about whether they want to be profiled, and that the company remains ambiguous about what it will do with the consumer information it compiles. By the time the markets closed, the company's stock fell another 15.75 to 90.75 at the end of regular trading.

On February 29, 2000, consumer pressure continued to mount. The Center for Democracy and Technology, in coalition with the Privacy Rights Clearinghouse, Consumer Action, the Gay & Lesbian Alliance Against Defamation (GLAAD), and the American Civil Liberties Union (ACLU), filed a report to the Federal Trade Commission seeking immediate action to prevent harm to consumer privacy as a result of DoubleClick's Abacus Online Alliance.³⁷⁷ The filing alleged that DoubleClick may be collecting sensitive information about consumer purchases, including video titles, salaries and search terms through its ad serving technology. Ari Schwartz of CDT offered a new basis for concern about the DoubleClick operation: "Companies could be transporting information that could be possibly used by DoubleClick in a personally identifiable way

³⁷⁵ "FTC Casts an Eye on DoubleClick". *The Standard.com*, February 16, 2000.
<http://thestandard.com/article/display/0,1151,10588,00.html>

³⁷⁶ Patricia Jacobus, "Michigan initiates DoubleClick inquiry". *CNET News.com*, February 17, 2000.
<http://news.cnet.com/news/0-1005-200-1553030.html>

³⁷⁷ The Center for Democracy and Technology's conclusions and request for relief is as follows: "Due to the high likelihood of harm to consumer privacy we respectfully request that the FTC enjoin DoubleClick and the Abacus Alliance from tying individuals' names, addresses, phone numbers, and emails to information collected through DoubleClick's cookies; and, prohibit Web sites from registering their subscribers or visitors in the Abacus Alliance profiling system without their affirmative consent, which cannot be made a condition of participation. Because other businesses may be deploying similar business models, we also request that the Commission enjoin all businesses from registering their subscribers in any third-party profiling system that ties personally identifiable information to online surfing habits absent the individual's affirmative consent, which cannot be made a condition of participation."
<http://www.cdt.org/testimony/000225ftcdstatement.shtml>

without the companies knowing, and they could be violating their own privacy policy without knowing it."³⁷⁸

The CDT's filing to the FTC also reported on the results of its campaign against DoubleClick. Within twenty days of the launch of the protest, over 40,000 individuals used CDT's resource to "opt-out" of DoubleClick's system. In addition, 25,000 visitors to CDT's Web site wrote to DoubleClick to protest the Abacus Alliance business plan. It was also reported that 'several thousand' individuals had written to various companies that participate in the DoubleClick Network to express their concern with the Abacus Alliance plan and to ask for a clarification of the members relationships with DoubleClick. "From conversations with Web sites that participate in the DoubleClick Network, we have reason to believe that thousands of additional letters have been sent to both DoubleClick and it's Network members."³⁷⁹ The filing suggested that other companies, such as the popular search engine Alta Vista, were being 'outed' for their relationship with DoubleClick. When visitors used the Alta Vista search engine, each term search was relayed to DoubleClick via a cookie. Alta Vista later reversed the practice of recording search terms in cookie files.

Fallout

On March 2, 2000, DoubleClick issued a Press Release with a statement from the company CEO Kevin O'Connor: "Over the past few weeks, DoubleClick has been at the center of the Internet privacy controversy. During this time, we have met and listened to hundreds of consumers, privacy advocates, customers, government officials and industry leaders about these issues." O'Connor acknowledged that the point of contention was determining under what circumstances a name can be associated with anonymous user activity across the Internet. He conceded that "It is clear from these discussions that I made a mistake by planning to merge names with anonymous user activity across Web sites in the absence of government and industry privacy standards."³⁸⁰ O'Connor was

³⁷⁸ Jim Hu, "Consumer group blasts DoubleClick in report to FTC". *CNET News.com*, March 1, 2000. <http://news.cnet.com/news/0-1005-200-1561502.html>

³⁷⁹ See <http://www.cdt.org/testimony/000225ftdcstatement.shtml>

³⁸⁰ Press Release from DoubleClick inc. "Statement From Kevin O'Connor, CEO of DoubleClick. New York, March 2, 2000.

http://www.doubleclick.net/us/corporate/presskit/pressreleases.asp?asp_object_1=&press%5Frelease%5Fid=2395

clear that DoubleClick had not yet implemented the plan to link names with anonymous activity. O'Connor also committed that in the absence of such standards, DoubleClick "will not link personally identifiable information to anonymous user activity across Web sites."³⁸¹ Developments in the DoubleClick controversy continued to attract coverage by both the online and offline press.³⁸²

On March 8, DoubleClick announced that Jules Polonetsky, formerly the Consumer Affairs Commissioner of New York City, was hired as DoubleClick's Chief Privacy Officer as part of its five point privacy initiative.³⁸³ The position of CPO was created by DoubleClick to act as an ombudsman for Internet users and to work with clients to institute and police their privacy policies and educate the public on the company's commitment to privacy. DoubleClick also announced that Bob Abrams, formerly the New York State Attorney General, would serve as the Chair of its Privacy Advisory Board. Abrams would lead an independent board of privacy, security, and online ethics experts external to the company to make recommendations and improve privacy procedures.³⁸⁴

Within two weeks, DoubleClick's newly assembled privacy public relations team was in settlement discussions with a number of states that were investigating the company's privacy policies. Both DoubleClick and the states, which included Michigan, New York, Connecticut and Vermont, were each reportedly preparing a draft proposal to

³⁸¹ *ibid.*

³⁸² See also: Pamela Parker, "DoubleClick Drops Controversial Plan". *Internet News*, March 2, 2000.

http://www.internetnews.com/bus-news/article/0,,3_314401,00.html ;

Evan Hansen, "DoubleClick postpones data-merging plan". *CNET News.com*, March 2, 2000.

<http://news.cnet.com/news/0-1005-200-1562746.html?dtn.head> ;

Dan, Gillmor, "DoubleClick backs away from linking consumers to data". *San Jose Mercury News* March 2, 2000. <http://www0.mercurycenter.com/svtech/news/indepth/docs/dg030300.htm> ;

Ben Hammer, "DoubleClick Beats a Retreat on Data Privacy". *The Industry Standard*, March 2, 2000.

<http://www.thestandard.com/article/display/0,1151,12563,00.html> .

The story was also covered in the print press, including in the *Wall Street Journal*, *USA Today*, *New York Times*, etc.

³⁸³ DoubleClick Press Release, "DOUBLECLICK APPOINTS CHIEF PRIVACY OFFICER AND PRIVACY ADVISORY BOARD CHAIRMAN: New York City Consumer Affairs Commissioner Polonetsky to be CPO Former Attorney General Bob Abrams to Head Privacy Board".

NEW YORK, March 8, 2000. http://www.doubleclick.net/us/corporate/presskit/press-releases.asp?asp_object_1=&press%5Frelease%5Fid=2394

³⁸⁴ See also Jim Hu, "Consumer advocates to head DoubleClick privacy efforts". *CNET News.com*, March 8, 2000. <http://www.news.cnet.com/news/0-1005-200-1566622.html>

develop "an Internet protocol that will address the privacy concerns".³⁸⁵ South Carolina's Attorney General Charlie Condon also announced that his state would investigate whether DoubleClick violates state laws by secretly tracking consumers' shopping habits online. He suggested that the firm's practice "is cyber snooping into the lives of South Carolina citizens."³⁸⁶

On May 17, 2000, DoubleClick announced the appointment of seven members to its Consumer Privacy Advisory Board. The following individuals were appointed to the board:

- Lori Fena, Chairman and co-founder, TRUSTe
- Daniel J. Weitzner, Technology & Society Domain Leader, World Wide Web Consortium
- Elizabeth Lascoutx, Director, Children's Advisory Review Unit and Vice President, Council of Better Business Bureaus
- Robert Litan, Vice President and Director Economic Studies, The Brookings Institution
- David Stazer, Vice President of Product Development/Strategy and co-founder, PlanetOut.com
- Harriet P. Pearson, Director of Public Affairs, IBM
- Stewart Baker, Partner, Steptoe & Johnson³⁸⁷

"We have put together a strong and diverse group of experts who will be instrumental in helping DoubleClick address the critical privacy issues that affect our business," said Jules Polonetsky, Chief Privacy Officer of DoubleClick. "As DoubleClick moves forward with its mission to deliver effective online advertising, this Board will be an important

³⁸⁵ Quote by Michigan Attorney General Granholm in "DoubleClick in settlement discussions". *Bloomberg News*, March 23, 2000. <http://news.cnet.com/news/0-1005-200-1582990.html>

³⁸⁶ Reuters, "DoubleClick Probe Widens". *Wired News*, March 17, 2000. <http://www.wired.com/news/politics/0,1283,35029,00.html>

³⁸⁷ DoubleClick Press Release, "DOUBLECLICK APPOINTS CONSUMER PRIVACY ADVISORY BOARD: To Include Leading Consumer Advocates and Online Privacy Experts". NEW YORK, May 17, 2000. http://www.doubleclick.net/us/corporate/presskit/pressreleases.asp?asp_object_1=&press%5Frelease%5Fid=2424

voice in ensuring that the company strives for the highest privacy standards."³⁸⁸ Unsurprisingly, DoubleClick critics were united in rejecting the board for their obvious pro-industry inclinations.

On June 13, 2000, Jodie Bernstein, the Director of the Federal Trade Commission's Bureau of Consumer Protection, presented "Online Profiling: A Report to Congress" before the Senate Committee on Commerce, Science, and Transportation.³⁸⁹ The FTC report described the nature of online profiling, consumer privacy concerns about these practices, and the Federal Trade Commission's efforts to address the concerns about the profiling practices of network advertisers. The report applauded the industry's effort to self-regulate their information practices, and in particular the emergence of the Network Advertising Initiative's formulation of working drafts to develop self-regulatory guidelines. The FTC did not make any recommendations to Congress regarding the legislation of privacy standards.

On July 27, 2000, the Federal Trade Commission issued the second part of their report on Online Profiling. The Commission unanimously applauded the Network Advertising Initiative (NAI) for developing an innovative self-regulatory proposal that they contended addressed the privacy concerns consumers have about online profiling.³⁹⁰ The report also recommended that Congress enact legislation to provide privacy protection for consumers with regard to such online profiling practices. This legislation would serve to complement the NAI self-regulatory structure by guaranteeing compliance by non-member network advertising companies. The FTC argued that legislation was necessary to ensure that the 10% of network advertisers that are not members of the Network Advertising Initiative will comply with the protections outlined in NAI's Principles and to guarantee compliance. The Commission found that the fair information practice principles of notice, choice, access, and security were sufficient to implement a protective policy.

The next day, shares in DoubleClick Inc. fluctuated as much as 13% after the news that the self-regulatory approach of the Network Advertising Initiative received

³⁸⁸ *ibid.*

³⁸⁹ Federal Trade Commission Press Release, "Federal Trade Commission Testifies on Online Profiling Report". June 13, 2000. <http://www.ftc.gov/opa/2000/06/profiling.htm>

endorsement by the FTC. The FTC approval of the guidelines would provide network advertisers with the go ahead to combine personal information about individuals with their surfing habits and merge offline and online together in the same database. At the end of the trading day on Friday, July 28, the DoubleClick share price improved 9% to close at 37 1/7.

In predictable fashion, the coalition of privacy advocates responded immediately to the FTC's decision. Fourteen organizations wrote a letter on behalf of "millions of American consumers and users of the Internet" to the Senate Commerce Committee urging them to examine the FTC agreement.³⁹¹ The letter argued that the self-regulatory standard that the FTC approved failed to provide an adequate level of privacy protection. Furthermore, the letter was critical that the FTC's negotiations with the NAI were undertaken without any involvement from the public or consumer and privacy groups. The letter from the consumer advocates cited a document sent to FTC Chairman Robert Pitofsky from the Senators on the Commerce Committee that suggested "self regulation negotiations that exclude consumers from the bargaining table represent an inadequate attempt at developing the appropriate policy regarding privacy protection."³⁹²

The Aftermath

In the months following the settlement over online profiling standards, the DoubleClick controversy waned in media interest and public scrutiny. Where there was media attention, it was typically in Internet and industry magazines, and much of the discussion focussed on the public relations disaster that plagued the company. The name DoubleClick came to be synonymous with privacy problems, with many companies vowing not to be 'the next DoubleClick'. In December of 2000, The Federal Trade Commission quietly ended their investigation of DoubleClick's information practices

³⁹⁰ Federal Trade Commission. *Online Profiling: A Report to Congress (Part 2): Recommendations*. July, 2000. <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>

³⁹¹ Letter to Senate Commerce Committee, United States Senate. August 9, 2000. The Letter was signed by: Center for Media Education, Computer Professionals for Social Responsibility, Consumer Action, Consumer Federation of America, Consumer Project on Technology, Consumers Union, Electronic Frontier Foundation, Electronic Privacy Information Center, Junkbusters Corp., National Consumers League, Privacy Journal, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group.

without much fanfare. With lawsuits pending, the Internet consumer privacy story of the year receded from the headlines.

In many respects, the DoubleClick case is paradigmatic of the concerns that individuals have regarding privacy issues on the Internet. In this sense, the conflict is indicative of the larger conflict about the future of the Internet, and in particular between those interests that advocate a free and open space in which to access and share information in an environment that is not governed by the rules of the marketplace, and those who envision the Internet as the space for the development of a new economy. Clearly, DoubleClick views itself as an enabler to commercial viability on a medium that offers new opportunities to advertise and develop new markets, and not as an enemy of privacy. However, their choice of action and their consequent policy decisions have merged the two different visions together. Furthermore, their impudent denial that there might be a problem with their business strategy reveals that they did not fully anticipate the public concern over the issue.

Although the conflict provides evidence that ideas are an important aspect with respect to how conflicts come to be resolved at the political level, it also demonstrates, as Regan suggests, that interests continue to dominate the politics of privacy in the United States. The ability of the industry to organize interests in the form of the Network Advertising Initiative clearly influenced how the and why the conflict was resolved. The N.A.I. was able to couple a solution (the N.A.I. self-regulatory guidelines) from a short list of ideas to the problem at hand that was acceptable to the governing authority, the FTC. The solution was responsive to the government and industry desire to embrace a self-regulatory regime to govern privacy policy.

In both the DoubleClick case and the controversy over the Longitudinal Labour Force File, the dynamics of conflict proceeded with a certain rhythm. This will be explored in the next chapter. In addition, the two conflicts will be compared and contrasted, and in examining the various stages of the respective conflicts, I will consider whether the analysis reveals any similar processes that might say something about the nature of privacy conflicts and the dynamics of focussing events.

³⁹² An image of the letter from the Senators to Chairman Pitofsky can be found at http://www.epic.org/privacy/internet/pitofsky_letter_0600.jpeg

Chapter Four: Privacy Politicized

Introduction

To this point, I have examined the philosophical, legal, and policy origins of the concept of privacy, and reviewed the contributions by political scientists who have studied the issue. In Chapters Two and Three, I presented case studies of two recent high-profile privacy conflicts, and described the policy landscape, the origins of the particular privacy problem, and the dynamics of these conflicts. In this concluding chapter, I will provide an analysis of the respective conflicts and offer remarks on the new politics of privacy. First, I will justify the examination of these particular cases, and highlight their similarities and differences.

Justification of Cases

The two cases that I have examined in Chapters Two and Three are in some respects very different. The first difference involves the scope of the respective conflicts. Chapter Two was concerned with a conflict that occurred in the public sector. The Longitudinal Labour Force File conflict addressed a privacy claim that was a concern to individuals in their role as citizens of the state. The privacy threat was identified as the aggregation, compilation, storage, and analysis of information in a government operated database. The LLFF database contained information on every registered Canadian citizen, and contained detailed and sensitive information on the interactions between the citizen and the various departments and programs of the state. The scope of information in this case was limited to information held in a government database. The DoubleClick conflict, on the other hand, was concerned with a conflict over privacy values in the private sector. In this case, the privacy threat was the ability and potential of an organization to match detailed aggregate consumer data, including habits, preferences, and tendencies, with extremely detailed personal information, such as location, income, assets, and consumer histories. The information held by the DoubleClick and Abacus databases contained sensitive and detailed records of preferences and interactions between individuals and the marketplace.

A second difference between these cases is the scale of the conflict. Although the Longitudinal Labour Force File conflict was large in scale in that it concerned every individual within the Canadian State, the conflict was limited to the boundaries of the nation state. Although the DoubleClick conflict was addressed within the context of the American State, its scale greatly exceeded the boundaries of the nation. The DoubleClick conflict concerned information collected on the World Wide Web, and as such, its scale was global, affecting individuals on the Internet regardless of their location or nationality.

A third major difference between these two cases is implicit in the differences between both the scope and the scale of these conflicts, namely, the purpose for the collection of this potentially sensitive information. In the Longitudinal Labour Force File Case, the purpose for collecting information was administrative – to assess the viability of labour market programs, to analyze existing programs, to evaluate existing policy, and to support the services provided by HRDC. The purpose for the collection and use of information in the DoubleClick case was to combine consumer information resources to provide consumers with relevant advertising that allegedly meets their interests, desires, and needs. In both of the cases, the purpose for the collection of information was considered legitimate by the defenders of the technologies. However, what was considered problematic by their critics was the processes by which the information was collected, used, and stored.

The final major difference between these two cases is the duration of the conflict. Whereas the conflict over the Longitudinal Labour Force File played out publicly over the course of three weeks, the DoubleClick conflict extended in excess of a year. Although there are a number of significant differences between these two conflicts, there is also a number of compelling similarities between these two cases that justify a comparative analysis.

The most profound similarity between these cases is that both of the conflicts involve concerns over record linkage. Record linkage refers to the ability of organizations to link separate files or dossiers on individuals together to aggregate information for ease of access, analysis, and storage. People are often sensitive about record linkage because it is often assumed that information held by organizations is kept separate and distinct from our other personal records. For example, individuals often assume that when they are

dealing with an organization, such as a government department that administers a public service, that the information provided to that organization remains within that organization. While most individuals understand that information is required to administer services, they are reluctant to provide information that may negatively influence their standing within that organization. The linkage of files into a master file might reveal aspects of their lives that they might have otherwise withheld.

A second commonality between these two cases related to record linkage is that both conflicts were concerned with fears about profiling. In both cases, vast quantities of data were compiled about individuals and stored in massive databases with the aid of record linkage. Profiling is essentially the practice of making the data obtained through record linkage meaningful to the holders of the data. Disparate pieces of information, once linked, can be compiled to construct an intensely detailed, though not necessarily accurate, description of an individual based on their habits, preferences and tendencies that can be used to predict individual behavior and make split-second decisions based on the assumed characteristics of the individual.

A third shared characteristic of these conflicts is criticism of the ‘spirit’ of the existing policies on privacy. In the case of the Longitudinal Labour Force File, the Privacy Commissioner acknowledged the legality of the database, but argued that HRDC’s policy did “not reflect the spirit of the Privacy Act, the principles of the Privacy Act or the objective of the Privacy Act.” Likewise, opponents of the DoubleClick plan were critical of the spirit of DoubleClick’s often-changing privacy policy. The policy originally stated that users who received targeted ads would remain “completely anonymous”. It was later modified to read “not personally identifiable”, and following the merger with Abacus, it again changed to state that their policy would be further revised to reflect its “modified data collection and data use practices.”

A fourth commonality is the notable absence of meaningful fair information practices in the collection and use of information in the respective databases. Both conflicts demonstrated a lack of transparency and openness in the way that information was assembled. In the case of DoubleClick, Internet users are unaware that information about them is being compiled unless they are aware of how advertising networks collect data on the Internet. In the LLFF conflict, the existence of the database was not widely

known or understood. The only notice and explanation of the database was in *InfoSource*, and the innocuous name of the database provided little indication of the scope of its contents. Moreover, both databases contained massive amounts of information, regardless of necessity or relevance, collecting any information that might perceivably be useful regardless of purpose. Likewise, neither of the databases required or encouraged the consent of the data subjects, despite the sensitive nature of the information that was collected. Furthermore, there was no guarantee of the accuracy or completeness of personal information contained within the databases, nor was there any requirement of special rules for protecting particularly sensitive information. Finally, the right of access to and correction of information stored in the databases was problematic. In the case of the LLFF, special procedures had to be established to provide information to concerned citizens after a Freedom of Information request was made, and the process was further complicated by requiring individuals to confirm that they still wanted access to their files after the announcement that the database would be dismantled. In the case of DoubleClick, individuals are not provided the opportunity to access or correct information, personal or otherwise, at all.

Fifthly, both of these conflicts received a great deal of public attention by the press, and both conflicts were elevated, over time, to the political agenda. This is perhaps the most significant shared characteristic of the conflicts. In many respects, these conflicts are paradigmatic of the concerns that individuals have over privacy violations in each of the sectors for which they are associated. The conflict over the Longitudinal Labour Force File exemplified the ability of the public sector to amass a great deal of sensitive information on the citizenry in one master file. Although the purpose for the data compilation can be seen as legitimate, the privacy 'costs' of such a database in the wrong hands or for illegitimate purposes represents a clear threat to the privacy of individuals living in the modern state. Likewise, the DoubleClick conflict demonstrated how a third party agency can collect huge volumes of data on consumers without their knowledge or consent, and for purposes which many consider to be an intrusion into their private lives. The significant media attention that these conflicts received publicized the threats to privacy that these databases posed, and in both cases, contributed to the establishment of a prominent image that effectively communicated the consequences of

the uses of these technologies. In both cases, public concern over the privacy-invading phenomena prompted significant protest by members of the public at large and by organized interests, who appealed to both the organizations operating the invasive technologies and the political organizations responsible for regulating the activities of the organizations entangled in the conflict. Analysis of these respective conflicts reveals some interesting dynamics that are evident in both of the cases. I will now turn to examine the dynamics of these privacy conflicts and highlight the rhythm by which these conflicts proceeded from their initial publicity through to their resolution.

The Dynamics of the Conflict

To both analyze the various dynamics at play and to understand the rhythm of the conflicts from their initial publicity through to their conclusion, the events of the conflict have been subdivided into a series of component stages. These stages have been constructed for both analytical and conceptual clarity. Despite differences in the scope, scale, purpose and duration of the conflicts, each of these cases provides evidence of a particular rhythm as it proceeded through stages of initial publicity, escalation, intensification, denial, reaction, and fallout.

It is important to analyze the dynamics of conflict for a number of reasons. First of all, it provides an effective method for explaining the issue at stake and the manner in which the conflict comes to be resolved. Secondly, it is important to understand the events that contribute to policy change, and the range of actors involved. Thirdly, analysis of the stages of the conflict reveals the various processes at play that contribute to the politicization of the issue. Fourthly, and perhaps most important, analysis of the conflicts can be used to anticipate the dynamics of future conflicts, and in particular to anticipate the effectiveness of various strategies of issue expansion and containment.

Initial Publicity

The initial publicity stage of the conflicts shared a number of common characteristics. In this stage, the advocates of policy change initially identified the privacy problem. In the case of the Longitudinal Labour Force File, the problem was originally publicized by the Privacy Commissioner. Stories on the radio, television, and in the newspapers quoted the Privacy Commissioner warning of a *de facto* citizen profile

containing a great deal of sensitive information on more than 30 million Canadians. In the DoubleClick case, the initial whistle-blowers were well known privacy advocates, Jason Catlett of Junkbusters and Marc Rotenberg of the Electronic Privacy Information Center. The policy problem was described as the creation of a *de facto* consumer profile on hundreds of millions of American consumers and Internet users.

A second feature of the initial publicity stage was the establishment of a prominent idea or image. In the case of the Longitudinal Labour Force File, the image of 'Big Brother' was effectively mobilized to communicate the implications of the technology and define the importance of resolving the conflict. In the DoubleClick case, the image or idea was defined as an unacceptable level of surveillance, and in particular the issue at stake was the end of anonymity on the Internet. In both cases, opponents of the privacy invading phenomena highlighted the contradictions surrounding the spirit of the policy governing the use of information.

After explaining the ways in which the practices of the organizations were contrary to the existing policies, the advocates for policy change highlighted the implications that these changes would have on the way we live. In this respect, they addressed the scope, scale, and potential of the respective technological problems. In each case, this resulted in significant and consistent criticism of the policy decision in the media, and resulted in increased publicity of the privacy interests. In both cases, representatives of the organizations defended the particular employment of technology and the need to use the information. They also argued that the use of the technologies met minimum legal provisions.

Escalation

In the second stage of the conflict, identified as escalation, both of the conflicts continued to share a number of similar characteristics. The most significant of these commonalities was the elevation of the respective issues onto the political agenda. In the case of the Longitudinal Labour Force File, the issue was openly debated in the Canadian Parliament. Much of the debate focussed on criticism of the government policy, and involved protest over the Government's need to maintain such a comprehensive database. The opposition criticized the ruling government of the continued mismanagement of information, which had its roots in the previous mismanagement of a different

government program. Critics of the government focussed specifically on the security of the database and argued that HRDC lacked the specific and necessary expert knowledge to properly administer the database. In defense of the program, the government assured Canadians that the information in the LLFF was secure and that the contents of the database had never been compromised.

In addition to challenging the security of the database, the opposition questioned the need for such a massive data repository. This provided the government with the opportunity to explain the purpose and need for the database and how the information was used by the department. However, it also provided critics with the opportunity to challenge the government's interpretation of the Privacy Act and to accuse the government of acting as an info-predator. The escalation of the conflict provided an opportunity for the stimulation of critical voices. A number of provincial privacy commissioners and politicians commented on the privacy implications of the database and put further pressure on the government to resolve the conflict. Focus on the privacy problem also drew attention to other public sector privacy problems.

The escalation stage of the DoubleClick conflict shared a number of similar features to that of the LLFF conflict. Privacy activists protesting the DoubleClick merger threatened to launch a campaign against the company similar to campaigns against other proposed invasive technologies. This provided an opportunity to draw attention to other privacy issues as well. Critics of the merger launched an open letter campaign to the Chief Executive Officers of the corporations involved in the merger, which cited their concerns about the consequences of the merger and announced their threat to initiate a campaign of protest against the merger. The privacy activists also wrote an open letter to the stockholders of the companies providing notice of the protest strategy and encouraging them to pressure the corporations to abandon the merger plans.

As in the case of the LLFF, the escalation stage of the conflict provided access to the political agenda and an opportunity to discuss the issue of online profiling. Access to the political agenda was first provided by a Federal Trade Commission Report to Congress on self-regulation and privacy that concluded that the issue of online profiling required further examination. An FTC workshop on profiling was organized, and it provided a venue for consumer groups, privacy advocates, industry representatives, and

government officials to address the issue in an open forum. The workshop also provided the opportunity for critical voices to be heard and to present a clear challenge to the authorities to address the threats posed by the business strategy and the use of the technology. On the eve of the workshop, privacy activists requested that the FTC ban the practice of online profiling.

Intensification

The third stage of the conflict, intensification, was marked by two important characteristics – the expansion of interests and a more critical analysis of the lack of a comprehensive application of fair information practices by the privacy-invasive organizations. In the conflict over the LLFF, the Canadian public was invited and encouraged to check the contents of their files by applying through the Freedom of Information Act. If Canadians were concerned about the contents of the database, they could confirm their fears by accessing the information held by HRDC in the Long File. Again in this stage of the conflict, the questions by the opposition about the privacy measures enacted to protect Canadian citizens were responded to by the ruling government's assurance of the security of the database. This prompted critics of the government to inquire about specific principles of fair information practice that were not directly concerned with the security of the database. In particular, opposition members were critical that the consent of Canadian citizens was not obtained prior to the compilation of the database. The government was also criticized for the lack of transparency regarding the existence of the database, and that citizens did not have the opportunity to ensure that the information held in the Long File was accurate and relevant. Again, attention to the privacy conflict in Parliament prompted the revelation of other privacy-related issues.

The intensification stage of the DoubleClick conflict was also characterized by the organization and expansion of interests. Perhaps the most significant development in this stage, and the whole conflict in general as well, was the creation of the Network Advertising Initiative. The N.A.I., a coalition of network advertisers, announced an initiative to clarify their position on the uses of information and the means by which information is collected. The three primary tenets of the initiative included a clear explanation of the information to be collected, the opportunity for individuals to opt-out

of information collection, and the development of an outreach and education program. They proposed a self-regulatory policy that would require network advertisers to provide notification of the information collected, reasonable and timely access to the information held by organizations, the ability to opt-out of the system, and adherence to an oversight and supervisory mechanism such as BBBOnline or Truste.

Privacy activists were immediately critical of the N.A.I. plan and their emphasis on an opt-out model. They alleged that the activities of the network advertisers were unfair and deceptive, and that the practice of profiling resulted in the diminution of autonomy and manipulation of the marketplace. As in the case of the LLFF, critics demanded that the full array of fair information principles be implemented to insure that information that is collected is used in a fair manner.

Critics of the DoubleClick merger launched a third round of letters to protest the practice of profiling, and membership in the coalition expanded to include a broader range of interests. The letter, addressed to the managers of socially responsible mutual funds, emphasized the importance of ideas over interests. The letter criticized the DoubleClick privacy policy, arguing that it represented a full-frontal attack on privacy and anonymity on the Internet. A separate campaign launched by the Center for Democracy and Technology yielded in excess of 10,000 protest emails sent to the company in four days. Despite the protest, DoubleClick formally announced that it had merged with Abacus Direct.

Denial

In the period following the intensification of protest and the organization of interests, the defenders of the alleged privacy-invasive technologies continued to deny any wrong-doing and focussed on deflecting criticism away from their organizations. In both cases, representatives of the organizations insisted that they were 'good actors' and accused their critics of spreading fear.

While the strategies of the organizations varied with respect to the context and nature of the conflict, it was evident that they shared a theme – the best defensive strategy is to focus on the offense. In this regard, defenders of the Longitudinal Labour Force File deflected criticism by counter-accusing their critics of engaging in and developing privacy invasive policies and practices. In the DoubleClick case, the corporation

attempted to deflect criticism by launching a public relations campaign based on a five-point initiative. The initiative was primarily concerned with addressing consumer education of privacy issues and Internet advertising, and on integrating a privacy perspective into the company's corporate culture. To achieve this objective, they announced that they would establish the position of Chief Privacy Officer on the executive committee and establish a privacy advisory board to address privacy concerns confronted by the organization.

In a fashion characteristic of the conflicts, critics of the organizations immediately denounced the activities and actions of their opponents. The Electronic Privacy Information Center filed a formal complaint against DoubleClick with the FTC, asking the FTC to invoke civil penalties for the violation of consumer privacy, enjoin DoubleClick from violating the FTC Act, and demanded that all files wrongfully obtained be destroyed. In the LLFF case, critics also demanded that the files held in the database be destroyed. In both cases, the tone of the press reports on the conflicts were becoming increasingly skeptical of the motives and intentions of the accused privacy violators. Critics continued to give prominent attention to the underlying philosophical and ethical issues over the legal issues, and continued to focus on the primacy of ideas over interests.

Reaction

In the period following the denial of fault and the deflection of criticism, critics of the organizations reacted harshly to their unwavering positions. In the case of the Longitudinal Labour Force File, this was represented by a number of critical letters to the editor in major newspapers across the country and by an increasing number of requests for information under the Freedom of Information Act. In the DoubleClick conflict, the CDT campaign undertaken during the intensification stage had yielded over 40,000 opt-out requests from the DoubleClick system, several thousands of letters of protest, and the publication of a number of previously unknown DoubleClick partners participating in the Abacus Alliance.

In addition to these actions, the FTC formally announced an investigation into DoubleClick's business practices, and a number of State Attorney Generals and private citizens launched a series of class action lawsuits against the company. In both cases,

there were renewed calls for the cancellation and dismantling of the projects, and numerous requests for the modernization of privacy laws.

Fallout

After a period of dormancy in which attention to the conflicts started to wane, political decisions on the fate of the projects were announced in each respective jurisdiction. In the case of the LLFF, HRDC announced that the massive database would be dismantled and information would be returned to the proper and relevant departments. The primary policy advocate in the conflict, the federal Privacy Commissioner, announced that the measures taken to dismantle the database was acceptable and that he supported the measures that HRDC would take. In addition to ensuring that the personal identifiers used to link the files would be removed, HRDC also announced a new governance structure for future social and labour market policy research. A new protective framework governing the use of information was also recommended.

In the DoubleClick case, like the LLFF conflict, there was an admission that the project was problematic and that it was a mistake to merge information in the absence of industry standards. In the same manner that the Privacy Commissioner commended HRDC for their decision, the FTC also applauded the industry attempts to resolve the problem and approved the principles that were proposed by the N.A.I.. The FTC also recommended that Congress enact legislation to complement the N.A.I. principles to ensure that advertisers not associated with the N.A.I. were governed by a common set of rules and principles.

Rhythm and Processes

The analysis of the dynamics of conflict in both the DoubleClick case and the conflict over the Longitudinal Labour Force File yield two important conclusions. The first is that the conflicts, despite differences in the ultimate nature of the conflict, share common characteristics, proceed with similar dynamics, and follow a certain rhythm. In both cases, as demonstrated in the analysis of the dynamics, actions taken by actors seeking to contain the conflict were immediately responded to by those who had an interest in expanding the conflict. For every action, there was an equal and opposite reaction. In other words, for every stimulus, there was a response.

Interestingly, there were a number of forces of resistance and acceleration at play in each of the conflicts. In this regard, the strategies of issue expansion and issue containment outlined by Cobb and Elder and presented in Chapter One were evident in both cases. The strategies employed by those seeking to expand the conflict were in accordance to the five general characteristics, including the degree of specificity, the scope of social significance, temporal relevance, the degree of complexity, and categorical precedence. In this regard, each of the conflicts were ambiguously defined to reach an expanded public, they were articulated as socially relevant, and the issues were important over a long period of time. In the case of DoubleClick in particular, the reason for adopting the policy choice was non-technical, and the issue was defined as lacking a clear precedent. Likewise, with regard to strategies of containment, representatives defending the actions of DoubleClick and HRDC provided a focus on symbolic rewards and reassurances that privacy considerations had been taken, with evidence of feigned constraint and the creation of new organizational units.

Secondly, the analysis of the dynamics of these conflicts reveal a number of processes that are important for both an understanding of privacy conflicts, and understanding the dynamics of focussing events for the larger field of political science. The first implicit process is attention to a critical event that can act as a triggering mechanism for policy change. In both cases, policy advocates presented cases in which a policy decision presented a crisis that had real implications for the existing policy regime. Without attention to the particular focussing event, the policy problem could have been easily obscured from the existing social landscape. In essence, the focussing event serves as a vehicle to link a concrete and practical problem to an abstract theoretical concern reflecting certain philosophical and ethical principles.

The second evident process is the establishment of a metaphoric image or prominent idea. In the two cases presented in this thesis, the image that was established was easily understandable and reflected the long-term consequences of the policy problem. The establishment of the image was tremendously important in both cases. In the LLFF case, the image of 'big brother' was well understood by the public at large and it highlighted the threat presented to the Canadian public. In the DoubleClick conflict, the problem image was less concerned with a metaphor than an important idea – the end of

anonymity on the Internet. However, the lack of a meaningful metaphor required that policy advocates and activists had to repeatedly explain the privacy risks inherent in the particular technological problem. An effective metaphor at the disposal of the policy advocates may have contributed to a better understanding of the conflict and greater attention by the public at large. However, the most relevant metaphor to explain the conflict, 'panopticism', is perhaps well understood within the academic community, but not generally understood by the general public. If this metaphor were to be used, activists would likely have to explain its meaning, which would have likely resulted in a loss of meaning because of misinterpretation and a lack of simplicity. In this regard, activists and advocates must avoid the use of complex metaphors and develop simple, less abstract metaphors to communicate their messages.

A third process, identifiable as widespread and diverse attention by the media, was followed by widespread and conspicuous public interest. Commentators have often mentioned the media's interest in publicizing privacy issues because of the wide range of emotions that privacy issues conjure. While both conflicts were attended to by much interest in the media, it is both interesting and significant to note the different media that were used to communicate the problem. In the LLFF case, the primary medium was the print media, and in particular coverage of the issue in both local and national newspapers. The issue was also publicized by the news media on radio and television. In the DoubleClick case, the primary medium was the Internet. While a number of stories on the conflict were reported in print, and in particular in newspapers such as the *New York Times*, the *Wall Street Journal*, and the *Washington Post*, the vast majority of the media reportage had its basis in specialized information sources that focus on the politics of information and the Internet, such as *Wired.com*, on Internet and technology trade publications such as the *Industry Standard*, and in specific privacy related information sources such as *EPIC*, *Privacy Times*, the *Center for Democracy and Technology*, and the *Electronic Frontier Foundation*. The coverage in the latter sources was significantly more specialized, but limited to an audience already concerned with the privacy issue. Despite the intensity of this specialized coverage, there was enough significant cross-over coverage that the issue could be expanded to a larger audience.

A fourth process, evident more in the DoubleClick conflict than in the LLFF case, is the creation of issue coalitions and the coming together of a diverse range of interests. That this process is more evident in the DoubleClick case is likely attributable to both the duration and context of the conflict. In the DoubleClick case, the range of interests was originally confined to interest groups directly concerned to the issue of privacy. However, as the conflict developed over time and intensified, a broader range of interests, including a number of civil liberties organizations, joined the coalition of interests opposed to the DoubleClick plan. The expansion of interests representing calls for social justice was significant in that the interests could claim a solidarity that was much broader than a coalition of interests concerned with a particular policy sector.

A fifth process, evident in both of the cases, is a focus on privacy as a common, public, and collective value rather than as an individual value. In this respect, the issues were considered to be common values in that they were socially relevant, and of value to all of society, not just to particular individuals within society. As a public value, privacy protection against the invasive characteristics of the technologies was also important. For example, in the case of DoubleClick, the utilization of the particular profiling technique could potentially reveal an individual's various associations, political affiliations and tendencies, and potentially limit his or her public expression. In both of these cases, privacy can also be considered a collective value, because an individual within society cannot claim privacy protection unless others in society share that opportunity as well.

A final process, evident in both of these cases, is political intervention and the process of balance. In both cases, the issue of privacy was not balanced against a competing right, rather it was balanced against a desired policy outcome. In the case of the Longitudinal Labour Force File, the various actors participating in the conflict recognized the importance of conducting social and labour market research, however they disagreed about the proper method and means of obtaining the relevant information. Without question, the publicity surrounding the conflict forced HRDC to consider the privacy implications of their information practices. The conflict provided the Privacy Commissioner with the opportunity to influence HRDC to review their policy by shaping the attitudes of the decision-makers. The Privacy Commissioner effectively educated the media, the public, and politicians on the privacy implications and consequences of using

the personal data in the particular policy context. When significant public pressure was put on the organization, they agreed to work closely with the Privacy Commissioner to find an acceptable alternative to the existing policy. In the DoubleClick conflict, on the other hand, the balance sought by the ‘balancers’, in this case the FTC, was based on the negotiation of a solution involving consideration of both privacy interests and the interests of the industry. The FTC adopted a pragmatic and somewhat flexible approach that invited a number of diverse interests to the table. The balance that eventually came to be ‘struck’ included a requirement to abide by particular rules of information practice, codified in a self-regulatory policy. In this sense, the type of balance that resulted reveals evidence of a ‘negotiated balance’. However, critics of both DoubleClick and the Network Advertising Initiative were disappointed with the FTC decision, the result of which is arguably best understood as the management of surveillance rather than the restriction of it.

While these cases demonstrate evidence of a type of balancing, the steering metaphor perhaps provides the best explanation for the conflict resolution. In both cases, the authorities concerned with the privacy problems achieved the desired outcome – the termination of the existing practice in the case of the Longitudinal Labour Force File, and the promotion of the self-regulatory framework in the DoubleClick case. In these cases, steering amounts to, as Raab suggests, “throwing weight against built-in tendencies and moving toward a desired state of affairs”. Furthermore, the authorities employed instruments within their respective ‘tool kits’ to address the issue and signal to others their desire resolve the crises in a manner consistent with their desired outcome.

Concluding Remarks: The Emergence of a Privacy Industry and the New Politics of Privacy

The concept of privacy has evolved over time, from its roots in Greek philosophy as a justification for the immaterial and unobservable space of the soul from which reason resided, to a liberal conception of privacy rooted in difference, and later culminating in the idea of a ‘domain of consciousness’. In this sense, justifications for the concept privacy were predominantly concerned with the inner life of the mind. At the turn of the twentieth century, privacy’s focus shifted from a philosophical perspective to a legal one,

in which the prominent motivation for concerns about privacy were related to the emergence of new techniques that were invading the sacred regions of domestic life. In this regard, consideration of privacy shifted from the protection of the inner life to protections of the outer spaces of daily life. With the advent of computerization and the development of database technologies, conceptions of privacy shifted again and stimulated the development of data protection and the enactment of rules and procedures to govern the uses of information. In this generation of privacy, concerns were largely attended to by specialists and technocrats, and the focus of protection was information held in databases that was abstracted from daily life. We are now in the midst of a new transformation of concern for and ideas about privacy. Although some claim that privacy is dead and the concept is no longer practical within the context of the emergent network society and digital culture, there is compelling evidence that concern for privacy has reached its apex. Advances in technology, an economy increasingly reliant on information, and increasingly sophisticated techniques of surveillance have drawn much attention to the issue of privacy. In this phase of concern over the issue, activists, advocates, and entrepreneurs have emerged as arguably the new guardians of privacy.

This new cadre of concerned individuals, interests, and organizations have not deviated from the previous aspects of preoccupation, but have transformed them in consideration of new threats and risks. While they are not necessarily concerned with matters relating to the inner life, they are concerned with the maintenance of the *digital soul*. The digital soul refers to the compilation of information based on inferred characteristics, assumed preferences, and recorded habits and preferences. This is not based on information willingly provided, but rather on data that is compiled and manipulated by information systems intent on recognizing and recording, classifying and categorizing, and coordinating and controlling our digital lives with tremendous precision to provide and deny us opportunities for communication, commerce, management, and recreation. Similarly, the new guardians of privacy remain concerned about the privacy of space, however in this regard they are concerned with cyberspace, and the digital spheres in which we operate. They also remain concerned about the protection of data and actively seek the implementation of and adherence to fair information principles. Unlike in the past, there is also a growing community of privacy activists and advocates who are

ready and willing to seek out violators of privacy, to publicize their practices and politicize the issues.

In the past, privacy has not been an issue that has tended to capture the imagination of the public to any great extent, nor has it received a great deal of political attention beyond the creation and implementation of data protection regimes. This trend, as the case studies in this thesis suggest, is quickly changing. Many observers have contended that the issue of privacy will be an important issue over the next decade, and perhaps the most important issue in the next three to five years. More than ever, individuals are becoming aware of new privacy threats. Accordingly, many are taking measures to protect their privacy, and are increasingly being educated about the risks associated with living and participating in the information economy. Correspondingly, a number of businesses are capitalizing on these emerging concerns about privacy, and incorporating a privacy perspective in their operations. A new industry devoted to addressing privacy concerns is emerging. Entrepreneurs have come to realize that privacy is not fundamentally at odds with technology, but rather that technologies can be employed to enhance privacy in the information age. For almost any type of potential privacy invasion, there is fast emerging a technique to protect individuals from that invasion. While this is certainly a positive development, it does come at a cost. Privacy protection is effectively becoming a value-added service. Techniques for protecting privacy are also increasingly becoming available as a technological add-on or 'plug-in'. While privacy protection is something that can still be obtained in an age marked by the free-flow and commodification of information, it is no longer something simply taken for granted, and it no longer comes for free.

Technologies designed to assist privacy protection are not the only aspects of the new privacy industry that can be bought and sold. Increasingly, the market for privacy specialists and consultants is in high demand, and the position of Chief Privacy Officer (CPO) is quickly becoming an important position within the corporate executive branch of industry. Many large organizations and Internet corporations have adopted the position of CPO to address privacy concerns within their companies. CPO's provide a range of important roles for their organizations, including keeping up on the current legislative environment, developing a corporate privacy policy, assessing the privacy risks in new

technologies and services, identifying potential privacy enhancing tools and privacy partners, training and educating employees on the privacy issue, and managing public relations in the event of a conflict or concern over privacy.

This groundswell of privacy interest and the emergence of the privacy industry does not signal the end of privacy conflicts and violations. On the contrary, the enhanced knowledge and awareness of privacy issues will likely result in an increasing number of privacy-related conflicts. While some companies will concede that good privacy policy is in the best interest of business, others will continue to realize that the violation of privacy is equally as lucrative, if not more so. However, the emergence of a vigilant core of privacy activists and the growing community of privacy advocates will continue to seek out privacy invaders and publicize their practices. This will no doubt lead to a number of class action lawsuits over privacy values and further attempts to politicize privacy infractions.

With this in mind, the analysis of the dynamics of privacy conflicts becomes all the more important. Actors on both sides of privacy conflicts will have to adapt to the new challenges presented by privacy conflicts, and strategies of issue expansion and containment will be in high demand. By understanding the dynamics of conflict, what works, and what does not, which issues appeal to mass audiences and what types of conflict will attract the attention of the political realm, the privacy community will be able to adapt to these new challenges and threats.

Academics must also continue to study the privacy issue, and expand their focus beyond the rationalistic and technocratic frameworks from which much of the analysis is undertaken. While the study of politics is considered a rational venture, one of the characteristic conditions of privacy is that it is fundamentally irrational. Fears over privacy invasion are deeply bound in emotion. These emotions often result in a distrust of technology, and technology is often considered to be antithetical to privacy. Ironically, our prevalent conceptions, ideas, and values regarding privacy have not developed in defiance of technology, but because of it. Technologies do not necessarily invade privacy, but the purposes to which they are put to use, intentionally or inadvertently, can result in erosions of privacy. For this reason, it is important to probe deeply into the uses of technology, and speak out against techniques that may be harmful. This will no doubt

reveal some deplorable practices, and induce conflict. However, conflict is not a glitch in the system of the politics of privacy, it is a feature. Until this is further addressed by intellectuals in the field, the most interesting and important dimension of the politics of privacy will be eluded.

Works Cited

- Alinsky, Saul. *Rules for Radicals*. New York: Vintage, 1971.
- Anderson, Diane. "The Trouble with DoubleClick". *The Industry Standard Online*, January 28, 2000.
<http://www.thestandard.com/article/display/0,1151,9261,00.html>
- Banisar, David, and Simon Davies. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *The John Marshall Journal of Computer & Information Law*. Volume XVIII, Number 1. Fall 1999. p. 1-111.
- Baumgartner, Frank R. and Bryan D. Jones. *Agendas and Instability in American Politics*. Chicago: University of Chicago Press. 1993.
- Better Business Bureau. Online Privacy Seal Program. <http://www.bbbonline.com>
- Bennett, Colin J. "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing". *Canadian Public Administration*, vol. 33, 1990. p. 551-570.
- Bennett, Colin J. "Review Article: What is Policy Convergence and What Causes It?" *British Journal of Political Science*. Vol. 21, 1991. p. 215-33.
- Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. London: Cornell University Press. 1992.
- Bennett, Colin J. "The International Regulation of Personal Data: From Epistemic Community to Policy Sector". *Canadian Political Science Association*. Prince Edward Island. 1992.
- Bennett, Colin J. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Information?" Philip E. Agre and Marc Rotenberg eds. *Technology and Privacy: The New Landscape*. MIT Press, Cambridge. 1996. p. 99-124.
- Bennett, Colin J. and David J. Todd. "Data Protection Policy in Canada". *Mathew Bender's International Computer Law*. 1999.
- Bennett, Colin J. "The Political Economy of Privacy: A Review of the Literature".
<http://sitka.dcf.uvic.ca/poli/bennett/research/gnom.htm#anchor3>
- Bicknell, Craig. "DoubleClick's Single Focus: You". *wired news*: www.wired.com June 14, 1999, 2:30 p.m. PDT.
- Birkland, Thomas A. "Focusing Events, Mobilization, and Agenda Setting". *Journal of Public Policy*. Vol. 18, no. 1. 1997. p. 53-74.

- Bloomberg News. "DoubleClick in settlement discussions". *Bloomberg News*, March 23, 2000. <http://news.cnet.com/news/0-1005-200-1582990.html>
- Business Week / Harris Poll. *A growing Threat*.
http://www.businessweek.com/2000/00_12/b3673010.htm
- Calgary Herald*, "Privacy concerns mount over 'invisible citizen profile'". May 20, 2000, Final Edition, p.A5.
- Canadian Press Newswire*. "Opposition slams ``Big Brother`` database. No worries, officials say". May 18, 2000.
- Canadian Press Newswire*, "RCMP, CSIS can access computer files on citizens without consent: report". May 19, 2000.
- Center for Democracy and Technology. *Action Against DoubleClick*.
<http://www.cdt.org/action/doubleclick.shtml>
- Cobb, Roger W. and Charles D. Elder. *Participation and American Politics: The Dynamics of Agenda-Building* Boston: Allyn and Bacon, 1972.
- Cranor, Lorrie Faith et al. "Beyond Concern: Understanding Net Users Attitudes about Online Privacy". <http://www.research.att.com/projects/privacystudy>
- Data Development and Technical Services Group. Evaluation and Data Development Branch. http://www11.hrdc-drhc.gc.ca/edd/vweb_medd.info?subs=DDTS
- Davies, Simon. "Spanners in the Works: How the Privacy Movement is adapting to Big Brother", in Bennett and Grant, eds. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, 1999. p. 244-261
- Direct Marketing Association. *What is the DMA?*
<http://www.the-dma.org/aboutdma/whatisthedma.shtml>
- DoubleClick, Inc. *Press Release*. DOUBLECLICK, INC. AND ABACUS DIRECT CORPORATION TO MERGE IN A \$1 BILLION STOCK TRANSACTION - Merger Creates The World's Leading Online Advertising And Database Marketing Company. NEW YORK, N.Y., 6/14/99.
http://www.doubleclick.net/us/corporate/presskit/pressreleases.asp?asp_object_1=&press%5Frelease%5Ffid=2327
- DoubleClick, Inc. DoubleClick's ad serving solutions description:
http://www.doubleclick.net/us/advertisers/adserving/default.asp?asp_object_1=&

DoubleClick, Inc. Corporate Privacy Policy.

<http://www.doubleclick.net/us/corporate/privacy/>

DoubleClick, Inc. *8-K Security Exchange Commission Filing*. Conformed June 13 1999.

Available at: <http://www.sec.gov/Archives/edgar/data/1049480/0001005477-99-002865-index.html>

DoubleClick, Inc. *DoubleClick Press Release*: "DoubleClick Completes Merger with Abacus Direct". November 23, 1999.

http://ir.doubleclick.net/ireye/ir_site.zhtml?ticker=DCLK&script=410&layout=-6&item_id=66808

DoubleClick, Inc. *DoubleClick Press Release*, "DoubleClick Announces Major Five-Point Initiative: 'Internet Privacy Education Campaign' to be one of the largest public service advertising campaign in Web history". New York, February 14, 2000.

http://www.doubleclick.net/us/corporate/presskit/press-releases.asp?asp_object_1=&press%5Frelease%5Fid=2400

DoubleClick, Inc. *Press Release*. "Statement From Kevin O'Connor, CEO of DoubleClick. New York, March 2, 2000.

http://www.doubleclick.net/us/corporate/presskit/pressreleases.asp?asp_object_1=&press%5Frelease%5Fid=2395

DoubleClick, Inc. *Press Release*. "DOUBLECLICK APPOINTS CHIEF PRIVACY OFFICER AND PRIVACY ADVISORY BOARD CHAIRMAN: New York City Consumer Affairs Commissioner Polonetsky to be CPO Former Attorney General Bob Abrams to Head Privacy Board". NEW YORK, March 8, 2000.

http://www.doubleclick.net/us/corporate/presskit/press-releases.asp?asp_object_1=&press%5Frelease%5Fid=2394

DoubleClick, Inc. *Press Release*. "DOUBLECLICK APPOINTS CONSUMER PRIVACY ADVISORY BOARD: To Include Leading Consumer Advocates and Online Privacy Experts". NEW YORK, May 17, 2000.

http://www.doubleclick.net/us/corporate/presskit/pressreleases.asp?asp_object_1=&press%5Frelease%5Fid=2424

Downs, Anthony. "Up and Down with Ecology: the issue attention cycle". *Public Interest*. Vol. 28, no. 1, 1972. p. 38-50.

Edmonton Journal, "Canadians tracked by huge gov't database: 'Every one of us is covered' in millions of individual files -- commissioner". May 17, 2000, Final Edition, p.A1 / FRONT.

- Electronic Privacy Information Center. "Complaint and Request for Injunction filed to the Federal Trade Commission in the manner of DoubleClick".
http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf
- Electronic Privacy Information Center. *EPIC Press Release*: "EPIC FILES FTC COMPLAINT AGAINST DOUBLECLICK, ALLEGES "DECEPTIVE AND UNFAIR TRADE PRACTICES" IN ONLINE DATA COLLECTION". February 10, 2000. http://www.epic.org/privacy/internet/ftc/DCLK_comp_pr.html
- Engage Inc. Engage.com Press Release.
<http://www.engage.com/press/releases/2qfiscal.htm>
- European Union Directive on the Protection of Personal Data and the Free movement of Such Data. 1995.
- Federal Trade Commission. Privacy Resources. <http://www.ftc.gov/privacy/index.html>
- Federal Trade Commission. "Self-Regulation and Privacy Online: A Report to Congress". July 1999.
<http://www.ftc.gov/os/1999/9907/privacy99.pdf>
- Federal Trade Commission. *Online Profiling Workshop*.
<http://www.ftc.gov/bcp/profiling/online.pdf>
- Federal Trade Commission. *Press Release*, "Federal Trade Commission Testifies on Online Profiling Report". June 13, 2000.
<http://www.ftc.gov/opa/2000/06/profiling.htm>
- Federal Trade Commission. *Online Profiling: A Report to Congress (Part 2): Recommendations*. July, 2000.
<http://www.ftc.gov/os/2000/07/onlineprofiling.htm>
- Financial Post* (National Post), "Will mining our information be governments' new profit centre? Federal database raises disturbing possibilities". May 18, 2000 page C19.
- Flaherty, David. *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press. 1989.
- Gazette, The (Montreal)*. "Ottawa has files on us all: Cradle-to-grave database open to abuse". May 17, 2000. Page A1.
- Gazette, The (Montreal)* "Canadians are requesting their HRDC files" May 20, 2000, Final Edition, p.A14.
- Gandy, Oscar H. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview Press. 1993.

- Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century*. Boston: O'Reilly and Associates. 2000.
- Gellman, Robert. "Does Privacy Law Work?" in Philip E. Agre and Marc Rotenberg eds. *Technology and Privacy: The New Landscape*. Cambridge: MIT Press. 1996.
- Gibson, Steve. "Privacy and Spyware Info on the Net". <http://grc.com/oo/news.htm>
- Gillmor, Dan. "DoubleClick backs away from linking consumers to data". *San Jose Mercury News* March 2, 2000.
<http://www0.mercurycenter.com/svtech/news/indepth/docs/dg030300.htm>
- Gurak, Laura J. *Persuasion and Privacy in Cyberspace: the online protests over lotus marketplace and the clipper chip*. Yale University Press. 1997.
- Hack Canada. *Report on the LLFF*.
<http://www.hackcanada.com/canadian/freedom/canadasbigbrother2000.html>
- Halifax Herald*. 'Letters to the Editor' May 19, 2000, First Edition.
- Hammer, Ben and Diane Anderson. "DoubleClick Strikes Back: Online ad firm attempts to counter privacy advocates' accusations with new site, two-click "opt-out" ability." *TheStandard.com*, February 14, 2000.
<http://www.thestandard.com/article/display/0,1151,10331,00.html>
- Hammer, Ben. "DoubleClick Beats a Retreat on Data Privacy". *The Industry Standard*. March 2, 2000. <http://www.thestandard.com/article/display/0,1151,12563,00.html>
- Hansard, Edited. 36th Parliament, 2nd Session. (Number 099). Wednesday, May 17, 2000.
http://www.parl.gc.ca/cgi-bin/36/pb_chb_hou_deb_ind.pl?36:2:e:099_2000-05-17
- Hansard, Edited . 36th Parliament, 2nd Session. (Number 100). Thursday, May 18, 2000
http://www.parl.gc.ca/cgi-bin/36/pb_chb_hou_deb_ind.pl?36:2:e:100_2000-05-18
- Hansard, Edited .36th Parliament, 2nd Session. (Number 101). Friday, May 19, 2000.
http://www.parl.gc.ca/cgi-bin/36/pb_chb_hou_deb_ind.pl?36:2:e:101_2000-05-19
- Hansen, Evan. "DoubleClick under email attack for consumer profiling plans". *CNET News.com*, February 2, 2000. <http://www.news.cnet.com/news/0-1005-200-1539478.html>
- Hansen, Evan. "DoubleClick postpones data-merging plan". *CNET News.com*, March 2, 2000. <http://news.cnet.com/news/0-1005-200-1562746.html?dtn.head>

- Hauben, Michael. "Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet".
<http://www.dei.isep.ipp.pt/docs/arpa--1.html>
- Holmes, Robert. "Privacy: philosophical foundations and moral dilemma's". *Privacy Disputed*. Pieter, Ippel, Guus de Heij and Bart Crouwers, eds. SDU Den Haag. 1995. p. 15-29.
- Howlett, Michael. "Issue-Attention and Punctuated Equilibria Models Reconsidered: An Empirical Examination of the Dynamics of Agenda-Setting in Canada". *Canadian Journal of Political Science*. Vol. XXX:1 March, 1997. p. 3-29.
- Howlett, Michael. "Predicable and Unpredictable Policy Windows: Institutional and Exogenous Correlates of Canadian Federal Agenda-Setting". *Canadian Journal of Political Science*. Vol. XXXI:3. September, 1998. p. 495-524.
- Hu, Jim. "Consumer group blasts DoubleClick in report to FTC". *CNET News.com*, March 1, 2000. <http://news.cnet.com/news/0-1005-200-1561502.html>
- Hu, Jim. "Consumer advocates to head DoubleClick privacy efforts". *CNET News.com*, March 8, 2000. <http://www.news.cnet.com/news/0-1005-200-1566622.html>
- Human Resources Development Canada Profile.
<http://www.hrdc-drhc.gc.ca/menu/profile-hrdc.shtml>
- Human Resources Development Canada. *News Release*: "HRDC Dismantles Longitudinal Labour Force File Databank". May 29, 2000.
- Human Resources Development Canada. "BACKGROUND: HRDC's Measures to Strengthen Privacy of Information". May 29, 2000.
- Info Source, Human Resources Development Canada Personal Information Banks: Sources of Federal Government Information 1999-2000.
http://dsp-psd.pwgsc.gc.ca/InfoSource/Info_1/HRDC-PB-e.html
- Jacobus, Patricia. "FTC investigates DoubleClick's data-collection practices". *CNET News.com*. February 16, 2000. <http://www.news.cnet.com/news/0-1005-200-1551521.html>
- Jacobus, Patricia, Courtney Macavinta, and Evan Hansen, "Is DoubleClick privacy plan adequate?". *CNET News.com*, February 14, 2000.
<http://www.news.cnet.com/news/0-1005-200-1549770.html>
- Jacobus, Patricia. "Michigan initiates DoubleClick inquiry". *CNET News.com*, February 17, 2000. <http://news.cnet.com/news/0-1005-200-1553030.html>

Junkbusters, Inc. <http://www.junkbusters.com>

Junnarkar, Sandheep. "DoubleClick accused of unlawful consumer data use". *CNET News.com*, January 28, 2000. <http://www.cnet.com/news/0-1005-200-1534533.html>

Jupiter Communications. <http://www.jup.com/sps/research/service2.jsp?service=ADV>

Katz v. U.S.. 386 U.S. 954 (1967). <http://laws.findlaw.com/US/386/954.html>

Kingdon, John W. *Agendas, Alternatives, and Public Policies*. Toronto: Little Brown and Company. 1984.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. *A Brief History of the Internet*.
<http://www.isoc.org/internet/history/brief.html>

Macavinta, Courtney. "Consumer group to fight DoubleClick deal". June 14, 1999. *CNET News.com*. <http://www.news.cnet.com/news/0-1007-200-343608.html>

Macavinta, Courtney. "DoubleClick not worried about privacy charges". *CNET News.com*. June 15, 1999. <http://www.news.cnet.com/news/0-1007-200-343680.html>

Macavinta, Courtney. "Privacy advocates rally against DoubleClick-Abacus merger". *CNET News.com*, November 22, 1999. <http://news.cnet.com/new/0-1005-200-1461826.html>

Courtney Macavinta, "Privacy fears raised by DoubleClick database plans". *CNET News.com*. January 25, 2000. <http://news.cnet.com/news/0-1005-200-1531929.html>

Marinaccio, Wendy. "Privacy advocates blast DoubleClick merger", *CNET News.com*. June 21, 1999. <http://news.cnet.com/news/0-1005-200-343915.html>

Martin, Edward C. "Privacy Torts". Cumberland School of Law, Samford University. <http://netlaw.samford.edu/Martin/AdvancedTorts/privacyhome.htm>

Miller, Greg. "Ad Firm's Practice Seen as Threat to Net Anonymity". *Los Angeles Times*. February 3, 2000.

National Post. "Ottawa defends 'big brother' database: Ministry kept public in the dark about data collection: Files contain up to 2,000 different details about lives of 33 million Canadians". May 17, 2000, National Edition, p.A1 / FRONT.

National Post, "'Time to review' Privacy Act, says Justice Minister- Outrage over database- Opposition attacks focus on Stewart". May 18, 2000, National Edition, p.A6.

National Post, "Keeping secrets". May 18, 2000, National Edition, p.A19.

National Post, "Ottawa's policy: Do ask, don't tell- They have massive files on us, but keep their doings secret". May 19, 2000, National Edition, p.A1 / FRONT.

Network Advertising Initiative. <http://www.networkadvertising.org>

Network Advertising Initiative. Press Release, November 9, 1999.
<http://www.networkadvertising.org/press/11-9-99-testimony.shtml>

New York Times. "AOL Admits Error in Gay Sailor Case", Jan. 21, 1998.
www.nytimes.com/aponline/w/AP-Navy-Gay-Dismissal.html

Oakes, Chris. "DoubleClick Plan Falls Short". Wired News. February 14, 2000.
<http://www.wired.com>

Ottawa Citizen. 'Letters to the Editor' May 19, 2000.

Pamela Parker, "DoubleClick Documents Reveal More Legal, Regulatory Troubles".
Internet News.com.
http://www.internetnews.com/bus-news/article/0,,3_305521,00.html

Parker, Pamela. "DoubleClick Drops Controversial Plan". *Internet News*, March 2, 2000.
http://www.internetnews.com/bus-news/article/0,,3_314401,00.html ;

Parsons, Wayne. *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*. Aldershot, U.K.: Edward Elgar, 1995.

Perin, Keith. "Privacy Activists File DoubleClick Complaint: Watchdog group EPIC alleges ad firm violated federal law, merits investigation." *The Industry Standard*, February 10, 2000.
<http://www.thestandard.com/article/display/0,1151,9694,00.html?nl=mg>

Pew Internet & American Life Project. *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*. <http://www.pewinternet.org/reports/toc.asp?Report=19>

Public Broadcasting Service. PBS Internet Timeline.
<http://www.pbs.org/internet/timeline/timeline-txt.html>

Privacy Act of Canada. Section 8 (2). <http://canada.justice.gc.ca/en/laws/P-21/text.html>

- Privacy Alliance. *Mission Statement*. <http://www.privacyalliance.org/mission>
- Privacy Commissioner of Canada. *AIDS and the Privacy Act*. Ottawa: Minister of Supply and Services. 1989.
- Privacy Commissioner of Canada. *Drug Testing and Privacy*. Ottawa: Minister of Supply and Services. 1990.
- Privacy Commissioner of Canada. *Genetic Testing and Privacy*. Ottawa: Minister of Supply and Services. 1992.
- Privacy Commissioner of Canada. *Annual Report 1994-95*. Ottawa: Canada Communications Group. 1995
- Privacy Commissioner of Canada. *Annual Report 1995-96*. Ottawa: Canada Communications Group. 1996.
- Privacy Commissioner of Canada. *News Release*: "Looking back, moving forward: the Privacy Commissioner releases his 1999-2000 annual report". OTTAWA, May 16, 2000.
- Privacy Commissioner of Canada. "ANNUAL REPORT 1999-2000".
<http://www.hrdc-drhc.gc.ca/menu/profile-hrdc.shtml>
- Privacy Commissioner of Canada. *Privacy Act Reform: Issue Identification and Review*. A Report by the Privacy Commissioner of Canada on Proposed Amendments to the Federal Privacy Act. June 16, 2000.
- Privacy Place. <http://www.privacyplace.com>
- Prosser, William L. "Privacy". *California Law Review*. Vol. 48, no. 3. August 1960.
- Province, The* (Vancouver), "Petter fears federal files open to abuse". May 18, 2000, Final Edition, p.A23.
- Raab, Charles. "Implementing Data Protection in Britain". *International Review of Administrative Sciences*. Vol. 62, no. 4. 1996. p. 493-511.
- Raab, Charles D. and Colin J. Bennett "Protecting Privacy Across Borders: European Policies and Prospects". *Public Administration*. Vol. 72, Spring, 1994. p. 95-112.
- Raab, Charles D. "From Balancing to Steering: New Directions for Data Protection", in Colin J. Bennett and Rebecca Grant eds. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press. 1996. p. 68-93.
- Reuters*, "DoubleClick sued over privacy: Internet advertising company accused of unlawfully obtaining and selling consumers' private personal information."

January 28, 2000.

www.zdnet.com/zdnn/stories/news/0,4586,2429053,00.html?chkpt=zdnnr1a

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press. 1995.

Reuters, "DoubleClick Probe Widens". *Wired News*, March 17, 2000.

<http://www.wired.com/news/politics/0,1283,35029,00.html>

Rosen, Jeffrey. *The Unwanted Gaze - The Destruction of Privacy in America*. Random House, 2000.

Rule, James, Douglas McAdam, Linda Stearns, David Uglow, *The Politics of Privacy*. New York: Elsevier, 1980.

Schattschneider, Elmer E. *The Semi-Sovereign People*. New York: Holt, Rinehart, and Winston. 1960.

Schwartz, Paul M. "Privacy and Democracy in Cyberspace". *Vanderbilt Law Review*. Vol. 52, 1998. p. 1609-1701.

Smith, Richard M. "The Web Bug FAQ".

<http://www.tiac.net/users/smiths/privacy/wbfaq.htm>

SpyChecker.com. www.spychecker.com/spyware.html

Standard, The. FTC Casts an Eye on DoubleClick". *The Standard.com*, February 16, 2000. <http://thestandard.com/article/display/0,1151,10588,00.html>

Statistics Canada Act. <http://www.statcan.ca/english/about/statact.htm>

Thomson, Judith Jarvis. "The Right to Privacy". *Philosophy and Public Affairs*. Vol. 4, no. 4. Summer, 1975. p. 295-314.

Toronto Star. 'Letters to the Editor' May 19, 2000, First Edition.

Toronto Star, "A warning worth heeding" May 20, 2000, First Edition.

Truste. Online Privacy Seal Program. <http://www.truste.com>

Vancouver Sun. "Ottawa keeps secret files on all Canadians: The privacy watchdog reveals the existence of a huge database on individual citizens." May 17, 2000. Final Edition, p.A1 / FRONT.

- Vancouver Sun*. "B.C. threatens to withhold personal data from Ottawa: Provincial officials react angrily to news Ottawa has secret files on all Canadians". May 18, 2000, Final Edition, p.A1 / FRONT.
- van de Donk, W.B.H.J., Colin J. Bennett, and Charles D. Raab, "The politics and policy of data protection: experiences, lessons, reflections, and perspectives". *International Review of Administrative Sciences*. Vol. 62, No. 4. December, 1996. p. 459-464.
- van de Donk, Wim B. H. J. and Hein van Duivenboden, "Privacy as Policy: a policy implementation perspective on data protection at shopfloor level in the Netherlands". *International Review of Administrative Sciences*. Vol. 62, no. 4. 1996. p. 513-534.
- Warren, Samuel D. and Louis D. Brandeis, "The Right to Privacy". *Harvard Law Review*. vol. 4, 1890.
- Westin, Alan F. *Privacy and Freedom* New York: Atheneum, 1967.
- Westwood, John. "Life in the Privacy Trenches: Experiences of the British Columbia Civil Liberties Association". Colin J. Bennett, and Rebecca Grant, eds. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, 1999. p. 231-243.
- Whitaker, Reg. *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York: New Press. 1999.

VITA

Surname: Todd

Given Names: David Jeffrey Allan Todd

Place of Birth: Winnipeg, Manitoba, Canada

Educational Institutions Attended:

University of Victoria	1998 to 2001
University of Manitoba	1992 to 1997

Degrees Awarded:

Bachelor of Arts	University of Manitoba	1996
------------------	------------------------	------

Honours and Awards:

Canadian Policy Research Award	2000
Usenix Association Conference Scholarship	2000
University of Victoria Travel Grants	2000
University of Victoria Graduate Teaching Fellowship	1998 to 2000

Publications:

"Data Protection Policy in Canada", with Colin J. Bennett. *Matthew Bender's International Computer Law*. 1999.

"Public Policy and the Analysis of Policy Instruments: The Implementation of a Canadian Policy for the Protection of Privacy in the Private Sector". *Government of Canada, Policy Research Initiative*. 2000

"The Demonization of Unauthorized Use: Jessica Litmann on Intellectual Property in the Digital Age". *Computers, Freedom, and Privacy*. 2000.

UNIVERSITY OF VICTORIA PARTIAL COPYRIGHT LICENSE

I hereby grant the right to lend my thesis to users of the University of Victoria Library, and to make single copies only for such users or in response to a request from the Library of any other university, or similar institution, on its behalf or for one of its users. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by me or a member of the University designated by me. It is understood that copying or publication of this thesis for financial gain by the University of Victoria shall not be allowed without my written permission.

Politicizing Privacy: 'Focussing Events' and the Dynamics of Conflict

Author



David Todd

April 30, 2001