

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI[®]

**Beyond Data Protection:
Applying Mead's Symbolic Interactionism and Habermas's
Communicative Action to Westin's Theory of Privacy**

by

Valerie Steeves, B.A., J.D.

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfilment of
the requirements for the degree of
Doctor of Philosophy
Communication Program
School of Journalism and Communication

Carleton University
Ottawa, Ontario
April, 2005

©Valerie Steeves, 2005



Library and
Archives Canada

Bibliothèque et
Archives Canada

0-494-08351-4

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file *Votre référence*

ISBN:

Our file *Notre référence*

ISBN:

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.


Canada

Abstract

Current privacy policy frameworks embody a set of data protection principles which privilege a narrow interpretation of privacy as informational control, in spite of concerns that data protection is neither resilient enough a concept to protect the social value of privacy nor able to account for the role privacy plays in the development of identity. Data protection laws draw heavily on Alan Westin's theoretical work on privacy. Westin's work is rich in sociality; however, since his data protection principles were first incorporated into legislation in 1970, the valorization of technology and managerial imperatives have worked to marginalize the social elements in his thinking. In addition, Westin himself limits his theoretical framework by focussing on information flow rather than the negotiation of privacy by social actors. This dissertation puts Westin into dialogue with the work of George Herbert Mead, as it has been applied and extended by Irwin Altman and Jurgen Habermas, in order to reclaim and extend the social elements in Westin's thinking. I apply Mead's theory of the social self to dissolve the apparent tension between Westin's atomistic individual and the social. I adopt Irwin Altman's definition of privacy as the boundary between self and other and apply Mead's dialogue between the social self and the undetermined I to locate privacy at the centre of identity formation. I then use Habermas's conception of communicative action to argue that privacy – as the line between self and other – is an essential element of the normatively guided interaction that a linguistically constituted form of inter-subjectivity makes

possible. Privacy can therefore be conceived of as a social emergent of communication which involves the inter-subjective negotiation of the boundary between the self and other. This conception frees the policy questions from narrow considerations of fair information practices, and reinvigorates the need to come to social judgment about the appropriateness of surveillance. To test whether this conception of privacy can better inform policy, I examine children's online privacy and compare how well data protection principles and a theory of privacy as a social emergent of communication can explain and address the issues.

Table of Contents

List of Tables	vi
List of Illustrations	vii
Chapter 1 – Current Themes in the Privacy Literature	1
Privacy and technology	4
Westin and the classical conception of privacy	8
Privacy and data protection policy	11
Critiques of data protection	13
Privacy and surveillance	25
Privacy as a social psychological concept	27
Gaps identified in the theory	32
Beyond Westin – Applying Mead and Habermas to the privacy debate	33
Chapter 2 – Legal Frameworks to Protect Privacy	49
Constitutional and criminal protections against the invasive power of the state	51
Property	54
Reasonable expectations of privacy	60
Chapter 3 – Data Protection Regimes: A Historical Exposition and Comparative Legal Analysis	69
The origins of data protection	73
The legacy of World War II	77
International Human Rights instruments	79
Early data protection instruments	81
Hesse Data Protection Act	90
Swedish Data Act	94
Council of Europe Resolution regarding private sector databases	99
Council of Europe Resolution regarding public sector databases	103
American Privacy Act of 1973	107
German Federal Data Protection Law	115
International data protection instruments	122
OECD Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data	122
Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	125

European Union Directive on the Protection of Personal Data with regard to the Processing of Personal Data and on the Free Movement of Such Data	130
Since 1985 – The Canadian experience	135
Chapter 4 – Exploring the Social in Westin’s Theory of Privacy	150
Westin’s legislative programme	153
Social elements in Westin’s conception of privacy	160
The disappearing social dimension	166
Chapter 5 – Applying Mead, Altman and Habermas to Privacy Theory	173
Altman’s appropriation of Westin	175
Applying Mead to privacy theory	180
Privacy and the social self	180
Privacy and identity	183
Privacy and role-taking	186
Privacy and autonomy	188
Applying Habermas to privacy theory	190
Privacy and communicative action	190
Privacy and democratic discourse	193
Privacy as a social emergent of language	199
Chapter 6 – Testing the Framework: A Case Study on Children’s Online Privacy	207
A snapshot of children’s online environment	210
Children’s experience of online privacy	231
The data protection response	236
The policy potential of a communicatively-based understanding of privacy	247
Chapter 7 – Conclusion	261
Appendix – Privacy Provisions in Selected Instruments	271
Table of Statutes, Treaties and Conventions	283
Table of Cases	286
References	287
Web Sites	305

List of Tables

Table		Page
1	Selected Privacy Studies 1970-1975	82
2	The Diffusion of Data Protection Legislation by Region	86
3	Stated Reasons for Adopting Fair Information Practices 1970 -1985 ...	88
4	Swedish Data Act	99
5	Council of Europe Private Sector Resolution	101
6	Council of Europe Public Sector Resolution	104
7	US Privacy Act	110
8	German Data Protection Law	117
9	OECD Privacy Guidelines	123
10	Council of Europe Personal Data Convention	126
11	Westin's Privacy States and Functions	161
12	Privacy as Informational Control	169
13	Privacy as Boundary	205

List of Illustrations

Illustration	Page
1 Cosmogirl Registration Page	213
2 Neopets Registration Reminder Page	216
3 zip4tweens Burger Boogie Game	221
4 Barbie Call Time Page	224
5 Beer.com Home Page	227
6 TVOKids Sponsor Page	242

Chapter One – Current Themes in the Privacy Literature

In the mid 1990s, there was a flurry of legislative activity in Canada around privacy, which culminated when the federal government passed comprehensive privacy legislation in 2000. However, in spite of the new legislative rules, a quick survey of the headlines indicates that Canadians continue to be concerned about government and private sector surveillance practices. News reports of detailed government dossiers on individual Canadians (Globe & Mail, 2000), airline passenger databases (CBC, 2003), and pharmaceutical companies paying doctors for access to patient records (Province, 2004), for example, have been met with public outcry and indignation. In this dissertation I argue that the current legislative framework has done little to address these public concerns because the dominant theoretical model of privacy as informational control has failed to protect the social value of privacy as it is understood by real social actors. In order to provide a deeper pool of policy ideas, privacy theory must therefore expand beyond current thinking, and address and explain the ways in which privacy is embedded in social praxis.

The seminal conception of privacy articulated by Alan Westin in 1967 was rooted in the sociological literature, and sought to theorize the social meaning of privacy as it is lived by social actors. However, in this dissertation, I argue that much of the social meaning of Westin's framework has been marginalized, both in the literature and in the realm of public policy. I attempt to reclaim and extend the

sociological potential in Westin's work, by drawing on Meadian conceptions of communication and social interaction. In doing so, I lay the groundwork for a theory that argues privacy is a social value that emerges through language and, as such, is an essential element of social interaction and democratic discourse. My thesis is informed by a critical intention not only to describe and explain the shortcomings of the existing policy framework, but to transform that framework by extending the social understanding of privacy as an essential element of the formation of human identity and social relationships.

A review of the literature indicates that privacy has indeed been an elusive concept to define (Margulis, 2003b; Bennett, 1995; Allen, 1988), and privacy theory is tied to broader inter-disciplinary debates about democracy and power. As such, it has generated discussion in the fields of law, economics, sociology, psychology, philosophy and communication. Bennett argues that all definitions of privacy are grounded in "questionable assumptions" about the individual, civil society and the state, and "it is those very assumptions that require careful interrogation if the 'politics' of privacy are to be unearthed" (Bennett, 1995, p. 2). The literature, however, tends to discuss privacy in terms of the individual's desire for secrecy, anonymity, autonomy and control. Margulis notes that the relationship between privacy and these other cognate concepts is difficult to determine because of an underlying disagreement about the boundaries of privacy (Margulis, 2003b, p. 244). Whereas some scholars maintain that privacy "protects behavior which is either morally neutral or valued by society" (Warren &

Laslett, 1977, p. 44) and, as such, is a positive value, others argue that privacy can be used to shield negative and morally dubious behaviour, including abuse of public office (Westin, 1967), lying (Derlega & Chaikin, 1977), deception (Posner, 1978; DePaulo et al, 2003) and vandalism (Altman, 1975).

A similar bifurcation exists in the policy literature. Privacy advocates seek to protect privacy because, as a fundamental human right and an essential part of a civil democracy, it is a good in itself (e.g. Westwood, 1999; Canada, 1997). Communitarian theorists and information collectors, on the other hand, view privacy as a barrier to other collective goods (Regan, 1995, p. 16). From this perspective, the individual's privacy detracts from legitimate social goals, such as government efficiency, economic growth and the creation of knowledge. The fact that, as Bennett notes, "over thirty years of semantic and philosophical analysis ... leaves [one] with the overwhelming sense that privacy is a deeply and essentially contested concept" (Bennett, 1995, p. 2) indicates that it is a key situs of social and political struggle, and worthy of further study.

However, current privacy policy frameworks privilege a narrow interpretation of privacy as informational control. Laws based on this definition of privacy focus on fair information practices that seek to protect the individual's right to control the collection, use and disclosure of his or her personal information. In this chapter, I argue that this conceptualization of privacy is not robust enough to restrict invasive practices enabled by new technologies, and serves to legitimize

the continued flow of personal information to public and private sector organizations. This conceptualization also defines privacy as an individual right divorced from any social value, which accordingly pits privacy against the social interest in using personal information to enhance efficiency and security; this masks the nature and importance of privacy as a social value and ensures that privacy protection will continue to give way before institutional arguments in favour of invasion.

This chapter begins with a survey of the privacy literature organized around six themes: privacy and technology; Westin and the classical conception of privacy; privacy and data protection policy; critiques of data protection; privacy and surveillance; and privacy as a social-psychological concept. I then argue that the work of George Herbert Mead and Jurgen Habermas can be used to revisit and extend Westin's theory of privacy as informational control, and provide the groundwork for a theory that accounts for the social and democratic value of privacy. Finally, I provide an overview of the material covered in each of the remaining chapters.

Privacy and technology

Over the past century, much of the struggle around privacy has been generated by practices enabled by new technologies. Warren and Brandeis popularized the classic definition of privacy as "the right to be let alone" in 1890 in response to their concerns that journalists were using the new technology of photography

to capture and publish images of private individuals. Moreover, Warren and Brandeis were sensitive to the commercial imperatives driving the use of this technology. They wrote:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.'

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'. For years, there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed ... (Warren & Brandeis, 1890)

Warren and Brandeis's interest in privacy was not a legalistic or theoretical one; it reflected their perception that new technologies and business practices were changing the modern experience of a private life by enabling others to invade established social boundaries (Steeves, 2002).

By the mid-1960s, concerns about the effect of technology on privacy had again come to the forefront, and generated what Regan calls a "literature of alarm" (Regan, 1995, p. 13). Bennett (1995, pp. 10-11) lists 21 examples of such books – including *The Naked Society* (Packard, 1964), *Privacy Under Attack*

(Madgwick, 1968), *The Death of Privacy* (Rosenberg, 1969), *The Assault on Privacy* (Miller, 1971), *The Rise of the Computer State* (Burnham, 1980) and *The Big Brother Society* (Will, 1983). The authors of these books argued that new communications technologies, such as listening devices and telephone taps, enabled the state to eavesdrop on conversations that were previously protected by the physical barriers between private and public spaces, permanently capturing the contents on audiotape. The information management powers of database technology raised the spectre of Big Brother, and many worried that the power of governments to monitor large populations would inexorably erode individual freedom and democratic governance.

This genre continues, with the publication of books like Charles Sykes' *The End of Privacy* in 1999 and Reg Whitaker's volume of the same name in 2000. Like the earlier literature, these books sound the alarm about the intrusiveness of modern technologies; however, the spotlight has broadened to include private sector surveillance. Whitaker, for example, argues that Big Brother has been "outsourced" to a myriad of "Little Brothers," private sector organizations that capture commercial and marketing data and use it to create detailed profiles of individual consumers. In this sense, private sector surveillance magnifies and extends the gaze of the state because it perfects the monopoly of information upon which Orwellian totalitarianism is based (Whitaker, 2000). However, as Bennett concludes, this genre has typically only painted a "crude picture of the

overall nature and effects of surveillance,” serving instead to draw public attention to the issue and highlight the weaknesses of the current policy regime (Bennett, 1995, p. 11).

The work of scholars considering issues of social interaction in networked spaces may help deepen the debate about privacy and technology. For example, Mulgan argues that “networks are nothing if not social” (Mulgan, 1991, p. 6); his analysis of the social relations emerging in the online world is based on a distinction between exogenous control, which is imposed and rational, and endogenous control, which is communicative and shared. Calhoun’s work on spatial organization also reminds us that technologically mediated relationships are still social relationships (Calhoun, 1992, p. 206). As such, both scholars provide a theoretical understanding of technological space as social space and address the need to apply social norms to new technologies. This may open up a more sophisticated debate about the effect of privacy invasive practices on technically mediated social relationships.

Samarajiva and Shields have attempted to theorize these relationships in the context of Custom Local Area Signaling Services, especially Caller ID. They draw on Giddens’ work on surveillance and argue that “one of the most dramatic discontinuities between non-modern and modern systems is the enormous expansion of stored information generated by the growth of capitalist enterprises and the nation-state” (Samarajiva & Shields, 1992, p. 407). They conclude that

Giddens' understanding of power as relational enables the theorist to critically unpack the dialectic of control emerging in the collection of transaction-based personal information over networks, and identify how this information is reconstituted as power .

Samarajiva and Shields also argue that Goffman's analysis of public spaces can inform our understanding of social interaction within the networked environment, particularly because the boundaries of private online spaces are negotiated by social actors (Samarajiva & Shields, 1992, p. 413). In this sense, integrating ethnomethodological analysis into privacy studies can help systematize inquiry regarding the relationships of social actors in electronically mediated spaces because ethnomethodology locates privacy in local social interaction.

Westin and the classical conception of privacy

However, Westin's 1967 classic, *Privacy and Freedom*, remains the most comprehensive attempt to theorize the relationship between technology and privacy. Like others writing at the time, Westin was concerned about the formidable surveillance capacities of emerging technologies. He sought to initiate a "discussion of what can be done to protect privacy in an age when so many forces of science, technology, environment, and society press against it from all sides" (Westin, 1967, p. 3).

As Regan notes, Westin did not reduce the problem to technology. Instead, he argued that the threat to privacy rests equally in technology and in the “organizational uses of these techniques and the benefits that various social, political, and economic actors gained through use of surveillance technologies” (Regan, 1995, p. 14). For Westin, technology is therefore both deterministic and shaped by social forces; a “projectile” that is thrown into organizational environments to shape and be shaped by the social practices and rules within that environment (Westin, 1980).

Westin feared that information technologies emerging in the 1960s threatened to disturb established democratic practices. He argued that liberal democracy requires a “balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance... The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life” (Westin, 1967, p. 24). Privacy accordingly involves two boundaries, one between the individual and others, and one between the individual and the state. Both boundaries are essential elements of a healthy democracy.

In this, Westin drew heavily from the liberal tradition of John Stuart Mill, who conceptualized society as an aggregate of rational individuals who act on both private, “self-regarding” purposes and on “other-regarding” matters relating to social order. For both Mill and Westin, there is a clear distinction between the

public and the private, and privacy is necessary so individuals can make rational, self-interested decisions with relative autonomy (Bennett, 1995, p. 4).

Westin hypothesized that privacy serves four functions: personal autonomy; emotional release; self-evaluation; and limited and protected communication. Personal autonomy is the wish to avoid being exposed to others or manipulated or dominated by them. Emotional release provides relief from the tensions of daily social life. Self-evaluation is the process of planning and contemplation that enables one to meaningfully integrate one's experiences. Limited communication is necessary to create and maintain interpersonal boundaries, and protected communication is used to share personal information with others in relationships of trust (Westin, 1967). As such, privacy serves to enable individuals to adjust to the emotional wear and tear of social life, and achieve self-realization.

Westin identified four states to achieve these ends: solitude; intimacy; anonymity; and reserve. Solitude is being free of observation by others. Intimacy involves withdrawal in small groups characterized by frank, relaxed and close personal relationships. Anonymity is achieved when one is in public and able to perform public acts without being identified or placed under surveillance. Reserve is the desire to limit the amount of information about you that is disclosed to others.

Westin's theoretical understanding of privacy as a necessary component of self-realization and healthy social interaction assumes a social context in which individuals make choices about the level of privacy they wish to enjoy. However, subsequent application of his framework has concentrated on information privacy as an attribute of the self in isolation from social praxis, and the social elements of his theory remain under-developed. Westin himself contributed to this dynamic in his later work which, for policymaking purposes, distinguishes between the attitudes of privacy fundamentalists, privacy pragmatists and privacy unconcerned individuals. He argues that the majority of people are pragmatic in their approach to privacy, and are willing to trade their own information for some benefit to themselves. This emphasis on privacy as trade-off mitigates against a more critical understanding of privacy as an emergent of social behaviour and a key component of democratic discourse.

Privacy and data protection policy

Although Westin's work has generated social and psychological research on the states and functions of privacy (as detailed below), it is most often quoted in regard to his 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" (Westin, 1967, p. 7). Indeed, Westin's claim that privacy is the individual's right to control his or her personal information has been at the root of most legislative activity since the 1970's, and continues to dominate the policy literature.

The majority of analysts either expressly or unconsciously limit themselves to questions about information privacy and the types of fair information principles required to operationalize privacy as informational control. For example, Reidenberg (1999) argues that the European Union's directive on data protection and the imperatives of the global information infrastructure will work to entrench fair information practices as the new global standard for privacy protection. Bennett and Grant (1999) contend that privacy has assumed the characteristics of a policy sector in which there is widespread international consensus around fair information practices as they have been articulated in data protection legislation. Cavoukian and Tapscott (1997), Cavoukian and Hamilton (2002), and Culnan and Bies (1999) argue that privacy can best be advanced by making the business case for compliance with data protection principles, and building the principles into privacy-enhancing technologies. Bennett and Raab (2002) envision a privacy "regime" that integrates privacy policy instruments – including data protection legislation, voluntary fair information codes and privacy-protective information practices – in a global economy which is characterized by regulatory interdependence.

As Bennett notes in his treatment of genetic privacy:

... many 'behavioural' privacy issues (e.g. video surveillance, polygraph testing, intelligent vehicle highway systems as well as genetic privacy) tend to become defined as information privacy questions. In all circumstances, personal information is collected or inferred as a result of

the observation of personal activity or behaviour. The subsequent storage, use and communication of that information raises a perennial set of information privacy claims (Bennett, 1995, p. 3).

Critiques of data protection

Even where analysts ascribe to a broader framing of privacy issues, fair information practices tend to dominate the discussion. For example, legal historian David Flaherty argues that “individuals in the Western world are increasingly subject to surveillance through the use of databases in the public and private sectors, and that these developments have negative implications for the quality of life in our societies and for the protection of human rights” (Flaherty, 1989, p. 1). As such, privacy protection is “going to require a more expansive effort at maintaining and encouraging all forms of privacy for individuals, not just enhancing data protection” (Flaherty, 1999, p. 29). Flaherty points to the need to strengthen constitutional protection, statutory torts for invasion of privacy and restrictions on some forms of surveillance. Nonetheless, he concludes that “I have never met a privacy issue that could not be satisfactorily addressed by the application of fair information practices... My fallback position would be to ransack the literature and practice of privacy and data protection for new ammunition for the protection of a valued human right” (p. 35).

However, the relationship between privacy as data protection and privacy as a

human right is problematic. I argue elsewhere that fair information practices do not capture the human rights side of the equation because they were designed by stakeholders to ensure that data will continue to flow into the information marketplace (Steeves, 1999a). Given the lack of bargaining power between individuals and information collectors, fair information practices such as consent provide the illusion of personal control without disturbing the flow of information. As Oscar Gandy notes, the individual's ability to withhold consent "is almost always insignificant in comparison with the power brought to bear when the organization chooses to withhold goods or services unless the information is provided" (Gandy, 1993, p. 19). Robert Gellman calls this "consensual invasion" and in his analysis of health privacy reform in the United States, he concludes that the consent process is designed to protect the interests of "everyone except the patient" (Gellman, 1999, p. 133). René Laperrière comes to similar conclusions in his analysis of Quebec privacy legislation. After reviewing the history of the province's data protection regime, he concludes that the ability of a consent-based regulatory scheme to protect privacy and contain a surveillance society is "highly debatable" (Laperrière, 1999, p. 183). Laperrière calls for a "deeper reflection" about the importance of privacy to democratic citizenship and the public interest.

Ursula Franklin (1996) argues that data protection does not lend itself to this "deeper reflection" because it is grounded in the language of the marketplace and accordingly restricts the policy options that are considered. She reminds us

that human rights discourses focus on citizenship, the relationship between groups in society, and the distribution and exercise of power. The language of the marketplace, on the other hand, speaks primarily about stakeholders and contractual agreements. As market discourses have come to dominate the policy debate, policy has been framed not in terms of rights and obligations between social actors, but in terms of contractual rights and fair information principles.

Some analysts have attempted to remedy the weaknesses in privacy as data protection by placing fair information practices in a larger context. For example, Gary Marx (1999) has attempted to broaden the issues addressed in the policy literature by incorporating an ethical analysis. Marx argues that fair information practices are limited because they do not provide a mechanism to question the appropriateness of the purpose for the collection, or the method used to gather the data. He sets out a comprehensive framework for an ethics of surveillance, based on a Kantian notion of respect for human dignity, that interrogates the means of collection, the context of collection, the social setting in which the principles are articulated and applied, and the use to which the information is put.

Similarly, Raab examines the paradigm of “balancing” the individual’s right to information privacy against societal benefits from a Dworkian conception of rights. He argues that weighing the value of privacy against commercial

efficiencies creates a danger that privacy protection may be absorbed into the “conceptual framework of consumerism” (Raab, 1999, p. 76). His point is well taken, given Regan’s work on the lobbying strategies and tactics used successfully by American business to weaken the European Data Protection Directive (Regan, 1999).

Some, like James Rule and Lawrence Hunter (1999) and Ken Laudon (1994) have argued that the commercial imperatives driving data collection can be offset by granting individuals a property right in their own personal information. This would lead to the development of marketplace mechanisms for individuals to make choices about how and when their personal information is used by others.

In spite of these correctives, many have concluded that the fair information practices which flow from Westin’s conceptualization of privacy as informational control have not, in effect, protected privacy; rather, they have served to privilege and legitimize the continued flow of personal information to institutions and technocratic elites (Rodota, 1976; Rule et al, 1980; Simitis, 1987; Gandy 1993; Steeves 2002).

The narrow focus on data protection in the policy literature has also made it difficult for policy makers to adequately address broader issues of privacy as a social value (Regan, 1995), human right and democratic value (Steeves, 2002; Canada, 1997). Regan’s 1995 *Legislating Privacy* is the most comprehensive

critique in this regard. There, Regan explores the effect of the current conceptualization of privacy on the policy making process in the United States. She concludes that privacy policy has failed because it is based on a notion of privacy that is rooted in a liberal understanding of the individual and society. If privacy is a right held by an atomistic individual against the state, then, since no right is absolute, it must be balanced against competing social interests (Regan, 1995, p. 16). The liberal conception of privacy is therefore vulnerable to communitarian attack because it pits the individual's interest in privacy against society's interest in competing social benefits, like medical research and protection against terrorism.

Communitarians have long argued that privacy may promote anti-social ends. In 1949, H.W. Arndt wrote, "the cult of privacy rests on an individualist conception of society, not merely in the innocent and beneficial sense of a society in which the welfare of individuals is conceived as the end of all social organization, but in the more specific sense of 'each man for himself and the devil take the hindmost'" (Arndt, 1949, p. 69). Similarly, Hannah Arendt's work was predicated on a rigid separation of public and private; and her interpretation of Kantian "reflective judgment" required that private, egocentric concerns be set aside in favour of those interests which are shared in common (Arendt, 1978).

These views resonate with the perspective of modern communitarians who argue that a good society must seek "a carefully crafted balance between

individual rights and social responsibilities” (Etzioni, 1999, p. 5). Since the individual’s right to be let alone detracts from the degree of participation, cooperation and community necessary to a healthy democracy, it must be balanced against competing social interests (Etzioni, 1994, 1999). Frank Cate puts it well:

... if privacy protects the combination to my safe..., it is extremely valuable to me and ... to society more broadly, which shares my interest in avoiding theft and criminal conduct. ... If, however, privacy permits me to avoid paying taxes or obtain employment for which I am not qualified, it may be very valuable to me, but extremely costly to society as a whole. It is clear, therefore, that neither privacy values nor costs are absolute ... What is needed is a balance, of which privacy is a part. Determining what that part is in any specific context requires a careful evaluation of subjective, variable and competing interests (Cate, 1997, p. 31).

The liberal conception of privacy as articulated by Westin reinforces both the dichotomy between the individual and the collective, and the need to balance privacy against other, competing interests. It is noteworthy that Etzioni defends the communitarian agenda with the following quote from Westin:

Each individual must, within the larger context of his culture, his status, and his personal situation, make a continuous adjustment between his need for solitude and companionship; for intimacy and general social intercourse; for anonymity and responsible participation in society; for

reserve and disclosure (Westin, 1967, p. 42, quoted in Etzioni, 1999, p. 200).

The concept of balance inherent in the classical conception of privacy has also made it difficult to advance human rights arguments in favour of privacy protection. Privacy as a human right is grounded in a belief in the value of human dignity and autonomy; in other words, privacy protection follows from a commitment to human dignity as a *prima facie* good. If human rights attach to the liberal individual, then they too are vulnerable to the communitarian attack because human rights require a leap of faith that an autonomous human actor infused with dignity is an inherently worthy ideal. As such, policy makers are often told to choose between the “relative” worth of individual dignity on the one hand, and collective goods, such as efficiency, security and cost-effectiveness, on the other. Regan argues that this search for balance has made it difficult to develop strong privacy legislation: “In policy debates, the individual interest was on weaker footing than the societal interest. Privacy was on the defensive because those alleging a privacy invasion bore the burden of proving that a certain activity did indeed invade privacy and that the individual privacy interest was more important than the societal interest” (Regan, 1995, p. 23).

Regan concludes that the dichotomy between the individual’s right to privacy and the collective interest is a false one, because privacy is a social value in and of itself. She writes:

Most privacy scholars emphasize that the individual is better off if privacy exists. I am arguing that society is better off when privacy exists. I argue that society is better off because privacy serves common, public and collective purposes. If you could subtract the importance of privacy to one individual in one particular context, privacy would still be important because it serves other important functions beyond those to the particular individual (Regan, 1993, p. 16).

Regan notes that Westin's work is "rooted in the social context": he is concerned with the ways in which social, economic and political factors detract from our experience of the private; he sees privacy as a cross-cultural phenomenon; and he argues that privacy serves important social functions in liberal democracy, such as religious tolerance, academic freedom, and restrictions on police powers (Regan, 1995, p. 27). However, Regan argues that Westin fails to develop the social meaning of privacy fruitfully because he anchors the concept to a "personal adjustment process" (Westin, 1967, p. 7) in which the individual decides for himself or herself, "with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public" (Westin, 1967, p. 42).

Regan argues that, for Westin and often for those policy makers building on his conceptualization of privacy as informational control, privacy is fundamentally at cross purposes with societal interests in disclosure (Regan, 1995, p. 28).

Privacy protection has therefore consistently given way in the face of what John

Westwood calls the “almost biological imperative” of governments and corporations to operate more efficiently in the promotion of collective interests (Westwood, 1999, p. 231). Regan concludes that “recognition of a social understanding of privacy will clear a path for more serious policy discourse about privacy and for the formulation of more effective public policy to protect privacy” (Regan, 1995, p. 220). She briefly introduces three models of privacy as a social value: privacy as a common value; privacy as a public value; and privacy as a collective value (pp. 221-231).

Regan’s first model, which conceptualizes privacy as a common value, draws on normative theory. Common values are those which, although they purport to protect the individual, are so fundamental that they are held in common by all members of society. The exercise of a common value may vary from individual to individual. For example, Regan argues that freedom of religion is enjoyed by individuals who believe in different things or belong to different religions. However, in spite of the differences in the manner of expression, all individuals share a common interest in the right itself. In like vein, the enjoyment of privacy may be defined by individuals in different ways, but all individuals share a common interest in privacy rights. Regan writes:

In both instances, prior to making the individual decision or choice about what to believe or where to draw a privacy boundary, individuals recognize the importance or need to develop their religious preferences and privacy boundaries. This step provides a common core that establishes space for

individual choices about what to believe or what should remain private.

More importantly, the common core also gives social importance to the freedom of conscience and privacy (pp. 221-222).

Regan argues that John Dewey's conceptualization of the public may provide theoretical grounds to link privacy to social relationships and democratic discourse. For Dewey, a public emerges from "the perception of consequences which are projected in important ways beyond the persons and associations directly concerned in them" (Dewey, 1927, p. 39). This perception of consequences creates a common interest, or, in Dewey's words, "concern on the part of each in the joint action and in the contribution of each of its members to it. Then there exists something truly social and not merely associative" (p. 181). Regan argues a similar common interest may exist in privacy, but does not develop this thought more fully.

However, Regan's reliance on Dewey does point to the possibility of enlarging the privacy debate by incorporating the insights of the American Pragmatists, such as Dewey and Mead. The Pragmatists argued that individuals are reflexive, intelligent beings capable of knowing themselves and the world, and therefore capable of the collective deliberation that is key to the ethical ideal of democracy. However, the act of knowing is not limited to individual consciousness; it is also part of a social process. Communication is key to democratic relationships because communication is what establishes the individual in a system of

common purposes, shared experiences and reflexive thinking. As such, Regan's desire to link privacy theory to Dewey's conception of the public supports my position that Mead's work on communication may help theorize the meaning of privacy as a social and democratic value.

Regan's second model, privacy as a public value, also draws on normative theory. From this perspective, privacy is important to the democratic process because it enables citizens to exercise other democratic freedoms, such as freedom of speech and freedom of association. Regan quotes from Thomas Emerson: "Democracy assumes that the individual citizen will actively and independently participate in making decisions and in operating the institutions of society. An individual is capable of such a role only if he can at some points separate himself from the pressures and conformities of collective life" (Emerson, quoted in Regan, 1995, p. 225).

Regan also suggests that privacy may be a public value because of the role it plays in restraining the exercise of power by the liberal state. In this sense, privacy does not only protect the individual; it also protects the community because it helps to set limits on the extent to which power can be used by the government. In addition, privacy may be essential to democracy because it is a pre-requisite for trust and accountability, and because it enables a sense of the common to develop. Here, Regan draws on Arendt, who argued that in order for the common to emerge, there must be "the simultaneous presence of

innumerable perspectives and aspects in which the common world presents itself and for which no common measurement or denominator can ever be devised” (Arendt, quoted in Regan, 1995, p. 226).

Regan’s third model, privacy as a collective value, is derived from the economic notion of public goods. Public goods are, by definition, indivisible; no one member of society can enjoy them to the exclusion of others. Because of their special nature, an optimal level of production of public goods will not be achieved through the market. Regan examines attempts to treat privacy as a private good, or commodity, that can be bought by individuals in the marketplace, and argues that this approach is inefficient for three reasons.

First, information collectors have no incentive to provide individuals with information about the ways in which privacy is commodified because it would discourage people from providing information which would, in turn, lower the market value of the commodity. Second, the collection or disclosure of personal information often occurs without the individual’s consent, both because many relationships are not truly voluntary and because the individual is often not a party to relationships which involve the exchange of information about him or her. For example, an individual applying for a bank loan cannot negotiate a level of privacy without losing access to the financial service, so disclosure in that case is not based on the individual’s consent; and employee medical records may be disclosed to the employer because the employer has a contractual

relationship with the group insurer independent of the individual employee.

Third, computer network design is so complex that, in order for the individual to enjoy some level of control over the flow of his or her personal information, privacy must be built into the system as a whole. Privacy, therefore, is less an individual attribute than an attribute of the information system itself.

Westin's conceptualization of privacy as informational control is therefore subject to a number of critiques in the literature. Much of the criticism reflects the fact that the social elements in Westin's theory remain undeveloped. This suggests that Mead's work may potentially advance the critique inherent in the classic conception of privacy by providing theoretical justification for privacy as a social emergent of language, and Habermas's appropriation and extension of Mead may provide fertile ground for understanding the role privacy plays in public life and democratic discourse.

Privacy and surveillance

The social consequences of invasive technologies have been explored in the sociological literature on surveillance. For example, in 1980, James Rule and his colleagues criticized Westin's theory of privacy because Westin's framework is unable to curb the insatiable appetite of bureaucracies for personal information. Although procedural rules regarding the collection and use of information may create fairer and more efficient data protection systems, they argued that information privacy rights ultimately cannot constrain the development of

increasingly invasive technologies. Accordingly, they concluded that Westin missed the point as he failed to address the underlying problem of social control enabled by the state's growing ability to place people under surveillance (Rule et. al., 1980).

The early work on surveillance followed Rule's lead and focused on the social effects of surveillance by state bureaucracies (e.g., Rule, 1974; Marx & Reichman, 1984; Marx, 1988; Clarke, 1989). In this sense, the problem was located in the imperatives of bureaucratic organization (Bennett, 1995, p. 11). Lyon notes that it was only "late in the day [that] sociology started to recognize surveillance as a central dimension of modernity, an institution in its own right, not reducible to capitalism, the nation-state or even bureaucracy" (Lyon, 1994, p. 219).

Oscar Gandy was one of the first to extend his inquiry beyond state surveillance practices. Applying the work of Marx, Ellul, Giddens, Weber and Foucault, he concluded that the massive surveillance conducted by the private sector on a daily basis is structured around a "panoptic sort", a "difference machine that sorts individuals into categories and classes on the basis of routine measurements. It is a discriminatory technique that allocates options and opportunities on the basis of those measures and the administrative models that they inform" (Gandy, 1993, p. 15).

David Lyon's work on surveillance is grounded in similar thinking. Lyon argues that modern surveillance enables a type of "social sorting" where computer code is used to classify groups of people in "ways that tend to reinforce social divisions" (Lyon, 2003). It also raises fundamental questions about "where the human self is located if fragments of personal data circulate within computer systems, beyond any agent's personal control" (Lyon, 1994, p. 18).

The insights of the sociological literature have not been well integrated into privacy theory, perhaps because many theorists of surveillance contend that privacy is too narrowly conceived to address the problems faced by advanced industrial states (Bennett, 1995, p. 9). It also reflects the fact that the policy literature is rooted in liberalism, whereas scholars examining surveillance have approached the issue from a more critical, sociological perspective. A theoretical framework which could account for the effect of surveillance on social relationships and human identity would accordingly advance the literature.

Privacy as a social psychological concept

Westin's work has generated empirical psychological research on the states and functions of privacy, and this research has both supported his theory (Pedersen, 1979, 1999) and extended it (Margulis, 2003a, p. 414). For example, Marshall has added seclusion and "not neighbouring" (or limiting contact with neighbours) to Westin's original four states (Marshall, 1970, 1974), deepening the connection

between Westin's categories and an empirical understanding of social behaviour. Hammitt has extended Westin's understanding of solitude by applying his framework in wilderness environments (Hammitt, 1982, 2000). Hammitt has found that, although people seek privacy in wilderness, their experiences of solitude are quite social and encompass close interaction with intimate others. In addition, a number of researchers have used Westin's work to develop scales to measure privacy (Marshall, 1974; Dawson & Hammitt, 1996; Hammitt, 1994; Pedersen, 1996, 1999).

The relationship between privacy and identity has also been explored in the philosophical literature. Charles Freid argues that privacy is an integral part of trust, respect for others and love; as such, it is central to human identity and healthy social relationships. Ethicist Greg Walters has built on Freid's work, and articulated a human rights framework in which privacy is a necessary condition of human action subsumed within the right to freedom:

A person's right to freedom is violated if she is subjected to ... procedures that attack or remove her informed control of behaviour by her own unforced choice. The right to freedom includes having a sphere of personal autonomy and privacy whereby one is left alone by others unless he or she unforcedly consents to undergo the actions of others (Walters, 2001, p. 165).

However, the most comprehensive social-psychological treatment of privacy was

developed independently by Irwin Altman. Altman informs his analysis by examining how people in different cultures regulate social interaction. He defines privacy as the “selective control of access to the self or to one’s group” (Altman, 1975, p. 18), and identifies eight features or properties of privacy:

- It is an “interpersonal boundary-control process” which is used to regulate and pace interaction with others;
- One may have too much or too little privacy. Privacy is optimized when the desired level of interaction with others (“desired privacy”) is the same as the actual extent of contact with others (“achieved privacy”);
- Privacy is a dialectic process, in which opposing forces for the opening or closing of the self to others shift over time;
- Privacy is an optimizing process, in which people seek a congruence between desired privacy and achieved privacy;
- Privacy involves an attempt to regulate both inputs *from* others and outputs *to* others;
- Privacy involves a variety of social relationships – between individuals, individuals and a group, groups and individuals, etc.;
- Behavioural mechanisms – including verbal and paraverbal behaviour, personal space, territory, and cultural mechanisms – are used to achieve privacy; and
- Privacy functions include the regulation of social interaction and self-identity.

For Altman, privacy is inherently a social process which is enacted in the local situation. As such, it is constructed in culturally specific ways, but remains a cultural universal (Altman, 1977).

Altman draws on the work of Erving Goffman to support his theoretical framework. For example, in his study of daily life in a mental institution, Goffman (1961) noted that patients were given little to no control over their bodies, clothing and possessions; staff forced patients to undress, bathe and have their hair cut without any input from the patients, and removed their personal possessions from them. Altman argues that these intrusions and the resultant lack of control infringes on the patients' privacy-regulation mechanisms and as such, "prevent[s] the self from being under the control of the individual" (Altman, 1975, p. 37).

Edward Hall's work on personal space is also instructive. Hall suggests that people recognize an invisible boundary around the self that is used to regulate social interaction, and notes that intrusions into this space cause discomfort and tension. Altman sees this space as one of many privacy-boundary mechanisms which, like clothing, possessions, and doors, are used by social actors to maintain a desirable level of privacy. Altman's link between these mechanisms and a sense of self also suggests that Mead's premise that the self emerges through symbolic interaction may provide fruitful ground for a theory of privacy that can account for privacy as a social value.

Like Westin's, Altman's theory has generated empirical psychological research on privacy that has supported and extended his work (Margulis, 2003b). For example, Kupritz (2000) identifies cognitive and environmental mechanisms which are used to achieve privacy. Petronio (2002) builds on Altman when he argues that privacy management is the "process of opening and closing a boundary to others" according to rules that determine how people decide whether or not to reveal or disclose personal information. Others have used Altman's framework to explore crowding (Evans, Lepore & Allen, 2000; Kaya & Erkip, 1999), territorial behaviour in a variety of social settings (Kaya & Weber, 2003; Rosenblatt & Budd, 1975) and interior architectural design (Demirbas & Demirkan, 2000).

Margulis notes that Westin's and Altman's theories share much in common.

They both:

- define privacy in the context of limiting control or regulating access to the self;
- conceive of privacy in terms of a dialectic process by which individuals respond to internal and external conditions;
- agree that privacy, although universal, takes culturally specific forms; and
- argue that privacy is necessary for self-evaluation, self-identity and individuality (Margulis, 2003b, pp. 245-246).

However, rather than focusing on the narrow confines of informational control as Westin does, Altman more fully develops the ways in which people use culturally

specific notions of privacy as a social universal to regulate social interaction. In that sense:

Altman's theory of privacy proposes an original idea that joins social psychological and environmental psychological concepts – people use human spatial behaviour techniques (that is, the environmental mechanisms of territoriality, personal space, and crowding) to regulate social interaction... Altmans' theory is comprehensive, one that should, in principle, subsume narrower theories that emphasize control over informational output to others, such as Westin's theory (Margulis, 2003a, p. 422).

Gaps identified in the theory

As noted above, the insights of the sociological literature have not been well integrated into privacy theory, and the current understanding of privacy as individual control over personal information is problematic. However, in spite of concerns that this narrow understanding is neither resilient enough a concept to protect privacy as a human right nor able to account for the role privacy plays in the development of identity, data protection continues to dominate the intellectual field. Accordingly a theory that can account for the sociality of privacy would advance the literature and strengthen our understanding of privacy as a social and democratic value.

Bennett argues that privacy:

... raises central and enduring questions about the power of the state, the respect for civil liberties, the relationship between the state and civil society, the definition of the 'subject' within conditions of modernity (or post-modernity). I would contend, however, that the political theory of privacy ... has largely operated within a liberal paradigm and has not yet confronted more profound ontological and epistemological issues (Bennett, 1995, p. 6).

Regan's three models of privacy as a social value provide entry into these issues. In particular, her reliance on Dewey's conceptualization of the public suggests a link between privacy and the self-reflexive conditions necessary for the workings of modern democracy.

Margulis identifies three ways in which privacy is social. First, privacy focuses on interpersonal communication and social interaction. Second, privacy can only be experienced and understood in the context of our social and cultural development. Third, groups as well as individuals enact privacy (Margulis, 2003a, p. 248). Margulis concludes that we have much to gain by revisiting Westin and Altman, and expressly incorporating social psychological insights into privacy theory (Margulis, 2003b).

Beyond Westin - Applying Mead and Habermas to the privacy debate

In this dissertation, I attempt to address these gaps in the literature by arguing three interconnected theses. First, I argue that Habermas's conceptualization of

communicative rationality helps to explain the ways in which the social meaning of privacy has been marginalized in favour of instrumental rules which privilege efficiency and control. Second, I argue that Mead's theory of communication can anchor privacy in social praxis, and provide a theoretical basis for privacy as a social emergent that flows from language. Last, I argue that Habermas's appropriation of Mead's work locates privacy at the centre of democratic discourse and can inform a theory that grounds privacy as a social and democratic value.

The current conceptualization of privacy as informational control focuses on data which has been divorced from its social context. Policy documents accordingly talk about data subjects and data holders, rather than people's concrete social experiences of privacy and privacy invasions. This makes it difficult for policymakers to adequately protect the social meaning of privacy in everyday life from communitarian arguments in favour of surveillance, even when that surveillance erodes the exercise of democratic freedoms.

Mead's theory of symbolic interactionism can act as a corrective to this because it locates the site of all action in the local situation and grounds the social in communication. From a Meadian perspective, the self is constructed through social interaction. As Burke notes, Mead sees the self "as a social product, stressing the sociality of action *and* reflection, and viewing thought as the internalization of objective relationships" (Burke, 1939, p. 292, emphasis added).

Mead argues that mind emerges through and within the social processes of communication. He identifies two phases of the communication process. Both phases presuppose the presence of two or more individuals who are interacting in a social context. He calls the first phase the “conversation of gestures.” In his famous example of the dog fight, he illustrates how, in this phase of communication, actors gesture in response to each other in a chain of stimulus-response:

The act of each dog becomes the stimulus to the other dog for his response. There is then a relationship between these two; and as the act is responded to by the other dog, it, in turn, undergoes change. The very fact that the dog is ready to attack another becomes stimulus to the other dog to change his own position or his own attitude. He has no sooner done this than the change of attitude in the second dog in turn causes the first dog to change his attitude (Mead, 1934, pp. 42-43).

This first phase of communication is unconscious because neither actor is aware of the response his or her gestures elicit in the other actor. Because of this, neither can respond to the gestures he or she is making from the standpoint of the other. Mead writes:

We have here a conversation of gestures. They are not, however, gestures in the sense that they are significant. We do not assume that the dog says to himself, “If the animal comes from this direction he is going to spring at my throat and I will turn in such a way.” What does take

place is an actual change in his own position due to the direction of the approach of the other dog” (p. 43).

Mead argues that language is what marks the transition from non-significant interaction in phase one to significant interaction in phase two. He defines language as “communication through significant symbols. A significant symbol is a gesture (usually a vocal gesture) that calls out in the individual making the gesture the same (ie. functionally identical) response that is called out in others to whom the gesture is directed” (Cronk, 2001).

The second phase, the “conversation of significant gestures”, is what makes intelligent social organization possible because it necessarily entails the ability of each actor to view his or her own gestures from the perspective of the other. This enables us to take on more complex sets of behaviours, or roles, because, by taking the position of the other, we learn to foresee or anticipate how the other will act and what is expected of us in a variety of social situations. It also enables the self to emerge, because, through language, we become conscious of a generalized other:

In any co-operative process, such as the family, the individual calls out a response from the other members of the group. Now, to the extent that those responses can be called out in the individual so that he can answer to them, we have both those contents which go to make up the self, the "other" and the "I." The distinction expresses itself in our experience in

what we call the recognition of others and the recognition of ourselves in the others. We cannot realize ourselves except in so far as we can recognize the other in his relationship to us. It is as he takes the attitude of the other that the individual is able to realize himself as a self (Mead, 1934, p. 194).

Mead's understanding of the self resonates with Westin's third function of privacy: self-evaluation. Westin argues that privacy is essential to the process of contemplation through which people can meaningfully integrate their experiences into their sense of self-identity. Mead, too, recognizes the need for withdrawal from others to enable the self to internalize what it has learned from social interaction. However, Mead's conceptualization is richer than Westin's because it is inherently social; he argues that the individual "can enter as an object only on the basis of social relations and interactions, only by means of his experiential transactions with other individuals in an organized social environment" (Mead, 1934, p. 225).

Mead's work also provides a third way which can resolve the impasse between the liberal individual and the communitarian collective. He writes:

Mentality on our approach simply comes in when the organism is able to point out meanings to others and to himself. This is the point at which mind appears, or if you like, emerges.... It is absurd to look at the mind simply from the standpoint of the individual human organism; for, although

it has its focus there, it is essentially a social phenomenon; even its biological functions are primarily social (Mead, 1934, pp. 132-133).

As such, the self emerges through language because it is through language that the individual learns to take the perspective of the other. Because the self is a social emergent, there is no inherent contradiction between the individual and the collective; the self is only able to form through interaction with the collective. Accordingly, Mead rejects the liberal view which prioritizes the self over the social. Locating privacy in this dialogue, then, may potentially dissolve the current stalemate which pits privacy against the social, and enable privacy theory to account for the social nature of the individual's experience of privacy.

Mead's work may also help theorize the relationship between privacy and autonomy. For Mead, the self's private response to the social environment is active, not passive. The "me" or the "conventional, habitual individual" (Mead, 1934, p. 197) consists of "the organized set of attitudes of others which one himself assumes" (p. 175) from symbolic interaction. However, the "I" consists of the creative response, or "novel reply" (p. 197) of the individual to the attitudes of others. Since the "I" is the individual's response to the social self, it cannot be known in the present, but only in the memories of the "me". However, the "I" emerging in the present implies a change in the "me" of the future. The "I" therefore can only be determined after it has occurred. Although the "I" is captured by the "me" as a historical figure, the emerging "I" cannot be subjected to predetermination and, as such, is free. Accordingly, Mead's understanding of

sociality implicitly recognizes the need for a reflective space in which the individual enters into a dialogue as an object to herself. This resonates with Westin's first function of privacy, personal autonomy. Autonomy is often connected to privacy in the literature, but the relationship between the two concepts has not been fully explored. The dialogue between the social "me" and the emergent "I" which occurs in a private, reflective space may provide a theoretical basis to better understand this relationship.

Mead's dialectical approach to identity formation through language also provides an interesting point of departure to deepen the four states of privacy Westin identifies: solitude; intimacy; anonymity; and reserve. Mead argues that it is the conversation of significant gestures that enables the social actor to view her own gestures from the perspective of the other. Collins explains:

Words are verbal gestures whose significance is the intended action they convey to their hearers; understand a language is made possible by taking the role of the other person... It is the Generalized Other – the open-ended capacity of humans to take the point of view of anyone at all – which constitutes a world of permanent objects for the individual mind (Collins, 1998, p. 682).

In this sense, there are different layers of symbolic interaction: the dialogue between the "me" and the "I"; the conversation of significant gestures in which each actor views his own gestures from the perspective of the other; and the dialogue with the Generalized Other.

From this perspective, Westin's four privacy states can be grounded in the social as each state relates to a different level or layer of symbolic interaction. Solitude is conducive to self-reflection, which involves a dialogue between the social self and the undetermined, emancipatory self. Intimacy – or interaction within a private sphere that includes trusted others – enables the individual to integrate social experiences into self-identity and form significant personal relationships with proximate others. Anonymity and reserve enable the individual to enter into dialogue with the Generalized Other while still maintaining the critical space between self and other that enables individuals to meaningfully integrate social experiences and, in so doing, together construct the meaning of the social. This approach, in which privacy is explained in the context of varying levels of social connection, is consistent with Altman's argument the privacy is an "inter-personal boundary control process" (Altman, 1975, p. 10) which is dialectic in nature and which seeks to regulate social interaction and self-identity.

Since "each individual stratifies the common life in a different manner, and the life of the community is the sum of all these stratifications" (Mead, 1964, pp. 276), privacy erosions which restrict the individual's ability to enter into symbolic interaction accordingly impoverish social life. Again, Mead's work offers a theoretical foundation for privacy that resolves the apparent conflict between privacy and the social interest and may more fully explain the social role privacy plays in the construction of community.

Mead's work is also significant because it is the foundation of social psychological and ethnomethodological studies of the everyday meaning of privacy. Indeed, Altman's insight that privacy is an inherently social process enacted in the local situation in culturally specific ways is rooted in Mead's social psychology, and ripe for further development. By exploring the ways in which privacy is embedded in everyday life, we can deepen our understanding of the role privacy plays in the social construction of meaning. This can inform a theory of privacy that explains privacy as a social emergent of language.

Habermas builds on Mead's insight that language is the medium in which we construct a sense of identity with respect to self, proximate others and the Generalized Other because it is the only medium in which we can take the perspective of the other. Habermas argues that this ability, the ability to take the perspective of the other, extends to general forms of interaction, including role taking. At a cognitive level, we come to understand the nature of roles within society and the rules surrounding interaction itself through communicative interaction. As such, social roles are not simply properties of a social system; they are contested and negotiated in the context of everyday life (Winseck, 2001). Placing privacy at the centre of communicative interaction (i.e. as a key component of the dialogue between self, other and Generalized Other) may help theorize the social consequences of privacy-invasive practices, including ways in which surveillance effects social interaction, democratic discourse and the exercise of fundamental freedoms.

Habermas moves in this direction when he discusses the relationship between private autonomy and public autonomy. Habermas criticizes liberal and welfare state models of law because both focus on individual or private autonomy; the bourgeois model seeks to guarantee private autonomy through individual rights, and the welfare state model seeks to generate and secure the material equality that is a precondition to the exercise of private autonomy. Habermas concludes that both models “lose sight of the democratic meaning of a legal community’s self-organization” (Habermas, 1998a, p. 18) because they fail to account for the inter-relationship between private autonomy and public participation.

Habermas applies the discourse principle to develop a proceduralist paradigm of law in which a public of private citizens participates in political communication to “articulate their wants and needs, to give voice to their violated interests, and, above all, to clarify and settle the contested standards and criteria according to which equals are treated equally and unequals unequally” (*ibid*). For Habermas, one of the central problems in modernity reflects the fact that this type of communicatively-derived consensus has been eclipsed by instrumental rationality. Habermas rejects the conclusion that domination is inherent in instrumental reasoning (Feenberg, 1999, p. 151) and argues that rational-purposive thinking is appropriate within the sphere of purely technical control over nature, a sphere he calls the systems world. However, he concludes that the systems world must be understood within a “conceptual framework that also includes a normatively regulated social ‘lifeworld’” (Feenberg, 1995, p. 79). The

operative principle of the lifeworld is not instrumental reasoning but communicative rationality, the pursuit through dialogue of agreement based on “a common world of norms and meanings, an identity” (p. 78).

For Habermas, the problem of technocracy is not that the rationalization of modern societies leads inexorably to domination, as Horkheimer and Adorno (1972) concluded. Rather, Habermas argues that the systems world has become uncoupled from the communicatively generated normative understanding of the lifeworld, and has imposed the rational-purposive pursuit of efficiency, control and predictability in an increasing number of lifeworld activities. Feenberg describes it this way:

Technocracy represents a generalization to society as a whole of the type of ‘neutral’ instrumental rationality supposed to characterize the technical sphere. It assumes the existence of technological imperatives that need only be recognized to guide management of society as a system.

Whether technocracy is welcomed or abhorred, these deterministic premises leave no room for democracy (Feenberg, 1995, p. 75).

As such, Habermas’s theory of communicative interaction may inform our understanding of the ways in which the discursively-generated understanding of privacy as it is lived in the lifeworld has been marginalized by the managerial interest in efficiency, security and control.

Habermas concludes that, in order to enable individuals and publics to regain

control of the socio-political and economic environment, the communicative rationality of the lifeworld must reassert ascendancy over instrumentalism. However, given the complexities of modern life, public discourse by itself can no longer coordinate the diverse and anonymous relations inherent in modern societies; what is needed is a form of “sociological translation” that can account for both social complexity and the normative principles articulated in the lifeworld through communication. He concludes that “[law] is the only medium that can fulfill the demands for society-wide integration and at the same time remain rooted in communicative interaction” (Habermas, 1999, p. 913).

For Habermas, then, democracy is derived from the “interpenetration” of communicative rationality and the legal form. Interpenetration occurs when the conditions for a “discursive exercise of political autonomy” are institutionalized in law as a “system of rights” that guarantees private autonomy *and* public participation (Habermas, 1999, p. 121). This can only be achieved if the law maintains a creative tension between social facticity and normative discourse.

Habermas moves beyond a self-evident notion of private autonomy grounded in an independent morality; instead, he links private autonomy to social fact through the exercise of inter-subjective dialogue. From this perspective, no legal regulation can:

... *adequately* concretize the equal right to an autonomous private life, unless it simultaneously strengthens the effectiveness of the equal rights

to exercise political autonomy, that is, the right to participate in forms of political communication that provide the sole arena in which citizens can clarify the relevant aspects that define equal status (Habermas, 1998a, p. 25).

As such, Habermas can inform our understanding of the ways in which legal protections that deal with privacy divorced from its social value can weaken the conditions necessary for democratic discourse.

This dissertation puts Westin into dialogue with Mead and Habermas, to gain a better understanding of the social elements of privacy theory that were marginalized when data protection principles became the focus of intellectual attention in this sphere. In addition, it lays the groundwork for a theory that: (1) conceptualizes privacy as a social value that emerges through language; and (2) explains why privacy is an essential element of social interaction and democratic discourse. Such a communication-based theory may provide policymakers with an alternative to data protection arguments, and help move policy discourse beyond the limits of the balancing paradigm inherent in conceptualizing privacy as informational control.

I begin in Chapter Two with a brief overview of the competing legal frameworks in place to protect privacy. I argue that the law has consistently translated the social experience of privacy into legal remedies, and that privacy was a sustained concern before the emergence of computing technologies in the 1960s

and 70s. In Chapter Three, I set out a historical analysis of the development of data protection regimes in Western democracies from the 1970s forward. This examination of the rise of data protection laws in early adopting jurisdictions focuses on the reasons why fair information practices were enacted. I use a summary comparative legal analysis to identify similarities and differences between data protection regimes in Europe, the United States and Canada, and apply Habermas's theory of lifeworld and systems world to explain how data protection laws have constrained and reconstructed the social meaning of privacy to accommodate the imperatives of managerialism and technical innovation.

In Chapter Four, I conduct a textual analysis of Alan Westin's seminal work on privacy, *Privacy and Freedom*, to identify the social elements of Westin's theory that have remained underdeveloped. I argue that Westin's work is rich in sociality; however, Westin does not fully develop the social nature of privacy because of his focus on information flow. By conceiving of privacy as social withdrawal, privacy protection is defined as the ability to control the flow of personal information from the complete privacy of solitude to increasing levels of exposure as the individual leaves solitude for interaction with intimate and general others. This places the individual's need for privacy in conflict with both his or her need for sociality and the community's need to invade privacy for the purposes of social control.

In Chapter Five, I examine how Irwin Altman has appropriated and extended Westin's social understanding of the private, through textual analysis of Altman's work on privacy. I then apply Mead's writings on symbolic interaction and the dialogue between the me and the I to deepen Westin's insights into the social value of privacy, and to extrapolate the ways in which privacy facilitates and is necessary to the Meadian understanding of social discourse. Next, I explore how Mead's work has been extended by Jurgen Habermas, through a textual analysis of Habermas's writings on inter-subjectivity and law. Last, I propose an alternative conceptualization of privacy as a social emergent of language which extends the sociological underpinnings of Westin's work and frees the policy questions from the current focus on an abstracted set of information practices.

In order to test whether or not this alternative conceptualization can inform more effective policy, Chapter Six compares and contrasts the policy implications of applying data protection principles to the protection of children's online privacy with a policy model that incorporates the theoretical insights of Mead and Habermas. This will test whether or not a communication-based theory of privacy can better protect the social value of privacy in this context. I argue that data protection principles are ineffective in protecting children's online privacy because consent-based mechanisms are easy to circumvent online, and children's consent is easily manipulated. By focussing attention on procedural rules, data protection also constrains the potential for a broader debate on the social value of aggressive online marketing to children. A communicatively

based understanding of privacy reopens this question, and enables policy makers to examine the impact of marketing practices on children's identity formation and social relationships.

Finally, in Chapter Seven, I summarize the results of the preceding analysis and outline a theory of privacy as a social emergent of language that can account for the ways in which privacy is embedded in social praxis, and potentially broaden the existing pool of policy alternatives to better protect the social and democratic value of privacy against technologies of surveillance and control.

Chapter Two – Legal Frameworks to Protect Privacy

Privacy protection is facilitated through a number of legal frameworks, including data protection, constitutional guarantees, criminal law, and the law of torts. Data protection draws heavily from Westin's definition of privacy as informational control, and data protection legislation typically adopts some or all of the information management principles Westin first identified in *Privacy and Freedom* (1967). These fair information practices (FIPs) include:

- **Accountability:** A data collector should be accountable to the individual for its collection and use of personal information;
- **Identified Purpose:** The data collector should tell the individual the reason why personal information is being collected at or before the time of collection;
- **Knowledge and Consent:** Personal information should only be collected, used and disclosed with the individual's knowledge and/or consent;
- **Limited Collection:** The data collector should only collect personal information which is relevant to the identified purpose, and should use fair and lawful means to collect the information;
- **Limited Use:** The data collector should only use the personal information for the identified purpose;
- **Retention:** Personal information should only be retained as long as necessary to fulfill the identified purpose;
- **Accuracy:** Personal information should be accurate, complete and up to

date;

- Security: Personal information should be protected by appropriate security measures;
- Openness: The data collector should be open and transparent with regard to its information practices; and
- Right of access and Correction: The individual should have the right to see his or her file, and to have any inaccurate information corrected.

As Chapter One demonstrates, Westin's model of privacy as informational control has come to dominate the privacy literature. In Chapter Three, I will examine how Westin's data protection program became the dominant model of policy making from 1970 forward.

This chapter contains a review of the legal tradition dealing with privacy that was in place before data protection came to dominate the legislative playing field. I argue that, prior to the introduction of data protection, the law consistently translated both the social experience of privacy and democratic principles into a number of legal remedies designed to protect privacy interests. These remedies cluster around three anchors: constitutional and criminal protections against the invasive power of the state; the sanctity of private property; and legal protections for reasonable expectations of privacy. The presence of these legal traditions indicates that privacy was a sustained concern well before the 1970s, prior to the penetration of computing technologies into everyday life. This supports one of the main themes of this thesis, that privacy is not a response to technological

imperatives but a social value with historical and cultural underpinnings, which is rooted in historical memory and social experience.

Constitutional and criminal protections against the invasive power of the state

Liberal democracies have traditionally sought to limit the exercise of governmental power against the individual. Accordingly, protecting the individual's private sphere has been a central theme in constitutional guarantees of political and legal rights. For example, the Fourth Amendment to the American Constitution protects the individual from unreasonable search and seizure. Rosen argues that the Fourth Amendment was a direct response to the types of invasive practices practiced by the British monarchy, and that Englishman John Wilkes's experience as a critic of King George III, for one, made a deep impression on early American lawmakers. After Wilkes (a duly elected Member of Parliament) attacked the King's policies both in Parliament and in the press in 1763, King George ordered his agents to break into Wilkes's home and seize his private diaries. Rosen argues: "The writers of the U.S. constitution drafted the Fourth Amendment banning unreasonable searches and seizures of persons, houses, papers and effects, with Wilkes' house and Wilkes' papers in mind" (Rosen, quoted in McDougall, 1999, p. 9).

Although there is no constitutional right to privacy in Canada¹, the Supreme Court of Canada has written a limited right to privacy into the *Canadian Charter of Rights and Freedoms*. Section 8 protections against unreasonable search and seizure include the right to be secure from such a search when the individual has “a reasonable expectation of privacy” (*Hunter v. Southam* (1984) 152 D.L.R. (4th) 577). Reasonable expectation has been defined as the expectation that the state will not surreptitiously record communications “that the originator expects will not be intercepted” without first obtaining a search warrant (*R. v. Duarte*, [1990] 1 S.C.R. 30 at 46). The Supreme Court has also found that s. 7 of the Charter, which guarantees the right to life, liberty and security of the person, contains a right to a reasonable expectation of privacy².

At the provincial level, Quebec is the only province with a quasi-constitutional right to privacy. Chapter III of the *Civil Code of Quebec* provides, “Every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person unless authorized by law” (s. 35). Under s. 36, the following acts are considered to invade a person’s privacy:

- entering or taking anything in his dwelling;
- intentionally intercepting or using his private communications;

¹ The original 1979 draft of the Charter included a right to privacy in 1979, but it was removed before the draft was finalized.

² See *Godbout c. Longueuil (Ville)* (1997), 152 D.L.R. (4th) 577 and *Blencoe v. British Columbia (Human Rights Commission)* [2000] S.C.J. No. 43.

- appropriating or using his image or voice while he is in private premises;
- keeping his private life under observation by any means;
- using his name, image, likeness or voice for a purpose other than the legitimate information of the public; and
- using his correspondence, manuscripts or other personal documents.³

In addition, s. 5 of the *Quebec Charter of Human Rights and Freedoms* provides, "Every person has a right to respect for his private life", and s. 8 ensures that, "No one may enter upon the property of another or take anything therefrom without his express or implied consent."

The *Criminal Code of Canada* also seeks to protect the liberal understanding of the relationship between the individual and the state. Accordingly, the state is not allowed to invade the individual's private sphere without just cause and prior authorization from a judicial officer.⁴ In addition, provisions restricting fundamental freedoms typically criminalize certain forms of expression, including obscenity⁵ and hate propaganda, only when uttered in public. Private expression

³ It is interesting to note that ss. 37-41 of the Civil Code include a set of fair information practices which apply when any person "establishes a file on another person." These sections of the *Civil Code* frame Quebec's data protection legislation by contextualizing fair information practices within a broader definition of privacy.

⁴ See for example s. 487 (search warrants) and ss. 184.1-188.1 (wiretapping provisions).

⁵ The one exception to the general rule that private expression will not be criminalized is s. 163.1(2) which makes simple possession of child pornography an offence. Private consumption of other forms of obscenity is not an offence; under s. 163, obscene material must be published or distributed in order to attract criminal liability.

is given much wider latitude⁶. The privacy of personal communications is also protected through criminal sanctions. For example, it is a crime to stop or search mail (s. 345), steal mail (s. 356), or intercept a private communication without the consent of the originator of the communication or the person intended to receive it (s. 184). Criminal and constitutional law are accordingly significant vehicles to protect privacy interests, especially those of the private citizen vis-a-vis the state⁷.

Property

The *Criminal Code of Canada* contains a number of provisions to protect private property. Offences, such as:

- break and enter (s. 348);
- being unlawfully in a dwelling house (s. 349);
- trespassing at night (s. 177);
- forcible entry (s. 72); and
- mischief (or the destruction of, damage to, or interference with the lawful enjoyment of real or personal property, s. 430);

all assume that the individual's private space should be protected against invasions from others. Similarly, it is a crime to watch or beset a person's residence or place of work with the intent to intimidate him or her (s. 423(1)(f)).

⁶ See Steeves (1998) for a fuller treatment of this dynamic.

⁷ However, as discussed on p. 60 ff. below, these discourses have been limited by the courts' reliance on reasonable expectations of privacy.

Civil actions for trespass and defamation also provide remedies when an individual's private property is violated or false statements are published which injur his or her reputation. In addition, statutory actions for invasion of privacy are available in British Columbia, Saskatchewan and Manitoba⁸.

The question of whether or not there is an actionable claim for invasion of privacy at common law remains an open one in Canada.⁹ In *Krouse v. Chrysler* ([1970] 3 O.R. 135), the plaintiff, a professional football player, sued Chrysler for invasion of privacy after Chrysler used a photograph including his image in an advertising campaign. An Ontario judge refused to dismiss the action in its early stages because he was not satisfied that a Court would not recognize a general right to privacy. When the *Krouse* case reached the Ontario Court of Appeal four years later, Justice Estey did not address this question. Instead, Estey held Krouse would be entitled to damages if his personality had been appropriated for commercial gain, because this would amount to "an invasion of his right to exploit his personality by the use of his image, voice or otherwise" (1 O.R. (2d) 225, revg. [1972] 2 O.R. 133, at p. 236). However, on the facts, it was not Krouse's personality but the game of football that was associated with the defendant's product in the advertising campaign and he was therefore not entitled to damages.

⁸ *Privacy Act*, R.S.B.C. 1996, c. 373; *Privacy Act*, C.C.S.M. c. P125; *Privacy Act*, RSS 1978, c. P-24.

⁹ American tort law recognizes a general claim for invasion of privacy.

The tort of appropriation of personality is an interesting example of the way in which law often seeks to protect privacy interests by advancing a property or commercial right. In *Krouse*, the Court of Appeal argued that a professional athlete's personality had commercial potential because of "his ability to attach his endorsement to commercial products or undertakings or to participate otherwise in commercial advertising" (p. 227). Once the interest in personality is framed by commercial imperatives, market interests come to the forefront. For example, Justice Estey in *Krouse* noted:

[E]xposure through the publication of photographs and information is the life-blood of professional sport. Some minor loss of privacy and even some loss of potential for commercial exploitation must be expected to occur as a by-product of the express or implied licence to publicize the institution of the game itself (p. 225).

[and]

The danger of extending the law of torts to cover every such exposure in public not expressly authorized is obvious. Progress in the law is not served by the recognition of a right which, while helpful to some persons or classes of persons, turns out to be unreasonable disruption to the community at large and to the conduct of its commerce. Much of this publicity will in reality be a mixed blessing involving the promotion of the game itself, but at the same time resulting in some minor or theoretical invasion of a player's individual potential for gainful exploitation (p. 236).

I will argue below that commercial imperatives similar to those cited by Justice Estey have significantly shaped the development of fair information practices in the United States, Europe and Canada. At this point, it is important to note that the law seems reluctant to recognize a broad right to privacy independent of some objective measure, such as an interest in property or a commercial value¹⁰.

The inter-relationship between privacy and property is also woven into legal mechanisms designed to constrain the state's power to invade the individual's private sphere. I argue elsewhere that the rule of law, with its inherent restrictions on the state's surveillance powers, was first developed through the establishment of private property rights:

The Magna Carta, for example, is considered to be a seminal document in which the King relinquished absolute power and first subjected his actions to the rule of law. The most oft-quoted paragraph of the Magna Carta reads as follows: 'No freemen shall be taken or imprisoned or disseised or exiled or in any way destroyed, nor will we go upon him nor send upon him, except by the lawful judgment of his peers or by the law of the land.'¹⁰ However, almost all of the remaining sixty-eight paragraphs in the document laid down strict limits on the King's power to seize the Barons'

¹⁰ American jurisprudence is the exception to the rule, and a general right to privacy has been recognized in the United States since the late 1800s (Cooley, 1888, p. 29; Warren & Brandeis, 1890). Dean Prosser argued that the right to privacy in American law encompasses four separate tortious claims: (1) intruding into the plaintiff's seclusion or private affairs; (2) publically disclosing private facts that embarrass the plaintiff; (3) publicity that puts the plaintiff in a false light; and (4) appropriating the plaintiff's image or name (Prosser, 1960).

property. In a feudal society where the Crown owned virtually everything, the protection of private property was a political revolution (Steeves, 1999b, p. 7).

Modern restrictions on police powers typically rely on physical parameters, such as property lines, walls and doors, to carve out an inviolate private space. For example, under s. 488 of the *Criminal Code*, police can only enter private property to execute a search warrant during the day unless there are reasonable grounds to execute the warrant at night; and once the search is completed or the warrant expires, the police must leave the property or become trespassers at common law (*R. v. Moran* (1987), 36 C.C.C. (3d) 225 (Ont. C.A.)).

Some analysts have suggested that expanding the legal conception of privacy to encompass a property right in personal information would best protect privacy interests in a networked environment (Laudon, 1994; Rule & Hunter, 1999). However, as Lawrence Lessig has pointed out, the reliance on property rights and physical barriers to protect privacy in the past has left a latent ambiguity in the law. In his discussion of the development of American constitutional protections for privacy in the late 1700s, Lessig argues that there were three competing theoretical interests at play. Some proponents of Fourth Amendment restrictions on unreasonable search and seizure were intent on preserving human dignity; others sought to protect the private sphere from all but minimal intrusion; and still others wished to ensure that the power of the state to interfere with the individual's freedom would be restricted by law. Hence, there was broad

support for enshrining protections against unreasonable search and seizure in the *Bill of Rights*. However, since physical barriers were sufficient to protect any or all of these interests, legislators failed to articulate which interest was paramount. Lessig concludes that:

Given the technologies of the time, there was no reason to work out which theory underlay the constitutional text: all three were consistent with existing technology. But as the technology has changed, the original context has been challenged. Now that technologies such as the worm can search without disturbing, there is a conflict about what the [constitutional protection against unreasonable search and seizure] protects... And this in turn forces us to choose (Lessig, 1999, p. 149).

The next chapter is devoted to analyzing the types of choices that were made when data protection schemes were first developed. Extending the same analysis to other legal frameworks for privacy would be a fruitful area of study, but it is outside the scope of this thesis¹¹. In general, it is important to remember that the development of constitutional and common law concepts of privacy are steeped in the liberal tradition and, as such, are vulnerable to communitarian

¹¹ Constitutional law dealing with privacy is currently under increased scrutiny, given anti-terrorist measures which were enacted after 9/11. In some ways, the anti-terrorist agenda has rekindled traditional legal discourses about the relationship between privacy and democracy. However, earlier research indicates that anti-terror measures are part of a managerial agenda which predates 9/11. See Steeves (2001) for example. Tort law has been the subject of less scholarly study than other privacy frameworks; a detailed critical analysis would further inform our understanding of the inter-play between privacy and property interests as they have been articulated within a liberal model of law. I intend to pursue these areas in my post-doctoral work.

attack for the same reasons Regan outlines in her discussion of Westin's theory of information privacy¹².

Reasonable expectations of privacy

Judicial discourses are also limited because they typically link protections against surveillance to reasonable expectations of privacy. For example, Canadian courts have held that there is a reasonable expectation of privacy in a hotel room (*R. v. Wong*, [1990] 3 S.C.R. 36 (S.C.C.)) but not in a public washroom (*R. v. LeBeau* (1988), 41 C.C.C. (3d) 163 (Ont. C.A.)). However, as technology continues to change our experiences of privacy, it becomes more difficult to restrict surveillance practices which are in widespread use by members of the public because the use itself means we no longer expect to have privacy.

For example, when the United States Supreme Court considered whether or not thermal imaging (a technology which can take a "picture" of the inside of a dwelling house without physically entering the property) constitutes an unreasonable search and seizure, it decided that the police could not use the technology without a warrant – but the decision was restricted to technology that is "not in general public use" (*Kyllo v. USA*, 99-8508 (USSC 2001))¹³. As an increasing number of people use email, webcams, and phone cameras, and

¹² See Chapter One, pp. 16-17.

¹³ The Supreme Court of Canada came to a similar conclusion in *R. v. Tessling* ([2004] 1 SCJ No. 63). See pp. 63-64 below.

closed circuit video surveillance continues to spread into places previously thought to be private, such as hotel rooms and the washroom stalls in malls, our reasonable expectation of privacy shrinks because the technology gives us no privacy and we all know it (Steeves, 1998; 2002). Accordingly, relying on a distinction between technologies that are not in general public use and those that are may soon mean we have *no* expectation of privacy.

The loss of the expectation of privacy due to the implementation of new technological infrastructures is precisely what motivated the United States Justice Department to subpoena hospital patient records in 2004. The Justice Department wished to determine whether or not patients were given late term abortions for the purposes of enforcing the *Partial Birth Abortion Ban Act of 2003*. Without reasonable grounds to suspect an offence had occurred, they were not in a position to obtain search warrants. However, the Department argued that there is no longer a reasonable expectation of privacy with respect to medical records because of changes in information management driven by new communications technologies. Accordingly, they attempted to compel hospitals to release the records without warrants (O'Connor, 2004). Although the argument was ultimately unsuccessful, it is a good example of the permeability of "reasonable expectations" in a social environment structured by invasive technologies.

There is also some evidence that judicial discourses are being influenced by

data protection principles in ways that limit the court's willingness to engage in traditional privacy discourses of autonomy, freedom and dignity. For example, in *R. v. Plant* ((1993), 84 C.C.C. (3d) 203) when the Supreme Court of Canada upheld a warrantless search of public utility records, the majority decision neglected the social and democratic implications of the practice and instead focussed on the nature of the information collected. Justice Sopinka wrote:

Section 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual (p. 204).

Sopinka concluded that hydro records, however, do not fall into that core as they do not reveal intimate details of the defendant's personal life.

Justice McLachlin disagreed. She argued that:

The records are capable of telling much about one's personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there. The records tell a story about what is happening inside a private dwelling, the most private of places. I think that a reasonable person looking at these facts would conclude that the records should be used only for the purpose for which they were made – the delivery and billing of electricity – and not divulged to strangers without proper legal authorization (p. 213).

Since the *Plant* decision, the Supreme Court has remained reluctant to examine the broader social and political implications of data collection practices. In *Smith v. Attorney General of Canada* ([2001] 3 S.C.R. 902) the Court upheld the federal government's practice of matching data in the Employment Insurance database against the Customs database in an attempt to catch "cheaters" who were travelling outside the country while collecting unemployment benefits. The Privacy Commissioner of Canada argued that this constituted an unreasonable search and seizure because it treated every Canadian traveller like a criminal suspect without reasonable cause, in effect allowing the state to place citizens under surveillance on the off-chance they have committed an offence. In its two-page judgment, the Court did not engage this argument and instead summarily concluded:

... that the appellant cannot be said to have held a reasonable expectation of privacy in relation to the disclosed portion of the E-311 Customs Information which outweighed the Canada Unemployment Insurance Commission's interest in ensuring compliance with self-reporting obligations of the Unemployment Insurance benefit program (pp. 903-904).

Three years later, when the Court considered the constitutionality of Forward Looking Infra-Red (FLIR) images that capture heat escaping from a house (*R. v. Tessling*, [2004] 1 SCJ No. 63), it distinguished between territorial privacy (where the police enter private property to gather information) and informational privacy

(where the police use technology to gather information without physically entering the property under surveillance). The Court held that the defendant had no reasonable expectation of privacy with respect to the use of FLIR technology because, “Everything shown in the FLIR photograph exists on the external surfaces of the building and in that sense it records only information exposed to the public (albeit the public, unaided by technology, cannot in fact observe the heat pattern in the detail FLIR imaging affords)”. Once again, the Court focussed on the piece of information, the manner of its collection, and the efficiency of government programs, rather than the social and political consequences of government surveillance practices.

However, the interaction between data protection legislation and broader judicial discourses regarding autonomy, dignity and social norms is a fluid one.

Common law articulations of privacy are of particular interest because they contextualize the act of surveillance by placing it in the everyday experiences of real social actors. This creates a potential moment in which the social meaning of data collection schemes which comply with fair information principles can be examined and challenged in the courts.

This was the case with Iceland’s national health sector database. In spite of strong criticism from the scientific and medical communities and the general

public¹⁴, the Icelandic government passed the *Health Sector Database Act* in 1998 (Act No. 139/1998). The Act paved the way for the creation of a database containing the genealogical history, genetic information and personal health records of every Icelander. The Act also incorporated data protection principles. For example, Article 5(1) requires that any licencees operating the database must use technical, security and organisational standards that meet the requirements of the Icelandic Data Protection Commission, and Article 7 provides that records, other data and information must be handled in a way that is consistent with conditions deemed necessary by the Data Protection Commission. In addition, Article 8 gives patients the right to “refuse permission, by notification to the Medical Director of Health, for information concerning them to be entered into the Health Sector.”

After the Act was passed, the government sold exclusive rights to use the data to deCode genetics, a bio-technology firm, for a 12 year period. deCode had previously signed an agreement to work with the Swiss-based multinational Hoffman-LaRoche on the development of drugs for 12 genetic diseases, effectively banning others in Iceland from doing research on those diseases. DeCode also planned to sell the information contained in the database to other pharmaceutical and health insurance companies (Hloden, 2000).

¹⁴ See Mannvernd, the Association of Icelanders for Ethics in Science and Medicine, for example at <http://www.mannvernd.is/english/home.html>.

The database has been highly controversial within Iceland, for a number of reasons, including (*ibid*):

- the potential detrimental effect on privacy;
- the use of implied consent for the collection of personal health information;
- the fact that data entered into the database before a patient opts-out of the program is not removed, making that person a research subject without consent of any kind;
- the potential for genetic discrimination; and
- the effect on research of monopolies on access to data.

However, in spite of significant dissent, the Icelandic government has continued to move forward with the program, relying on the provisions of the *Health Sector Database Act* to quell citizens' concerns.

When the issue was adjudicated in the case of *Ragnhildur Guðmundsdóttir v. The State of Iceland* (No. 151/2003), the Icelandic Supreme Court was able to look beyond the narrow meaning of data protection and examine the broader social ramifications of surveillance in this context. The case was brought to court because Guðmundsdóttir had notified the Medical Director of Health that she wished to opt out of the database. She had also provided notice that she did not want her deceased father's information to be collected; given the nature of the information, collection of her father's DNA would reveal a great deal of information about herself as well. Although the government discontinued

collecting her information pursuant to Article 8, the Medial Director continued to add her father's information to the database.

After examining the facts, the Court concluded that, under Article 8, Guðmundsdóttir could not exercise the statutory right to opt out as a substitute acting on behalf of her father. In other words, the data protection principles incorporated into the Act did not provide her with the privacy protection she sought. However, in spite of the limitations of Article 8, the Court held that she did have an interest in barring the transfer of health information about her father to the database “for reasons of personal privacy” (p. 5). They reasoned:

... extensive information is entered into medical records on people's health, their medical treatment, lifestyles, social circumstances, employment and family. They contain, moreover, a detailed identification of the person that the information concerns. Information of this kind can relate to some of the most intimately private affairs of the person concerned, irrespective of whether the information can be seen as derogatory for the person or not. It is unequivocal that the provisions of Paragraph 1 of Article 71 of the Constitution [Act No. 33/1944] apply to information of this kind and that they guarantee protection of privacy in this respect (p. 8).

The case of the Icelandic health sector database is a good example of how constitutional, tortious and criminal law articulations of privacy interests may

operate to focus judicial attention on the social ramifications of surveillance schemes. Although the remainder of this thesis will examine the development of statutory provisions to govern the flow of personal information, judicial discourse remains in the background because it contains a potential moment of social negotiation outside of the narrow interests of special interest groups.

However, the preceding analysis also illustrates that, although privacy was a sustained concern before the 1970s, information-based definitions of privacy have limited the common law's response to traditional and emerging concerns. Cases like *Plant*, *Smith* and *Tessling* demonstrate that the focus on information has weakened the connection between privacy and traditional discourses about autonomy, freedom, and dignity. The next chapter traces the ways in which data protection principles have restructured the legal understanding of privacy by focussing on procedural rules of informational control.

Chapter Three - Data Protection Regimes: A Historical Exposition and Comparative Legal Analysis

When human rights inform the language in which the discussion among you and the general public and Parliament takes place, you speak then, rightfully about citizens and all that comes with that. On the other hand, if the emphasis is primarily on the protection of data ... [then] it is the language of the market that informs your discourse... When those who primarily locate themselves in the human rights climate speak about citizens, about the relationship between groups and power, those who are in the market language speak primarily about stakeholders. And when one speaks about rights and obligations, others speak about binding contracts (Franklin, 1996).

As you know, there are two approaches to privacy: the human rights approach and the data protection approach. We intend to crush the human rights approach (Personal interview with a telecommunications executive in 1999).

The main goal of this chapter is to identify the conceptual core of data protection legislation in several countries, in order to set the stage for the theoretical reflection on the nature of privacy that is undertaken in Chapters Four and Five. As discussed in Chapter Two, data protection laws are based on the set of fair

information practices that Westin first identified in 1967. Some jurisdictions, such as the United States and Germany, expressly adopted Westin's definition of privacy as informational control as well as his set of information practices; others have implicitly done so. Westin's model is therefore central to the current legal framework dealing with privacy.

This chapter provides an in-depth analysis of early data protection legislation from 1970 onward¹, with special emphasis on the motivations which led to the enactment of instruments in Europe and North America. These early instruments are particularly important because they have served as the model for subsequent legislation, including the Canadian *Privacy Act* (R.S.C. 1985, c. P-21) and *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5). This analysis allows us to identify the reasons why data protection principles were adopted in the first instance, and unpack the assumption that data protection gives individuals control over their personal information so they can protect the social meaning of privacy.

As Bennett & Raab (2003) point out, data protection regimes based on fair information practices are operationalized through a variety of methods, including transnational policy instruments, legislation, regulatory agencies, voluntary codes and practices, and technological instruments. I am interested in exploring the

¹ Further details on the specific provisions in the instruments discussed in this chapter can be found in the Appendix.

reasons why data protection was selected by policy makers in response to privacy concerns. I have therefore focussed my analysis primarily on the development of transnational policy instruments and early domestic data protection legislation in Hesse, Sweden, the Council of Europe, the United States, Germany, the Organization for Economic Cooperation and Development and the European Union. I have chosen Hesse, Sweden, the Council of Europe, the United States and Germany because they were the first jurisdictions to adopt data protection legislation. Accordingly, the instruments they produced are the result of the inter-play between competing interests during the formative years of data protection; and, as such, they are social artefacts which concretized negotiated compromises at particular points in time. I have also chosen the Organization for Economic Cooperation and Development and the European Union because a historical analysis of the ways in which these international organizations took up data protection enables one to unpack the interplay between the European conceptualization of data protection and American privacy policy; these two factors have been the dominating influences on data protection legislation as it has diffused throughout more than 40 jurisdictions in Europe, the Americas, Australasia and the Middle East since 1970. I conclude the chapter by comparing and contrasting the European and American experience with the development of data protection laws in Canada.

The similarities and contrasts which are revealed are significant not just from an international comparative point of view, but because they identify the problems

that need to be reflected upon theoretically. I argue that legal responses to privacy concerns from 1970 onward have been constrained by two technical and institutional brakes: the valorization of technology; and managerialism. Both brakes have served to marginalize historical and sociological concerns about privacy by recasting privacy protection as a procedural set of informational rules.

The American experience demonstrates that privacy protection has been limited by the valorization of technology and the privileging of technical innovation. American policy has accordingly prioritized the need to unshackle technology from cumbersome legislative and regulatory mechanisms over the need to protect the social experience of privacy. In Habermasian terms, technology was maintained in an autonomous sphere that was impervious to socio-cultural inputs. The interaction of technology as a steering medium of the systems world on the one hand, and privacy as an organizing principle of the lifeworld on the other hand, is particularly important to a critical understanding of the social value of privacy, because the communicative rationality that arises in the lifeworld can only function if the necessary social conditions are in place to support intersubjectivity. As we will see in Chapter Six, when instrumentalism is allowed to penetrate the dialogic interaction of the lifeworld, to invade privacy *per se*, there are profound consequences for both social interaction and the emergence of identity.

European experience, on the other hand, indicates that policy makers prioritized

modernization and administrative efficiency over public concerns about surveillance. The European interest in managerialism sought to constrain and redefine both historical memory and the sociological meaning of privacy, by privileging discourses based on instrumental logic, routine practices and administrative control. Data protection legislation accordingly took on a pedagogical function; it sought to reconstruct public concerns in ways which were consistent with the managerial imperative, by “educating” the public about the meaning of privacy and privacy remedies. Since the managerial understanding of data protection is decoupled from the social experience of privacy as articulated through communicative interaction in the lifeworld, data protection policy continues to be at odds with public demands for restrictions on surveillance.

The origins of data protection

Most scholarly treatments start with the premise that data protection was enacted in the 1970s and 1980s to protect personal privacy from invasive practices enabled by new technologies. For example, Bennett and Raab write:

In recognition of the power of new information and communication technologies in the hands of large public and private agencies, states and lesser jurisdictions began to pass information privacy, or data protection, statutes. These were designed to give individuals greater control over the information collected about them, and to stem the erosion of personal privacy (Bennett & Raab, 2002, p. 3).

However, closer examination makes it clear that there were a number of competing agendas that came together and formed a consensus in favour of the enactment and implementation of data protection regimes. As Flaherty notes, the presence of these competing interests is not easy to identify. In his 1989 study of the implementation of data protection regimes in Germany, Sweden, France, Canada and the United States, he wrote:

All of the countries studied here had similar problems with invasions of privacy that triggered the enactment of their data protection laws. I have been concerned with understanding just how congruent these problems really were and, relatedly, why similar statutory solutions were sought and enacted. *Identifying the opponents of data protection has not been an easy task, since there has been virtual legislative unanimity in its favor...* (Flaherty, 1989, p. 14, emphasis added).

Flaherty's work accordingly focused on "[trying] to discover the countervailing pressures and the attempts to sidetrack the process" (*ibid*). He concluded that implementation of fair information practices encountered resistance from "entrenched political and bureaucratic centers of power" and that the emergence after enactment of competing interests such as "reducing the costs of government, locating terrorists, or discouraging fraudulent activities in the welfare and taxation systems" have "tempered initial enthusiasms for data protection" (p. 15).

However, I argue that these competing interests were at play *during* the negotiation of data protection legislation and that fair information practices were adopted not in spite of these interests but because of them. Competing and often contradictory interests in human rights², the state's desire to retain sovereignty over its populace and control over its bureaucracy, the bureaucratic search for administrative efficiency, and the facilitation of trade and commerce, came together because the language of fair information practices was ambiguous enough to satisfy the various stakeholders' concerns. These concerns were not mutually reinforcing. Indeed, there was an inherent tension between the managerial interest in access to personal information for the purposes of trade and social control, and the desire to protect the social meaning of privacy as a human right. Typically, legislation was legitimized by appeals to human rights concerns flowing from the European experience of totalitarianism and the desire of individuals to assert control over the collection and use of their personal information. However, as data protection became entrenched, the statutory language used to operationalize that informational control privileged administrative efficiency and trade concerns over the social meaning and experience of privacy.

² Since the human rights conception of privacy is grounded in human dignity and autonomy, it embodies many concerns about privacy as a social value. Clearly there is a well-developed body of theoretical literature on human rights in general and privacy in particular. For example, see Walters (2001). However, given the focus of this thesis, I have chosen to restrict my inquiry to the theoretical foundation of privacy as a social value. Accordingly, my interest in privacy as a human right in this chapter is focussed more on the links between privacy and social relationships and human identity than it is on privacy as an individual legal right.

This chapter examines each of the various competing interests by placing them in historical context. I will demonstrate that privacy concerns which arose in the 1970s were rooted in the social experience of World War II and the threat of post-War totalitarianism. Paradoxically, however, as fair information practices were entrenched in data protection regimes, the law's ability to translate the social meaning of privacy into legal remedies was weakened. The American valorization of technology and the privileging of technical innovation over competing social values helped to decouple technology from the political and social norms (including privacy norms) articulated in the lifeworld. Westin evidences this in *Privacy and Freedom* when he warns that information technologies are creating the "strict records surveillance" that is the hallmark of authoritarian states, and that this "accidental by-product of electronic data processing" is out of keeping with the conscious articulation of American social and political values. However, he concludes, "There is no way to stop computerization. As Professor Robert M. Fano of MIT has remarked, 'You can never stop these things. It is like trying to prevent a river from flowing to the sea. What you have to do is to build dams, to build waterworks, to control the flow'" (Westin, 1967, p. 326).

European managerialism, on the other hand, privileged modernization and administrative efficiency over the social experience of privacy. The continuing conflict between privacy concerns articulated through communicative interaction in the lifeworld and the managerialism of the systems world continued to put

pressure on the law to develop remedies which would account for the social meaning of privacy. Data protection legislation accordingly took on a pedagogical aspect, seeking to “educate” the public about the meaning and nature of privacy problems and solutions in ways that are consistent with managerial imperatives. Accordingly, both dynamics – the American valorization of technology and European managerialism – worked to decouple legal responses from historical memory and the social experience of privacy in the lifeworld.

The legacy of World War II

As noted above, privacy protection took to the legislative stage in most developed countries in the 1970s. However, concerns of the time that new information technologies would place persons at risk of harm were rooted in the events which occurred 25 years earlier. Europeans in particular were sensitive to the ways in which central record keeping had facilitated the identification and exportation of Jewish people during the Nazi occupation of Europe. Accordingly, the promise of faster, more efficient computerized record keeping raised the spectre of mass deportation and oppressive social control (Flaherty, 1979, p. 44; Riley, 2004; Burkert, 2000, p. 60).

In his seminal work on the history of data protection, Flaherty writes:

... the development of computers and data banks [in the 1970s] has aroused elemental anxieties. In England in particular, such sentiments are fuelled by the presence of individuals who have lived under totalitarian

regimes and who fear the potential abuse of data banks by governments or invading forces... [Abuse of population registers] is a common fear in European countries that suffered under Nazi occupation, or were seriously threatened by it ... (Flaherty, 1979, p. 44).

Flaherty recounts how the Nazi-controlled Vichy government used French population censuses in 1940 and 1941 to identify and track Jewish citizens. Pre-existing census data may also have been used to facilitate the deportations that led to the Holocaust. Flaherty quotes historian Robert Paxton:

It appears unlikely that these [pre-existing] census files were a fundamental tool for the deportations [of Jewish French citizens in 1942]. They were not gathered together in one place, and they were not brought up to date for correction of addresses and the like. Xavier Vallat, the Vichy French Commissioner for Jewish Affairs, testified at his trial that the censuses had not served this purpose. But some census data was centralized at the departmental level, and French police certainly had access to it. Furthermore, the German officials drew their estimates of the number of Jews living in occupied France from this data (Paxton, quoted in Flaherty, 1979, p. 45).

Historian A.S. Milward argues that the Norwegian secret police were able to use census data to track people with “unwanted blood,” and some Norwegian authorities believe that this occurred (*ibid*). F. W. Hondius, who lived in Amsterdam during the war, argues that Dutch local population registers first

created in the 19th century provided the Nazis with “a perfect system of population records [that] combined with personal identity cards had facilitated the arrest and deportation of thousands of innocent people by the German occupation forces.” The mandatory identity cards introduced by the Dutch government in 1940 were reviled by the Dutch people, who spontaneously destroyed them at the end of the war (*ibid*).

International human rights instruments

The post-war international community concluded that “disregard and contempt for human rights ... resulted in barbarous acts which have outraged the conscience of mankind” (*Universal Declaration of Human Rights*, Preamble), and came together through the United Nations General Assembly to adopt the *Universal Declaration of Human Rights* (General Assembly resolution 217 A (III)) on December 10, 1948. The Declaration expressly provides for the protection of privacy; Article 12 declares, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Privacy is also indirectly protected through provisions guaranteeing the right to life, liberty and security of person, and freedom of thought, conscience and religion. The right to freedom of religion expressly includes the right to practice a religion or belief in public or private. The Declaration also lays the groundwork

for respect for privacy as a social right tied to the right to the free development of personality³.

When the Council of Europe (COE) first passed the *Convention for the Protection of Human Rights and Fundamental Freedoms* (Rome, 4 XI 1950) in 1950, it incorporated similar privacy rights, subject to such limitations “as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others” (Articles 8 & 9). And when the United Nations adopted the *International Covenant on Civil and Political Rights* (General Assembly resolution 2200A (XXI)) on December 16, 1966, once again protections for privacy were included which mirrored the provisions of *Universal Declaration of Human Rights*.

The language used in these instruments creates a broad legal right to privacy and casts that right as an essential element of human dignity, freedom and the democratic process. As such, legal protections for privacy which flowed from the experiences of World War II recognized privacy as a fundamental human right, and protected it accordingly.

³ The role of privacy in identity formation is explored more fully in Chapter Five.

Early data protection instruments

As Chapter One demonstrates, privacy concerns returned to the forefront of public debate in the late 1960s, when the authors of Regan's aptly-named "literature of alarm" (Regan, 1995, p. 13) raised concerns about new surveillance technologies and the information management powers of database technology. The debate raised the spectre of Big Brother, and many worried that the power of governments to monitor large populations would inexorably erode individual freedom and democratic governance. As Table 1 demonstrates, legislators responded with a flurry of studies and reports, exploring the potential impact of computerized databases on government information practices.

Table 1 – Selected Privacy Studies 1970-1975

1971:

G.B.F. Niblett, ed. *Digital Information and the Privacy Problem*. Informatic Studies No. 2. Paris: OECD.

1972:

B. C. Rowe, ed. *Privacy, Computers and You: Workshop of the Data Bank Society Manchester*.

British Computer Society. *Privacy and the Computer - Steps to Practicality*. London: British Computer Society.

Canada. Department of Communications and Department of Justice. *Privacy and Computers: A Report of the Task Force*. Ottawa.

Great Britain. Home Office. *Report of the Committee on Privacy*. London: Cmnd. 5104.

National Academy of Sciences Project on Computer Databanks. *Databanks in a Free Society*. Washington.

Sweden. Committee on Automated Personal Systems. *Data and Privacy*. Stockholm.

Sweden. Justice Department. *Data and Privacy*. Stockholm: Almanns Foraget.

1973:

United States. Department of Health, Education and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers, and the Rights of Citizens*. Washington, D.C.

1975:

Great Britain. Home Office. *Computers and Privacy*. London: Cmnd. 6353.

The 1973 Report of the United States Department of Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems provides an interesting picture of the times. The Committee notes that:

Most of the advanced industrial nations of Western Europe and North America share concerns about the social impact of computer-based personal data systems... The discussions that have taken place in most of the industrial nations revolve around themes that are familiar to American students of the problem: loss of individuality, loss of control over information, the possibility of linking data bases to create dossiers, rigid decision making by powerful, centralized bureaucracies.

...

Concerns about the effects of computer-based record keeping appear to have deep roots in the public opinion of each country, deeper roots than could exist if the issues were manufactured and merchandised by a coterie of specialists, or reflected only the views of a self-sustaining group of professional Cassandras (United States, 1973, Appendix B).

Accordingly, early interest in privacy legislation on the part of the public, the United Nations and the Council of Europe focussed on socio-democratic issues such as the impact of new technologies on individuality and freedom, and the exercise of bureaucratic or governmental power. These concerns were shared by scholars who were "motivated by a desire to build institutional and cultural barriers against the comprehensive monitoring of private life that appeared –

before the Second World War and later, during the Cold War years – as a necessary condition for the functioning of totalitarian or authoritarian regimes” (Bennett & Raab, 2002, p. 23).

However Bennett argues that, although public worries about growing state intrusiveness and declining government accountability were a necessary condition for the spread of privacy legislation, they alone cannot explain the way that data protection laws have proliferated in the past 30 years. He argues that a “network of policy experts that enjoyed constant communication through informal personal meetings, international organizations, conferences, articles, and books” (Bennett, 1997, p. 227) contributed significantly to the diffusion of data protection legislation to 43 states in Europe, North America, South America, the Middle East and Asia since 1973. (See Table 2). The interaction between these policy experts has resulted in a surprisingly uniform set of practices being adopted in countries with widely varying practices of governance and social rules about privacy.

If privacy is conceived of solely within the human rights perspective, with its emphasis on individual rights and democratic freedoms, then this uniformity is difficult to explain as the same set of rules has been adopted and applied in established democracies, the newly democratizing states of Eastern Europe, and Asian countries with political traditions rooted in authoritarianism. Burkert reports that “even China [is] giving [data protection legislation] a thought by means of an

already very active Hong Kong data protection commissioner” (Burkert, 2000, p. 60).

Table 2 – The Diffusion of Data Protection Legislation by Region
 (Bennett & Raab, 2003, p. 102, updated from 2000 to 2004
 and expanded, reproduced with permission)

	1970s	1980s	1990s ff.
W. Europe	Sweden (1973) W. Germany (1978) Denmark (1978) Austria (1978) France (1978) Norway (1978) Luxembourg (1978)	Iceland (1981) UK (1984) Finland (1987) Ireland (1988) Netherlands (1988)	Portugal (1991) Spain (1992) Switzerland (1992) Belgium (1992) Monaco (1993) Italy (1996) Greece (1997)
East & Central Europe			Slovenia (1990) Hungary (1992) Czech Republic (1992) Russia (1995) Estonia (1996) Lithuania (1996) Poland (1997) Slovak Republic (1998) Latvia (2000) Malta (2001) Romania (2001) Liechtenstein (2002)
Americas	United States (1974)	Canada (1982)	Chile (1999) Argentina (2000)
Australasia		New Zealand (1982) Australia (1988)	
Middle East & Asia		Israel (1981) Japan (1988)	South Korea (1994) Hong Kong (1995) Taiwan (1995) Thailand (1988)
Pending legislation:			
In 1996, Brazil introduced Bill No. 61 dealing with personal register and database structuring in the Senate in 1996.			
In 2001, the Senate of Mexico, 58th Congress, introduced a Bill for a Federal Personal Data Protection Law.			

Bennett & Raab argue that “privacy protection was set on a particular trajectory as a result of some common assumptions about the nature of the information privacy problem... The policy responses that developed – data protection or information privacy statutes – were driven for the most part by a shared understanding among policy elites about the nature of the problem they were facing” (Bennett & Raab, 2003, pp. 18-19). Bennett and Grant argue that, by the 1990s, privacy had become a policy sector that enjoyed “a process of international policy convergence” motivated by “international harmonization efforts, intensive attempts at cross-national learning, as well as the imperatives of increasingly global communications networks” (Bennett & Grant, 1999, pp. 5-6). The remainder of this chapter is concerned with identifying the nature of those imperatives and the assumptions that were brought to the table by policy elites. Table 3 summarizes the findings.

Table 3 – Stated Reasons for Adopting Fair Information Practices 1970 - 1985

	Sweden: sovereignty, legitimization	COE 1st Resolution: personal privacy, political integration	COE 2nd Resolution: personal privacy, political integration, legitimization, efficiency	US: legitimization, efficiency, (trade)	Germany: personal privacy, efficiency	OECD: trade, efficiency, economic integration	EU Convention: economic & political integration
Total FIPs	9	5	7	7	7	8	8
Accountability	✓				✓	✓	✓
Identification of purposes	✓		✓	✓	✓	✓	✓
Knowledge/ Consent		Knowledge only	Knowledge only		✓		
Relevance	✓	✓	✓	✓		✓	✓
Use limitation	✓	✓	✓	✓	✓	✓	
Retention	✓	✓	✓		✓	✓	✓
Accuracy	✓	✓	✓	✓			✓
Security	✓	✓	✓	✓		✓	✓
Openness	✓		✓	✓	✓	✓	✓
Access	✓			✓	✓	✓	✓

Table 3 demonstrates that there was no clustering of certain fair information practices (FIPs) around competing agendas. Rather, the number of FIPs proliferated as human rights concerns about privacy were constrained by both trade interests and managerialism. Ironically, the most complete set of fair information practices were adopted by Sweden in 1973, completely independent of any interest in preserving personal privacy. Early Council of Europe resolutions, rooted in human rights concerns about the effect of surveillance, adopted some FIPs but contextualized them with broad statements of principle and wholesale restrictions on surveillance. However, as the COE's position was restructured by the demands of European integration and administrative efficiency, substantive restrictions on surveillance practices were abandoned in favour of additional procedural rules about information processing. The American emphasis on trade and the autonomy of technology brought about a paradoxical result – by rejecting an administrative approach based on FIPs and leaving more issues to the private sector, American law provided a space for the evaluation of specific surveillance practices on a case by case basis, keeping privacy regulation in the political realm and therefore potentially more sensitive to the social understanding of privacy unfolding in the lifeworld.

The following section is organized chronologically, and examines each instrument in turn. This “long march through the instruments” is necessary in order to unpack the common assumption that fair information practices are designed to ensure that individuals retain control over their personal information

so that they can protect the social meaning of privacy. The chapter concludes by comparing the European and American experience with Canadian attempts to regulate privacy, finally drawing some conclusions about ways in which the policy debate can be reinvigorated by returning to the social elements of privacy contained in Westin's theory.

Hesse Data Protection Act

The West German state of Hesse became the first government to articulate fair information practices when it passed the *Hesse Data Protection Act* (Gesetz und Verordnungsblatt I (1970), 625) on September 30, 1970. Hesse's motivations were quite different than those of the United Nations and the Council of Europe. Burkert (2000, pp. 44-45) argues the law was passed to resolve conflicts between local governments and the state bureaucracy on the one hand, and between the legislature and the executive on the other. Under German constitutional law, state and federal laws are administered by local authorities (footnote 5). State governments were using computers to centralize information gathering and processing powers, and local governments worried that this centralization would in effect transfer the power and influence traditionally held by local authorities to the state bureaucracy. For its part, the state legislature was concerned that data processing would enhance the executive's power, especially if the legislature was cut off from information held in the computers owned and operated by the state bureaucracy (*ibid*).

Although German citizens were beginning to fear the effect computer databases would have on them in general, and their employment in particular, the concern for confidentiality only gradually became an important argument among legislators, and the confidentiality clauses eventually contained in the Act were quite weak. Confidentiality was not required where distribution was permitted by regulation or “if processing was necessary” (*ibid*). Accordingly, the primary motivation behind the Act was to resolve conflicts over the distribution of state and bureaucratic power. Data processing was seen as a tool to enhance power and control; the various levels of government competed for access to the tool to enhance their own effectiveness, and wished to set out basic ground rules to protect administrative turf.

Prior to this time, international instruments had cast privacy as a human right. The Hesse Act, on the other hand, set out a set of procedural rules, ostensibly to create a level playing field for various levels of government vying for access to information processing power. The Act also incorporated rules previously established on a case by case basis through adjudication – the right to access a person’s own record, the right to have errors in the record corrected, and a set of remedies where information is collected unlawfully – and established an ombudsman to respond to citizen complaints and direct the complaints to the appropriate authority.

Burkert concludes that, “While the power conflict part of the Hesse law only

resurfaced occasionally in the legislation of the other states, the confidentiality part of the law set a legislative program into motion” (p. 45). Citizen concerns about confidentiality and privacy clearly remained an important thread as the fabric of that legislative program was woven; however, for our purposes, the Hesse Act demonstrates that the earliest articulation of fair information practices was consistent with bureaucratic and political interests in safeguarding their respective spheres of power. The rights of access and correction were also consistent with the administrative need for data integrity – individual oversight of records safeguarded the data itself and helped ensure that the information used for policymaking and administration was indeed accurate.

Perhaps the most important legacy of the Hesse Act was the negative default rule – information was required to be kept confidential unless disclosure fell within an enumerated exemption. As Burkert argues, “The processing of personal data was seen as interference per se that needed legitimization” (p. 49) by managers. The need to legitimize emerging information practices was also evident in the 1973 report of the United States Department of Health, Education and Welfare Secretary’s Advisory Committee on Automated Personal Data Systems. The Committee noted that, “Even though there is little evidence that any of these adverse social effects of computer-based record keeping have occurred on a noticeable scale, they have been discussed seriously since the late sixties, and the discussions have prompted official action by many governments as well as by international organizations”. The Committee

continued:

The fragility of computer-based systems may account for some of the concern... The active opposition of even a few percent of those whom a system means to serve can cripple the powerful, but fragile, mechanism of a highly automated system. Nor is it necessary for this opposition to be manifested in physical sabotage of the computer itself (although that has happened); it is merely enough to withhold cooperation... Thus, the very vulnerability of automated personal data systems, systems without which no modern society could function, may make careful attention to the human element transcend national boundaries (United States, 1973, Appendix B).

The Committee's comments highlight a number of interesting dynamics. First, concerns about potential privacy invasions articulated by citizens in the lifeworld (although discounted due to a lack of evidence) were clearly perceived by the bureaucracy as creating pressure on governments to legislate controls over data processing. Second, automated personal data systems were seen as absolutely essential to the workings of a modern state; they were not optional. As Flaherty notes, the bureaucratic faith in the efficacy of automated data processing systems is endemic in government:

... aspiring civil servants seek data on individuals to design and evaluate programs, to augment their prestige and power, and, as a product of a supposed technological imperative, to enable them to use the latest

hardware and software programs. Bureaucrats are thus a major source of government initiatives for information collection, because of the standard delusion that more data will solve problems. (Flaherty, 1989, pp. 13-14)

Third, the benefits of computerization could be lost unless the public accepted and cooperated with new information systems.

The need to construct trust in both public sector and private sector information systems is a theme which has recurred throughout the 30 years following the Hesse Act as various states introduced data protection legislation. The managerial pursuit of efficiency and control have been facilitated by the adoption of information practices that enable administrators to collect and process vast amounts of personal information. However, both the technologies and the practices they enable have met with continuing resistance in the public sphere, as they come up against socially grounded concerns about surveillance and its effect on human dignity, autonomy and freedom. Data protection legislation has therefore continued to play a pedagogical role, reconstructing public concerns about privacy as the need for greater control over personal information.

Swedish Data Act

When Sweden became the first national government to pass data protection legislation in 1973, it was both the most computerized country⁴ (Burkert, 2000, p.

⁴ On a per capita basis.

48) and the country with the most routine surveillance in Europe (Flaherty, 1989, p. 98). Since 1947, every Swedish citizen has been assigned a Personal Identification Number (PIN) that is used to identify him or her throughout his or her lifetime. Personal information, including PINs, is freely available due to a tradition of openness, mostly notably embodied in the Swedish *Freedom of the Press Act* (1949)⁵. The national population register includes every citizen and resident's name, PIN, address, parents' names, marital status, and nationality; and personal information contained in the Register is distributed to government departments, to the Church of Sweden, and to corporations and organizations through the Swedish Population and Address Register (SPAR). SPAR also collects and distributes information on an individual's taxable income and the extent of his or her real estate holdings. In addition to making information available to corporations through SPAR, the public sector participates in "liberal exchanges of data" with the private sector (*ibid*).

Flaherty calls Sweden "the model surveillance society in the Western world, because of its high degree of automation, the pervasiveness of Personal Identification Numbers (PINs) to facilitate record linkages, and the extent of data transfers between the public and private sectors" (p. 4). Jan Freese, former director-general of the Swedish Data Inspection Board, calls Sweden a "paradise" for data banks (Freese, 1987, p. 108). Flaherty concludes that

⁵ The *Freedom of the Press Act* is part of the Swedish constitution.

“Sweden illustrates the kind of surveillance society that results when record linkages are so easy to accomplish that the power holders cannot resist using them to try to solve real and alleged social problems.” (Flaherty, 1989, p. 94)

Data protection laws were first proposed in the 1972 report of the Parliamentary Commission on Publicity and Secrecy of Official Documents. Citizen concerns about the automation of the 1970 census data had raised questions about personal privacy; however, the government’s interest in data protection was rooted in the desire to protect Sweden’s national sovereignty against the possibility of automated registers falling into the hands of a foreign power (Riley, 2004; Burkert, 2000, p. 48). A later study, published in 1976 by the Swedish Ministry of Defence, summarizes the concerns well:

A possible aggressor, who is trying to gain effective and complete control of the population when engaged in acts of war on Swedish territory, may find it necessary to have access to population registers. This assumption is confirmed by experience from the Second World War ... Today, Sweden has ten or so computerized central population registers. In most cases these registers contain very detailed information which would be extremely valuable for a possible aggressor aiming to establish control of Swedish territory. (Sweden, 1976, p. 9).

When the *Data Act* (Sweden, 1973) was passed on July 1, 1973, it created a licensing and registration system administered by the Data Inspection Board

(DIB)⁶. Under the Act, any public or private sector organization wishing to create a personal file, defined as “any file, list or other notes kept by automatic data processing and containing personal data referable to the individual concerned” (s. 1), must apply to the DIB for a licence to do so. Accordingly, the Act only applies to automated data processing, and does not extend to paper records.

Privacy advocate Jan Freese argued that central registration and licencing would enable citizens to see how much data processing was in fact occurring (Freese, 1981, p. 8). However, when the Act was amended in 1979 and 1982, there was a “fundamental retreat” from licencing, in favour of a simple registration system (Flaherty, 1989, p. 95), except for databases containing sensitive data⁷.

Section 3 of the Act provides that the DIB shall grant permission to a public or private sector organization to set up and keep a personal file “if there is no reason to assume that ... undue encroachment upon the privacy of registered persons will occur”. The section then enumerates the factors to be taken into account in judging what constitutes undue encroachment. Special attention is to be paid “to the nature and quantity of the personal data to be recorded in the file,

⁶ The DIB is an independent government agency. Members of its Board of Directors are appointed for four year terms, and are chosen to represent the political parties in the Swedish legislature, the major labour unions, industry, and the public administration.

⁷ Under s. 4, sensitive data includes information about a person’s criminal record, health, psychiatric treatment, receipt of social welfare benefits, political beliefs, and religious beliefs. Amendments in 1982 added sexual history and race to the list.

to how and from whom the data are to be collected, and *to the attitude to the file held, or which may be assumed to be held by, the persons who may be registered*" (emphasis added).

Although the section purports to limit the creation of invasive databases, it is important to remember that the restriction is contextualized by both actual and assumed attitudes about the value of data registers. The Swedish bureaucracy has consistently assumed surveillance is consistent with good government and citizen expectations. The National Tax Board (NTB), for example, collects a great deal of personal information from Swedish citizens. Gert Persson reports that a senior official of the NTB stated that, "coming under surveillance is a privilege" (Persson, 1986, p. 4); and a NTB brochure on the benefits of the National Population Register states that, "the population should themselves feel that there is a good reason for being recorded in the population registration system. They should feel that such registration simplifies life for them and is an efficient support in achieving a correct distribution of social rights and obligations" (Sweden, 2003).

Moreover, by 1970 the Swedish people had already accepted a high level of surveillance from both the public and the private sectors. Much of the tolerance for surveillance in Sweden reflects the fact that it is a highly managed society. Since the paternalistic Swedish state is perceived by citizens to be trustworthy, citizens are less worried about invasion when privacy conflicts with surveillance

initiatives put in place by the government (Flaherty, 1989, pp. 98-99).

Data protection in Sweden was accordingly seen as a way to protect national sovereignty, to maintain the flow of information to the public and private sectors, and quell citizen concerns about the automation of census data. It is noteworthy that Sweden chose to enact nine of the ten fair information practices listed on pp. 42-43 above to meet these goals.

**Table 4 –
Swedish Data Act**

1. Accountability	✓
2. Identify purpose	✓
3. Knowledge & consent	–
4. Limit collection to purpose	✓
5. Limit use to purpose	✓
6. Retain only as long as necessary	✓
7. Accurate	✓
8. Secure	✓
9. Open (no secret systems)	✓
10. Access & correction	✓

Council of Europe Resolution regarding private sector databases

On September 26, 1973, two months after Sweden passed its *Data Act*, the Council of Europe passed a *Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector* (COE Resolution (73) 22). The Resolution was the result of two concerns. First, a COE Committee of Experts on Human Rights had surveyed European human rights legislation in 1968-1970, and concluded that “existing law does not provide sufficient protection for the citizen against intrusions on privacy by technical devices” as it is limited to narrow interests such as privacy of correspondence or

property rights⁸. International documents, including the European *Convention for the Protection of Human Rights and Fundamental Freedoms*, were not sufficient to remedy this gap, because they only apply to public authorities and do nothing to restrict intrusive behaviour on the part of private organizations (COE Resolution (73) 22, Explanatory Report, para. 2). Second, the COE was created in part “to achieve a greater unity between its member States” (COE Resolution (73) 22, Preamble). Since legislation was required to protect individuals from abuses enabled by electronic databanks, the COE felt it was “urgent, pending the possible elaboration of an international agreement, at once to take steps to prevent further divergences between the laws of member States in this field” (*ibid*).

The COE adopted five of the ten FIPs. However, the practices included in the Resolution are contextualized by broader statements of principle rooted in the COE’s commitment to human rights. For example, there is an explicit concern with the potential for discrimination. Paragraph 1 of the Annex reads, “In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.” Examples of potentially discriminatory data include

⁸ This is consistent with the analysis presented in Chapter Three.

criminal records and health records (COE Resolution (73) 22, Explanatory Report, para. 19).

Both criminal records and health data are defined as sensitive data in s. 4 of the Swedish *Data Act*.

However, the Swedish law is silent with respect to discrimination, and only requires that the data

collector obtain a licence before collecting

sensitive data. The COE Resolution states that in

general this data should not be collected at all; and where it is necessary to

collect it, it should not be disclosed because of the inherent risk that the

disclosure of this information will lead to discrimination.

Moreover, although the Resolution does not forbid the collection of information for harmful purposes, the Explanatory Report makes it clear that the COE failed to do so because of the international nature of the document itself: “However, it is not appropriate to lay down in an international instrument criteria as to what purposes should be permissible. In general, a consequence of the freedom of the individual is that any purpose is allowed save when explicitly forbidden” (COE Resolution (73) 22, Explanatory Report, para. 20). The implication is that individual states have the power to expressly restrict the collection of data for certain purposes.

The ability to restrict purposes is consistent with the COE’s statement that “it

Table 5 – COE Private Sector Resolution

1. Accountability	–
2. Identify purpose	–
3. Knowledge only (no consent)	–
4. Limit collection to purpose	✓
5. Limit use to purpose	✓
6. Retain only as long as necessary	✓
7. Accurate	✓
8. Secure	✓
9. Open	–
10. Access & correction	–

seems advisable to adopt a rule which would halt unbridled hoarding of data” (*Ibid*, para. 21), particularly given the potential for data matching (*Ibid*, para. 37). Although the Resolution makes it clear that, “governments should take care that the introduction of new rules on electronic data processing should not have a side effect that modernisation of administration becomes more difficult” (*Ibid*, para. 9), there is an express desire to limit the wholesale collection and use of personally identifiable data. For example, paragraph 10 of the Annex to the Resolution states that, “Statistical data should be released only in aggregate form and in such a way that is it impossible to link the information to a particular person”. Paragraph 37 of the Explanatory Report elaborates that this restriction is “owing to the special facility of computers to trace correlations”. Accordingly, even though “[o]ne of the main purposes of the data bank is to provide managers with statistical information, which will enable them to make executive decisions,” managerial practices which “create certain dangers to privacy” should be curtailed (COE Resolution (73) 22, Explanatory Report, para. 37).

The COE’s primary interest in filling the gap in the law to restrict the negative effects of surveillance technologies is bracketed by competing interests in political integration and administrative modernization. However, the Resolution subordinates managerial imperatives to collect large amounts of information and to use that information to manage risk and effect social control to the need to protect privacy. Instrumental technologies are, as such, not rejected out of hand, but are constrained by the social concerns of the lifeworld. The Resolution

accordingly contains fewer technical rules to govern information management and instead seeks to encourage the establishment of broad restrictions on information collection and domestic political control over the purposes for which surveillance is initiated.

Council of Europe Resolution regarding public sector databases

One year later, the COE's interest in protecting privacy in the lifeworld began to give way to the imperatives of European unification and administrative efficiency. On September 20, 1974, it passed its *Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector* (Resolution (74) 29). The Preamble to the Resolution does not discuss the prevention of abuses in order to protect individuals, as did the earlier Resolution on private sector databases. Instead, it makes it clear that the Resolution is intended to promote greater unity between member states by contributing to "public understanding and confidence with regard to new administrative techniques which public authorities in the member states are using in order to ensure the optimal performance of the tasks entrusted to them" (Resolution (74) 29, Preamble).

The "problems" the Resolution seeks to resolve are no longer grounded in historical memory or social experience; instead they reflect the "increasing concern about the protection of the privacy of individuals" which have arisen because of new technologies (*ibid*). Moreover, the Explanatory Memorandum

that accompanies the Resolution makes it clear that it is public anxiety and not bureaucratic abuses which the COE seeks to allay:

Public anxiety has arisen not because many abuses of information technology have actually been discovered but rather from the possibility of abuse ... the public is not sufficiently informed about the new information technology ... In the absence of general rules and of a proper information of the public, the discussion is apt to flare up on the occasion of each new project for the use of information technology. In this connection, it should be kept in mind that the success with which computers can be used in public affairs will depend very much on the degree of confidence the public is willing to give to their use (COE Resolution (74) 29, Explanatory Memorandum, para. 5).

The Resolution accordingly takes on a pedagogical role, and seeks to allay public concerns by “sufficiently informing” them about new technologies in order to manufacture public trust in emerging administrative practices. The tool of preference is a set of “general rules” focussing on procedural issues; accordingly, the Resolution adopts two more FIPs.

Table 6 – COE Public Sector Resolution

1. Accountability	–
2. Identify purpose	✓
3. Knowledge only (no consent)	–
4. Limit collection to purpose	✓
5. Limit use to purpose (no consent)	✓
6. Retain only as long as necessary	✓
7. Accurate	✓
8. Secure	✓
9. Open	✓
10. Access & correction	–

These general rules are clearly a part of the managerial agenda. The Resolution

expressly promotes the use of electronic data processing because it is “an efficient and powerful instrument” capable of solving “complex social problems” which has “in certain fields ... already become virtually indispensable” (*ibid*, para. 2). The Preamble is intended to reaffirm “that the use of computers for purposes of public administration should in general be regarded as a positive development. The purpose of the present resolution is not to oppose such use but to reinforce it with certain guarantees” (*ibid*, para. 9). These guarantees will expressly contribute to the public’s willingness to accept data practices which promise to “rationalize administrative work,” raise “administrative productivity,” and enable “several administrations, at different levels (central, regional, local) to pool their data” (*ibid*, para. 2). Accordingly, the COE expressly incorporates FIPs to legitimize the electronic collection and use of personal information by government bureaucracies in order to promote efficiency and continental integration through “mutual administrative assistance” based on the “growing importance” of the exchange of information between European states. The pedagogical function of the Resolution is demonstrated by the attempt to thematize public concerns about privacy in such a way that enables information collectors to socially manage the introduction of new technologies. The COE is also the first legislative body to create an exception to data protection rules, in effect carving out certain types of information use for unregulated collection and use; the Resolution expressly states that FIPs do not apply to information used for statistical, scientific or historical purposes, thus freeing up data for instrumental uses.

At the same time that the Resolution seeks to embed managerial principles of efficiency, proceduralism and control into privacy legislation, it moves away from general restrictions on surveillance that resonate with the concerns articulated in the lifeworld about the ways in which new technologies are being used to invade privacy. There is no general provision restricting the collection of potentially discriminatory data; instead, paragraph 3 provides that, “especially when electronic data banks process [such] information”, certain FIPs apply. The Explanatory Memorandum states that data must be accurate, as “errors can cause considerable damage to the individuals particularly when a decision unfavourable to him is taken on the basis of wrong or obsolete information” (COE Resolution (74) 29, Explanatory Memorandum, para. 16); however, it also states that the requirement that data be accurate and up to date “aims at the proper management of computerised data” and that “the authority in charge of the data system has a professional interest in maintaining the good quality of the information that it is keeping” (*ibid*, para. 17).

Accordingly, by 1974, the European legislative response to privacy concerns was restructuring in order to accommodate managerial interests. The COE retreated from broad restrictions which spoke to the deep historical memory of the excesses of totalitarianism, and instead recast legislation as a way of legitimizing bureaucratic information practices.

American Privacy Act of 1973

On December 31, 1974, shortly after the second COE Resolution, the United States enacted the *Privacy Act of 1974* (5 U.S.C. § 552a). Although several congressional committees had examined privacy issues since the House of Representatives Special Subcommittee on Invasion of Privacy first met in 1965, the Act was especially influenced by the Report of the Secretary's Advisory Committee on Automated Data Systems (Bushkin & Schaen, 1975). The Report (United States, 1973) was commissioned by one of the largest public sector data holders in the United States, the Department of Health, Education and Welfare. The Report is an unusual document in the sense that it uses data protection language to probe the social relationships between individuals and record-keeping organizations. The fit is an awkward one.

For example, the Committee argued that privacy is “essential to our well-being – physically, psychologically, socially, and morally” (United States, 1973, Section III), and sought to understand “changes in American society which may result from using computers to keep records about people” (*ibid*, Preface). In this sense, it addressed itself to questions about the social consequences of automated record-keeping systems. Moreover, it concluded that existing constitutional and civil protections for privacy were inadequate because the courts had not been aggressive enough in protecting privacy:

There is little evidence ... that court decisions will, either by invoking Constitutional rights or defining common law principles, evolve general

rules, framed in terms of a legal concept of personal privacy, that will protect individuals against the potential adverse effects of personal-data record-keeping practices. Indeed, there are many court decisions in which seemingly meritorious claims that could have been sustained by recognizing a right of privacy were denied because the courts would not permit such a right to override other legal considerations (*ibid*, Section III).

However, it concluded that “dictionary definitions” of privacy as “seclusion, secrecy, and withdrawal from public view” are inappropriate when examining the relationships between individuals and record-keeping organizations because, “They all denote a quality that is not inherent in most record-keeping systems” (*ibid*). Records, by their nature, are often public and therefore are neither secluded nor secret. Even when records are not public, they are created for “purposes that would be defeated if the data they contain were treated as absolutely secluded, secret, or private” (*ibid*). Accordingly, the Committee sought to “formulate a concept of privacy that is consistent with records”; to do that, they adopted Westin’s 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” (*ibid*).

The Committee argues that Westin’s definition is significant because it recognizes that at least some personal data will be disclosed: “An important recognition is that privacy, at least as applied to record-keeping practices, is not

inconsistent with disclosure, and thus with use”. However, it is limited because it gives the data subject a “unilateral role in deciding the nature and extent of his self-disclosure”. Since “records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals” (*ibid*), individuals must give up unilateral control over the record; in exchange, the record-keeper should agree to abide by a set of FIPs (including knowledge, limiting use to the stated purpose, accuracy, security and access and correction).

The Committee’s discussion is an interesting one, because it implicitly recognizes the sociality inherent in Westin’s understanding of privacy. This dynamic will be more fully explored in Chapter Three. For the purposes of the current discussion, it is interesting that the Committee explicitly acknowledged the fact that Westin’s formulation is consistent with the record-keeping organization’s need to collect and use personal information, and, when the *Privacy Act of 1974* was drafted, all of the Committee’s recommendations were incorporated into the legislation.

Unlike the COE Resolutions, the *Privacy Act of 1974* applies to electronic and non-electronic personal record systems. It is limited to record systems maintained by federal agencies and, as such, does not extend to the private sector. The Act contains seven FIPs, including a provision that the agency cannot disclose information for “other than a routine purpose” without the

individual's consent (FIP No. 5). However, there is a long list of exceptions to this rule. For example, there is no duty to inform the individual when information is disclosed to: the Bureau of Census (s. (b)(4)); the National Archives and Records Administration (s. (b)(6)); any American agency for "for a civil or criminal law enforcement activity" (s. (b)(7)); or the House of Congress (s. (b)(9)). The use of exceptions (first introduced by the Council of Europe) becomes a commonplace of data protection legislation after 1974, especially regarding the application of Westin's "controlling principle for information flow in a data-stream society" (Westin, 1967, p. 375), consent. These exceptions enable legislators to claim to be sensitive to the demands for privacy arising in the lifeworld without limiting managerial or technocratic access to data⁹ by circumventing or negating social demands for privacy.

Table 7 – US Privacy Act

1. Accountability	–
2. Identify purpose	✓
3. Knowledge & consent	–
4. Limit collection to purpose	✓
5. Limit use to purpose	✓
6. Retain only as long as necessary	–
7. Accurate	✓
8. Secure	✓
9. Open (no secret systems)	✓
10. Access & correction	✓

Although both American and European legislation incorporate FIPs, the American approach to privacy differs significantly from that of the Europeans. Traditionally, scholars argue that Americans perceive data protection primarily as a trade issue and have accordingly resisted any legislative restrictions on the

⁹ This is typical of Canadian health privacy laws, for example, which are promoted as protecting the privacy of Canadian's personal health information while giving prescribed "custodians" unrestricted access to health records. (See for example the *Ontario Health Information Protection Act, 2003* (LAO Bill 31, 2003)).

collection, use and disclosure of personal information by the private sector. For example, Eger (1978) and Bigelow (1979) argue that, from early on, the US saw European data protection legislation a form of trade protectionism and that, for their part, Europeans saw the American reluctance to regulate private sector flows of information as a way to maintain American economic hegemony. This discourse has been a central element in the negotiation of privacy rules at the international level (as discussed below), and concessions have consistently been made in favour of economic integration. As Burkert writes:

Right from the outset, the concept of data protection in Europe was not merely a European affair. American international companies and their subsidiaries, even if they regarded themselves to be European companies, conveyed the American view on regulation and on privacy regulation in particular. European companies could point to those companies and issue warnings about their own international competitiveness (Burkert, 2000, 65-66).

However, one of the main differences between the American and European approaches is that Americans are motivated less by managerialism than the desire to free technical innovation and trade from cumbersome regulatory mechanisms. For example, unlike the majority of European countries that have passed data protection legislation since 1973, the United States chose not to

establish a supervisory authority¹⁰ for privacy matters (Bennett & Raab, 2003, p. 106-107). The Secretary's Advisory Committee on Automated Data Systems expressly rejected the idea of a centralized, independent federal privacy agency, to avoid impeding innovation in information management technologies:

The number and variety of institutions using automated personal data systems is enormous. Systems themselves vary greatly in purpose, complexity, scope of application, and administrative context... We doubt that the need exists or that the necessary public support could be marshalled at the present time for an agency of the scale and pervasiveness required to regulate all automated personal data systems. Such regulation or licensing, moreover, would be extremely complicated, costly, and might uselessly impede desirable applications of computers to record keeping (United States, 1973, Section III).

This privileging of innovation is closely linked to the American trade agenda, in which restrictions on the flow of information are seen as unnecessary brakes on the diffusion of technology into consumer society.

A second difference in the American reliance on "pinpointed, detailed legislation to protect informational privacy" (Flaherty, 1979, p. 24) rather than a general legislative framework governing information practices. The first American

¹⁰ Instead, the *Privacy Act of 1974* requires that each agency establish an internal Data Integrity Board to oversee data matching (s. (u)) and the Office of Management and Budget is mandated with the task of prescribing guidelines and regulations under the Act.

legislative response to privacy questions arising in the 1960s was the *Fair Credit Reporting Act* (15 U.S.C. § 1681 et seq) which was passed in 1970. As Flaherty (pp. 307-308) reports, it was followed by:

- the *Family Educational Rights and Privacy Act* (20 U.S.C. § 1232.) in 1974 (restricting government access to and use of personal education records and providing individuals with a right of access)
- the *Right to Financial Privacy Act* (12 U.S.C. § 3401) in 1978 (regulating public sector access to private sector financial records)
- the *Privacy Protection Act* (42 U.S.C. § 2000aa et seq) in 1980 (restricting government searches of newspaper corporations)
- the *Debt Collection Act* (18 U.S.C. § 2415(i); 31 U.S.C. § 3701, 3711(f), 3716-3719) in 1982 (dealing with the release of public information on bad debts to credit agencies)
- the *Cable Communications Policy Act* (PL 98-549) in 1984 (providing privacy protections for cable television subscribers)
- the *Electronic Communications Privacy Act* (18 U.S.C. § 2510) in 1986 (banning the interception of some electronic communications), and
- the *Video Privacy Protection Act* (18 U.S.C. § 2710) in 1988 (restricting access to video rental records).

Passing targeted legislation in response to specific invasive practices that drew heavy criticism from public interest groups and the public at large provided a mechanism whereby the social experiences of invasion could potentially be

translated into legal restrictions on surveillance. Legislative scrutiny of many information privacy issues in the United States continued in the 1990s and early 2000s¹¹; it is noteworthy that 50 privacy bills were introduced or debated in Congress in 2003 alone¹².

The success of each of these legislative attempts to restrict invasion has been mixed, and some acts have been watered down or gutted by private sector lobbying¹³. In addition, in the absence of specific legislation, the private sector is left largely to itself. Corporations are expected to be self-regulating and to develop mechanisms to ensure they comply with any applicable industry Codes or standards. American privacy advocates continue to call for omnibus legislation along European lines¹⁴.

¹¹ See, for example, the *Driver's Privacy Protection Act* (18 U.S.C. § 2721) in 1994 (regulating the release of motor vehicle registration information to the private sector), the *Children's Online Privacy Protection Act* (15 U.S.C. §§ 6501-6506) in 1998 (setting out rules to govern the online collection of children's personal information), and the *Health Insurance Portability and Accountability Act* (PL 104-191) in 1996 (dealing with electronic transfers of health information to private sector insurers).

¹² For example, see the *Stop Taking Our Health Privacy (STOHP) Act of 2003* (H.R.1709.IH), *Defense of Privacy Act* (H.R.338.IH), *Consumer Privacy Protection Act of 2003* (H.R.1636.IH), *Video Programming Consumer Privacy Protection Act of 2003* (H.R.3511.IH), *Personal Data Offshoring Protection Act of 2004* (H.R.4366.IH), *Wireless 411 Privacy Act* (S.1973.IS; H.R.3558.IH), *Library, Bookseller, and Personal Records Privacy Act* (S.1507.IS), *Video Voyeurism Prevention Act of 2003* (S.1301.RS) and *Wireless Telephone Spam Protection Act* (H.R.122.IH).

¹³ For example, in his discussion of health privacy reform in the United States, Gellman (1999) argues that lobbying on the part of health insurers and private health care companies has brought about a system that protects everyone but the patient, and that the provisions of the *Health Insurance Portability and Accountability Act* were watered down to avoid constraining the ability to link patient records with other data.

¹⁴ See the Electronic Privacy Information Center, for example at www.epic.org.

However, the American rejection of a comprehensive regulatory framework has paradoxically kept privacy issues in the political arena, subject to public scrutiny and sensitive to public opinion. For example, the *US PATRIOT Act* cedes extensive surveillance powers to the state to facilitate terrorism investigations, including a power to access library patron records. Librarians are also forbidden from giving patrons notice in the event federal agents obtain their records. The American Library Association has publically condemned the law, and a number of libraries across the country are practising direct action to resist the law. For example, public libraries in Boulder are retaining only the minimum of information on patrons and erasing borrowing records as soon as books are returned, and libraries in California and Illinois are shredding records daily (Cada, 2003). Continuing public scrutiny of surveillance practices provides a potential moment in which the communicative interaction in the lifeworld can resist the imperatives of instrumentalism and generate law that protects the social experience of privacy. As Emily Sheketoff, executive director of the Washington office of the ALA notes, "We've been working on legislation to limit access to library records since before the *PATRIOT Act* passed... Right after Sept. 11 [2001], lawmakers didn't even want to talk to us because if they did their patriotism was questioned. *Now their constituencies, by pursuing this issue, have given them permission to look at legal remedies*" (*ibid*, emphasis added).

German Federal Data Protection Law

The gap between data protection principles and a socially based understanding

of privacy is perhaps most interestingly illustrated in Germany, with its deep historical memory of Naziism and Communism. Flaherty (1989, p. 24-25) argues that Germany's historical experience created two contradictory social imperatives: the desire to restrict state surveillance and protect individual autonomy; and the quest for order. He concludes that the interaction between these two dynamics has brought about a highly legalistic data protection regime that is bracketed by constitutional guarantees for human dignity and the free development of personality.

Germany's data protection regime was also heavily influenced by Westin's understanding of privacy as informational control. When the federal government began to consider data protection after a number of German states followed Hesse's example and legislated in their respective jurisdictions, it called upon a group of experts at the University of Regensburg to develop potential legislative models. Burkert (2000, p. 49) recalls that their ongoing work in the field was heavily influenced by American writers, especially Westin and Miller; and it was a member of the original research team who first coined the phrase "informational self-determination".

The Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Law) was passed on January 27, 1977. Under the Law, public data holders are accountable to the Federal Commissioner for Data Protection (ss. 24, 37), who has both investigatory and advisory powers. The

Law incorporates seven FIPs, and was the first act to provide that personal information should only be collected with the individual's consent. However, once again, legislators relied upon exceptions to carve out significant areas where consent is not required and where use for secondary purposes is allowed.

1. Accountability	✓
2. Identify purpose	✓
3. Knowledge & consent	✓
4. Limit collection to purpose	–
5. Limit use to purpose	✓
6. Retain only as long as necessary	✓
7. Accurate	–
8. Secure	✓
9. Open	–
10. Access & correction	✓

The Law was passed after five years of public hearings and consultations, and was supported by all political parties in the legislature. At first blush, the Law may appear to exemplify what Bennett and Raab call the emergence of a “strong consensus on what it means for the responsible organization to pursue fair information practices responsibly” (Bennett & Raab, 2003, p. 19). However, determining the meaning of the Law’s provisions has been a source of controversy and contention. As Flaherty writes, “Although the general inspiration for the development of data protection laws is apparent, the goals are rarely spelled out in satisfactory detail” (Flaherty, 1989, p. 30), and the specific provisions of each act have been subject to a number of inconsistent interpretations by stakeholders.

For example, s. 1 of the original 1977 *Federal Data Protection Law* provides that, “The purpose of data protection is to ensure against misuse of personal data during storage, communication, modification and erasure and thereby to prevent

harm to any personal interests that warrant protection.” Spiro Simitis, former Data Protection Commissioner for Hesse, took this to mean that the purpose of the law is “to protect the personal interests of the individuals affected by the storage and retrieval of their data and thus to ensure the free development of their personality” (Simitis, 1987, p. 700, quoted in Flaherty, 1989, p. 31). For Hans Peter Bull, the first Federal Commissioner for Data Protection, the Law was “a kind of human rights protection in a technological society” (Bull, 1981, p. 1, quoted in Flaherty, 1989, p. 31). These interpretations are based in a recognition of the sociality of privacy and the essential role that privacy plays in healthy identity formation in the lifeworld. On the other hand, federal bureaucrat H. Auernhammer argued that the Law is intended to regulate the “input of data into a data processing system, their processing, their transmission and their alteration and obliteration while inside the system” and as such, the “right to process personal data ... is related to the practical task to be performed with the aid of data processing” (COE, 1983, p. 32, quoted in Flaherty, 1989, p. 31). Bull’s successor, Dr. R. Baumann, felt the Law was intended to both “[protect] people from excessive probing by the State” and “to help the maintenance of administrative efficiency and of even increasing it through the use of computer systems” (Baumann, 1984, p. 6, quoted in Flaherty, 1989, p. 31).

In his detailed study of the German Law, Flaherty concluded that, “The vagueness and imprecision of the law’s language results in frequent differences of opinion” (Flaherty, 1989, p. 32), and noted that a group of German experts felt

“it would be impolitic and counterproductive to attempt to spell out the goals of data protection in detail” (p. 30). The differences of opinion, however, are telling: the German experience indicates that fair information practices are rooted in a number of conflicting agendas, including the desire to protect the social meaning of privacy, the technological imperative and the managerial search for administrative efficiency. These agendas are not reinforcing. When the social experience of privacy seeks to restrict the autonomy of technology and instrumentalism, data protection privileges the managerial perspective and constrains the ability of data protection commissioners to translate the social meaning of privacy in the lifeworld into policy. This is clearly illustrated by the German reaction to the national census in the 1980s.

When the federal government first called for a census in 1983, six years after the *Federal Data Protection Law* was passed, the proposal led to “enormous public controversies”. One opinion poll revealed that 25 per cent of the 25 million eligible households would refuse to complete the form and 52 per cent of the population did not trust the census questions (Flaherty, 1989, p. 79). In spite of his own concerns about the intended use of census data to correct population registers, the Federal Commissioner for Data Protection Hans Peter Bull issued a press release stating that citizen fears were unfounded as census data would be adequately protected by the data protection rules contained in the Law. The federal legislature unanimously passed a special law in favour of the census, and the special census law was supported by the major German data protection

commissioners (p. 81). Once again, data protection sought to restructure public concerns about privacy and quell social demands by claiming that set of procedural rules and practices provide adequate protection.

However, public anxieties about the census were profound, and generated vigorous public debate about the broader issues of government surveillance and the role of technology in society. The office of the Hesse Data Protection Commissioner received hundreds of telephone calls from citizens, and Simitis called the controversy “the first mass movement for data protection in West German history” (p. 80). The controversy only abated when, on December 15, 1983, the Federal Constitutional Court found the census law unconstitutional because it violated guarantees of the inviolability of the dignity of man (Article 1(1)) and the “right to the free development of [one’s] personality” (Article 2) contained in the *Basic Law for the Federal Republic of Germany of 1949*. The Court held that Germans have a right to informational self-determination, and that the right to free development of personality necessitated the ability of citizens to control what personal information is collected about them by the state and the purpose for which it is used. Any restrictions on this right must be clearly communicated to the citizen and proportionate to the benefit that will accrue from the violation.

As in the case of the Icelandic health database, judicial discourse grounded in constitutional guarantees of privacy and/or personal dignity and autonomy

provided a moment of resistance to managerial and technological imperatives; constitutional challenges in both cases enabled judges to reflect on legal principles as they are lived by social actors in the lifeworld and articulate law that accommodated the social meaning of privacy. However, managerial and technical imperatives were quick to reassert themselves. In spite of the fact that the Court's decision reinforced the indispensable role to be played by an independent data protection commission in the protection and advancement of this right, one year after the decision both Bull and Baumann argued that public concerns about the census were irrational and based on misinformation (Flaherty, 1989, p. 83). When a second controversy erupted during the 1987 census, many experts, including Flaherty, concluded that the problem was not that data collection violated the social expectations of privacy in the lifeworld but that public discourses about the nature of privacy were flawed:

The specific surveillance issues are largely symbolic and based on a nonexistent or inadequate public awareness of the true nature of statistical work and of the protective measures for confidentiality that are already in place... What is evident, and at the same time unfair, is that a census law in West Germany that has passed all the necessary legislative stages and benefited from the good advice of data protectors – *even if not all of that advice has been accepted* – can still encounter vigorous and even violent public reactions (Flaherty, 1989, p. 83, emphasis added).

International data protection instruments

OECD Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data

In 1980, as data protection legislation began to spread through Western Europe¹⁵, both the Council of Europe and the Organization for Economic Cooperation and Development (OECD) passed comprehensive instruments containing FIPs. The OECD process had begun in 1974, when an OECD seminar on policy issues in data protection and privacy was held in Paris (OECD, 1976). Between 1974 and 1981, OECD membership consisted of: 19 European states (**Austria**, Belgium, **Denmark**, Finland, **France**, **Germany**, Greece, Iceland, Ireland, Italy, **Luxembourg**, Netherlands, **Norway**, Portugal, Spain, **Sweden**, Switzerland, Turkey and the United Kingdom); three Australasian states (Australia, Japan, and New Zealand) and two North American states (Canada and the **United States**). Every country that had passed data protection legislation prior to 1980 (marked in bold) was an OECD member.

The OECD's stated mandate is to "build strong economies in its member countries, improve efficiency, hone market systems, expand free trade and contribute to development in industrialised as well as developing countries" and to reform public sector management practices "to promote efficient functioning of

¹⁵ Denmark, Austria, France, Norway and Luxembourg passed data protection laws in 1978 and, in 1980, Canada, Belgium, Iceland, the Netherlands, Spain and Switzerland had prepared draft bills.

government and the promotion of good governance” (OECD, 2004).

Accordingly, the OECD’s work on data protection is explicitly contextualized by the prioritization of economic integration and managerial efficiency. Because the OECD was one of the key international institutions seeking to set out rules to govern data collection, it became the major forum for dialogue between the United States and Europe on privacy issues. In addition, many Asian countries participated in conferences and meetings as observers (Burkert, 2000, p. 51). Its approach to privacy has accordingly been strongly influenced by the American perspective which, as noted above, relies on self-regulation in the private sector and seeks to minimize any trade barriers to the free flow of information or the development of new technologies.

The OECD *Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data* (OECD Doc. C(80)58, Oct. 1, 1980) contain eight of the ten FIPs. Although the Guidelines limit collection to lawful and fair means, they only require that information be collected with the individual’s knowledge and consent “where appropriate” (s. 7). The meaning of “where appropriate” is not specified, but the section is drafted to imply knowledge and consent are the exception and not the norm. This is consistent with the defined scope of the Guidelines. Under

Table 9 – OECD Privacy Guidelines

1. Accountability	✓
2. Identify purpose	✓
3. Knowledge & consent	–
4. Limit collection to purpose	✓
5. Limit use to purpose	✓
6. Retain only as long as necessary	–
7. Accurate	✓
8. Secure	✓
9. Open	✓
10. Access & correction	✓

s. 2, the Guidelines only apply to personal data “which, because of the manner in which they are processed, or because of their nature of the context in which they are used, pose a danger to privacy and individual liberties”. The implication that not all non-compliant collection of personal data violates privacy (or data protection principles) is explicitly spelled out in s. 3(b): “These Guidelines should not be interpreted as preventing ... the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties.”

Moreover, countries are asked to “take all reasonable and appropriate steps to ensure that transborder flows ... are uninterrupted and secure” (s. 16) and to avoid passing domestic legislation “in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection” (s. 18). The importance of the uninterrupted flow of information in the international marketplace was underlined in the *OECD Declaration on Transborder Data Flows* in 1985 (OECD Doc. 11, April 1985). The Declaration states that these flows are “an important consequence of technological advances and are playing an increasing role in national economies” (p. 1). Since “computerised data and information now circulate, by and large, freely on an international scale” (*ibid*) and this circulation brings “social and economic benefits resulting from access to a variety of sources of information and of efficient and effective information services,” OECD Member states agreed to “promote access to data and

information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information” (p. 2).

Thus, the OECD Guidelines were at least in part intended to promote the flow of personal data between states to enhance trade and promote efficiencies. FIPs were not perceived to be inconsistent with these goals; indeed, the admonition to avoid laws “in the name of the protection of privacy and individual liberties” that would obstruct the flow of personal data (s. 18) implies that FIPs were adopted because they minimize the risk to economic and bureaucratic goals that could be posed by privacy legislation based on a perspective other than data protection.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

On January 28, 1981, three months after the OECD Guidelines were passed, the COE opened its *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (CETS NO. 108, Strasbourg, 28.I.1981) for ratification. Although the Convention only applies to the automated processing of personal data, its provisions are very similar to the OECD Guidelines. Burkert argues that the similarity is not surprising, since both were drafted more or less by the same group of experts (Burkert, 2000, p. 52; Bennett, 1988; Bennett, 1992). In addition, both processes were influenced by the American perspective. As a member of the OECD, the United States took an active role in drafting the OECD Guidelines, and the COE Convention “received

special wording to provide for the unlikely event that the US would join” (Burkert, 2000, p. 66).

The Convention contains eight of the ten FIPs.

Although the earlier COE Resolutions contained some FIPs, the Convention introduced a number of interesting innovations. First of all, the Preamble reaffirms the member states’ “commitment to freedom of information regardless of frontiers” and states that it is “necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.”

Table 10 – COE Personal Data Convention

1. Accountability	✓
2. Identify purpose	✓
3. Knowledge & consent	–
4. Limit collection to purpose	✓
5. Limit use to purpose	–
6. Retain only as long as necessary	✓
7. Accurate	✓
8. Secure	✓
9. Open	✓
10. Access & correction	✓

Freedom to information is included in the COE *Convention for the Protection of Human Rights and Fundamental Freedoms*, as part of the right to freedom of expression. Article 10 of the Human Rights Convention states:

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and *to receive and impart information and ideas without interference by public authority and regardless of frontiers*. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises (emphasis added).

It is arguable that corporations may be included within the definition of “everyone” and, as such, have a right to receive information without interference from the state. In Canadian law, for example, s. 24(1) of the *Canadian Charter of Rights and Freedoms* has been interpreted to say that everyone, including artificial persons such as corporations, can apply for a remedy under the Charter (*R. v. Big M Drug Mart Ltd.* (1985), 18 C.C.C. (3d) 385 (S.C.C.)); however, s. 7 Charter rights to life, liberty and security of the person have been held not to apply to corporations as the rights protected therein can logically only apply to human beings (*Irwin Toy Ltd. v. Quebec (A.G.)*, [1989] 1 S.C.R. 927; *R. v. Wholesale Travel Group Inc.* (1991), 67 C.C.C. (3d) 193 (S.C.C.)). Even if the word “everyone” in Article 10 of the Human Rights Convention is interpreted to include corporations, the right to receive information conferred in that Article is contextualized within the broader democratic right to free speech. The intention of Article 10 is to ensure that democratic dialogue is not unduly restricted by government censorship. Access to information in this context requires that citizens be able to participate in public discourse by listening to and reading about issues without interference from the state.

It is arguable that this right to receive information should not be extended to include a right in the hands of corporations to collect and disclose personal information for commercial purposes, as this is not in keeping with the original intention of the drafters. Nor is it clear that this Article confers a right on governments to access personal information. Right to information legislation,

such as Canada's *Access to Information Act* (R.S., 1985, c. A-1) gives citizens the right to access government documents, not the other way around. The citizen's right to information strengthens democratic governance because it can be used to make government decision-making more transparent and therefore more accountable to the citizen. The argument organizations have a right to access of personal information is accordingly problematic in law. Nonetheless, it is often used to justify privacy invasive practices on the parts of data collectors¹⁶.

For our purposes, the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* explicitly attempts to "reconcile" the "fundamental value" of privacy with the "fundamental value of ... the free flow of information" (Preamble). Although the Convention does not infer that access to information is a right co-equal with privacy, it implies that organizational access to information is a competing interest of equal importance. This is inconsistent with the COE's original strong statements against managerial practices which create dangers to privacy, and shows how the COE's original concerns about the social value of privacy have been eclipsed by managerial demands for access to data irregardless of any social expectation of privacy.

¹⁶ One of the earliest drafts of s. 3 of the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) stated that the purpose of the Act was to establish information rules that recognize "the right of privacy of individuals with respect to their personal information and the right of organizations to collect, use or disclose personal information" until it was pointed out to the drafters that organizations do not have a "right" to information. The word "right" was changed to "need".

This “process of forgetting” is also evidenced by the priority that the Convention gives to the free disclosure and exchange of personal information. Article 12(2) provides that “A Party shall not, *for the sole purpose of the protection of privacy*, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party” (emphasis added). This is a surprising statement from a human rights perspective, as it implies that a state is prohibited from restricting the flow of data to a fellow signatory to the Convention solely because the restriction is required to protect privacy. Although a member state can derogate from this provision for “certain categories of personal data ... because of the nature of those data” (art. 12(3)(a)), the wording of the Article indicates that, in the event of a conflict between data protection and the “protection of privacy” (art. 12(2)), privacy loses.

The Convention also builds in significant exceptions to data protection requirements. Like other instruments we have examined, information needed for the purposes of security, public safety, crime control, statistics and scientific research is exempt; however, the Convention’s list of exceptions also includes data required to promote “the monetary interests of the state” (art. 9). It is difficult to conceive of restrictions placed on other human rights, such as the right to free speech or security of the person, for example, justified solely on the basis of fiscal benefits.

In sum, the COE’s adoption of FIPs coincided with a weakening of provisions to

protect the social value of privacy.

European Union Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data

As the European Union and the United States continued to dispute what constitutes appropriate regulation of the trade in personal information, data protection regimes were created in Israel, Canada, New Zealand, the United Kingdom, Finland, Ireland, the Netherlands, Australia, Japan, Thailand, Slovenia, Portugal, Spain, Belgium, Switzerland, Hungary, the Czech Republic, Monaco and South Korea. Much of the interest in data protection grew from European calls for international harmonization for trade purposes.

By the late 1980s, the European Union had become concerned that “discrepancies in data protection could impede the free flow of personal information throughout the EU and obstruct the creation of the Internal Market. Data protection ... was also intrinsically linked to the operation of international trade” (Bennett & Raab, 2003, p. 78). Accordingly, the EU enacted its *Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data* (Brussels, OJ No. L281 24 October 1995) in 1995. The Directive calls for member states to harmonize their privacy laws around a basic set of FIPs in order to promote trade.

Bargaining among stakeholders was intense throughout the five-year drafting

process, both among and between the public sector players (Simitis, 1995; Bainbridge, 1996) and private corporations (Regan, 1999). The Direct Marketing Associations within Europe and the United States spent millions of Euros to successfully lobby the drafters to remove the requirement for opt-in consent (Regan, 1999). The second part of the title referring to the “Free Movement of Such Data” was added to the second draft because of “the influence of private sector lobbying, but is also consistent with the economic motivations that permeated [earlier] OECD thinking” (Bennett & Raab, 20003, p. 78). The EU Directive was accordingly a negotiated response to an international trade issue, which was drafted to accommodate data collectors’ interests in maintaining access to personal data. This is in keeping with both the European interest in managerialism and the American valorization of technical innovation.

The Directive was also a key part of the policy structure developed to support the information superhighway, and demonstrates how privacy policy has been reconstituted to help create social conditions conducive to the adoption and mass implementation of new technologies. Like the Council of Europe before it, the European Union was concerned that consumers would not adopt e-commerce unless they were confident that there were rules protecting their personal information¹⁷. The Directive reflected the “perception, enunciated from

¹⁷ As discussed above, the COE made the same argument to support FIPs in the public sector; data protection was essential to building citizen trust in new government databases. See the Preamble to the Council of Europe Resolution regarding public sector databases (Resolution (74) 29) in particular.

the highest circles of governmental and inter-governmental policy-making, that trust and trustworthiness were key elements of the climate in which [information highway] initiatives would flourish” (Bennett & Raab, 2003, p. 79). Once again, privacy policy takes on a pedagogical role; instead of reflecting dialogic consensus about the importance of privacy as it is experienced in the lifeworld, privacy policy becomes a tool with which to reconstitute social experiences and make them conducive to the prerogatives of technical innovation.

One of the more contentious provisions in the Directive was the requirement that European states ban the export of personal information to countries which do not have substantially similar data protection legislation in place. In particular, the Directive states that “Member States shall provide that the transfer to a third country of personal data ... may take place only if ... the third country in question ensures an adequate level of protection” (art. 25) unless the data subject consents, the transfer is necessary to fulfill a contract or protect important public interests or the “vital interests of the data subject”, or the data is part of a public register (art. 26). Although the Americans continued to resist pressure to pass global data protection legislation for the private sector, this did not bar them from actively participating in the EU process. The United States attended the first European Parliament hearing on privacy and the “discourse on how to draft the Directive was a discourse that involved the US from the beginning” (Burkert, 2000, p. 66). Once the Directive was passed, this dialogue continued, and direct negotiation between Director-General of DG XV John Moog and US Under-

Secretary for Commerce David Aaron led to the Safe Harbour Agreement.

The Safe Harbour framework was developed to enable “US companies to avoid experiencing interruptions in their business dealings with the EU “ by voluntarily self-certifying with the Department of Commerce their intention to comply with a basic set of FIPs¹⁸. The FIPs required include the principles of accountability, identify purpose, accuracy, security, openness and access and correction. Data subjects must also be able to opt out of disclosures to third parties or disclosures for a secondary purpose. Certified companies which fail to comply with the specified principles are subject to an investigation by the Federal Trade Commission under its mandate to regulate unfair and deceptive trade practices. In spite of the lack of provisions requiring knowledge and consent (other than the negative opt-out for third party disclosure), limiting collection to a specified purpose or collecting only information that is relevant to the purpose, the EU held in 2000 that corporations certified under the Safe Harbour agreement provide adequate protection as required by Articles 25 and 26 of the Convention.

The above analysis indicates that data protection principles were adopted by a number of jurisdictions to promote a wide variety of interests, including:

- the protection of personal privacy in the advent of computer technology
- the protection of national sovereignty

¹⁸ By July 2004, 340 companies had certified their intention to comply with the Safe Harbour framework with the Department of Commerce.

- the resolution of conflicts over the distribution of power within states
- the legitimization of information practices adopted by the public and the private sectors
- the promotion of public sector and private sector efficiency
- the promotion of trade
- the promotion of technological development and innovation
- the promotion of economic integration
- the promotion of political integration

Although there was a great deal of discussion in the lifeworld in the early 1970s about the invasive nature of new technologies, the first states to draft data protection legislation – Hesse and Sweden – did so for reasons wholly unrelated to the ongoing public debate about privacy. And, as Table 3 indicates, privacy remained an ambivalent thread as data protection legislation was enacted by European and American law makers. The COE was the only jurisdiction to approach the issue from a perspective rooted in both historical memory and the social experience of totalitarianism. However, the COE's original broad statements of principle and legislative limits on surveillance purposes were soon replaced by a heavy reliance on procedural rules, as managerialism and the valorization of technology constrained and reconstructed the data protection agenda. Interestingly, the more the COE moved away from privacy protection as a dominant concern, the more FIPs it adopted.

Perhaps the provision with the most potential to evaluate whether or not new

surveillance mechanisms were appropriate *before* they were implemented was the licencing requirement in the 1973 Swedish Act. Licensing inherently provides an opportunity to exercise some form of oversight before surveillance practices are put in place. Jan Freese argued that licencing was essential in order to identify who was collecting what information so the public could exercise some control over data processing (Flaherty, 1989, p. 94). The Americans rejected the Swedish approach precisely because licensing threatened to choke off the explosive development in information technology occurring in the 1970s (United States, 1973, Section III). By 1981, Sweden itself had replaced licensing with a simple registration system¹⁹ because, according to the Ministry of Justice, licencing had proven to be inefficient and necessitated an unacceptable level of interference with the information practices in both the public and private sectors (Flaherty, 1989, p. 95).

Since 1985 – The Canadian experience

As data protection legislation has diffused throughout many parts of the world since 1985, managerial interests in efficiency and security, and the privileging of technical innovation have continued to drive the kinds of provisions adopted. Canadian privacy laws are typical in this regard. Canada's *Privacy Act* (R.S.C. 1985, c. P-21) governs public sector collection, use and disclosure of personal information. Although the Act implements FIPs to restrict the collection, use and

¹⁹ Except for databases containing sensitive information.

disclosure of personal information, the conditions under which collection is allowed are very broadly drafted and include any purpose that “relates directly to an operating program or activity of the [government] institution” (s. 4).

Accordingly, the government can justify the collection of information merely by creating an operating program or activity.

Moreover, any true ability to control the collection of one’s personal information is limited by vague language and exceptions to the general rules. For example, the individual must be advised of the purpose for collection, but only when the information is collected directly (s. 5 (1)), and indirect collection is allowed whenever direct collection is not possible (s. 5(2)). However neither requirement applies when they “might” result in inaccurate information or “defeat the purpose or prejudice the use for which information is collected” (s. 5(3)). As such, the government can legally collect personal information without the individual’s knowledge or consent, and the test to determine whether notification may be avoided is met if there is a mere possibility that notice might prejudice the use of the data as it is defined by the state²⁰.

The *Smith v. Attorney General of Canada* ([2001] 3 S.C.R. 902) case discussed

²⁰ The Act also provides that information can only be used or disclosed for the stated purpose or “any use consistent with that purpose” unless the individual consents (ss. 7 and 8). However, there is a long list of exceptions to this rule, including use or disclosure for enforcement of a law or the carrying out of a lawful investigation by an investigatory body, for archival purposes, for statistical purposes, or “for any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure (s. 8(2)(i)).

on pages 58-59 above is an interesting example of what happens when data protection principles conflict with a socially grounded understanding of privacy. Prior to the implementation of the data matching agreement between Customs Canada and what was then Revenue Canada, the Department of Justice consulted with the Privacy Commissioner of Canada to determine if he had any concerns about the program. The Commissioner advised the Department that there were serious implications for privacy should the state use personal information from government databases to profile citizens randomly without reasonable grounds to suspect that they have been involved in illegal activity. This kind of fishing expedition is traditionally viewed as an abuse of state power, and has the potential to significantly shift the relationship between the citizen and the state. On these grounds, the Commissioner strongly urged the government to abandon the program. However, the Department of Justice rejected the Commissioner's advice because the matching program complied with the provisions of the *Privacy Act* and was accordingly legal.

The gap between government practices and citizen expectations emerging in the lifeworld became apparent in 2000, when the Privacy Commissioner revealed that Human Resources and Development Canada had compiled detailed electronic dossiers on 33.7 million²¹ Canadians (Canada, 2000a). The databank, called the Longitudinal Labour Force File (LLFF), contained up to 2,000 discrete

²¹ The numbers reflect the fact that dossiers were compiled on living and dead Canadians.

pieces of information about each Canadian. The data were drawn from a number of government documents, including income tax returns, child tax benefit payment records, welfare files, job training and employment files, federal job program files, employment insurance records and the nation health insurance master file. Each file contained detailed personal information such as the individual's name, social insurance number, gender, date of birth, language spoken, citizenship/landed immigrant status, ethnicity, marital/family status, disabilities, income, employment history, employment insurance records, receipt of social assistance benefits and education.

The LLFF was compiled, from 1985 onward, for the purpose of assisting the government in evaluating the effectiveness of its labour market and social programs. In addition, information from the LLFF was released to private sector firms which used the data for planning, generating statistics and conducting labour market research, uses that were deemed to be consistent with the stated purpose under s. 8(2)(a) of the Act. However, when the public became aware of the LLFF's existence, there was a sharp outcry. Forty-eight hours after the Privacy Commissioner's concerns were first published in the press, over 500 Canadians had filed access to information requests with HRDC demanding to see their files. Two weeks later, HRDC had received over 69,000 such requests (Child, 2001).

In the wake of media scrutiny and public dissent, HRDC announced that it would

dismantle the LLFF. But the Minister of HRDC, Jane Stewart, never acknowledged that the LLFF was an unwarranted privacy invasion. She stated that, "there has never been a known breach of security with regard to this databank, and HRDC has been acting within the existing *Privacy Act*" (Canada, 2000). The Minister accordingly failed to acknowledge that it was not a potential security breach but the government's access to the database itself that violated Canadian's expectations of privacy. At the same time that she understated the privacy issues, the Minister underlined the importance of government efficiency, arguing that "Canadians expect programs that are well designed, continually improved, and responsive to their changing needs" (*ibid*). Although the Minister agreed to dismantle the database "given public concerns about privacy issues in this era of advanced and constantly changing technology" (*ibid*), she did not remove the data matching software that constructed the database, and still has the ability to compile profiles.

The Minister's comments reflect the complex set of goals embodied in data protection legislation, particularly the bureaucratic need to collect and use personal information to promote efficiency. Both the *Smith* case and the LLFF demonstrate how data protection principles work to privilege access to information when there is a conflict between managerial needs and the social experience of privacy in the lifeworld. The fact that legislation is in place structures citizen concerns about invasive practices on the part of the government because they assume the law constrains unacceptable surveillance.

As Privacy Commissioner Bruce Phillips pointed out during the LLFF controversy:

My problem here is ... the *Privacy Act* at the moment is insufficient to prevent these kinds of informational collections," he said. "The Canadian public believes, for example, that when they send their tax information, it doesn't go out of the tax department. Well, in fact, it does, many times and to many places. There's something like 200 informational exchange agreements between Revenue Canada and various other agencies, plus other governments (quoted in MacLeod, 2000).

The LLFF did not become a cause célèbre for 15 years, primarily because Canadians expected their privacy was given greater protection that it currently enjoys under the *Privacy Act*²².

Canadian private sector privacy legislation is equally structured by managerial needs and the valorization of technology. When Canada first began to consider passing a law, it was in direct response to the EU Directive. At the time, Quebec was the only Canadian jurisdiction with private sector legislation in place²³, and

²² In like vein, a 2003 study indicated that 57 percent of Americans mistakenly believe that the presence of a privacy policy on a web site ensures the data collector will not disclose their personal information (Turow, 2003, p. 21).

²³ By 1998, most of the provinces had enacted public sector data protection legislation, as follows: Alberta: *Freedom of Information and Protection of Privacy Act*, S.A. 1994 c. F-18.5; B.C.: *Freedom of Information and Protection of Privacy Act*, R.S.B.C.1996, c.165, *Privacy Act*, R.S.B.C. 1996, c.373; Manitoba: *Freedom of Information Act*, S.M. 1985-86, c.6 (C.C.S.M.c.F-175), *Privacy Act*, S.M. 1970, c.74 (C.C.S.M. c.P-125); New Brunswick: *Right to Information Act*, S.N.B. 1978, c. R-10.3, *Right to Information Amendment Act*, S.N.B. 1995, c.51; Nova Scotia: *Freedom of Information and Protection of Privacy Act*, R.S.N.S. 1993, c.5; Ontario: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c.F-31; Quebec: *An Act Respecting Access to*

the Canadian government was accordingly concerned that the absence of data protection rules would create a barrier to trade with Europe. In their joint discussion paper *Building Canada's Information Economy and Society: The Protection of Personal Information*, Industry Canada and the Department of Justice argued:

The ability to provide effective protection for personal information may be crucial to Canada's ability to remain competitive internationally in the global information economy. ... This [EU] Directive has the potential to make the protection of personal information a major non-tariff trade barrier with Canada ... Canadian businesses may be forced to undertake individual comprehensive negotiations to show compliance with the European Union rules. This process will be fraught with uncertainty and could become lengthy and expensive (Canada, 1998, p. 7).

Throughout the document, data protection legislation was cast in terms of trade and e-commerce. Prospective legislation was needed to “strike the right balance between the *business need* to gather, store, and use personal information and the *consumer need to be informed* about how that information will be used” (p. 2, emphasis added). From this perspective, data protection was seen as an essential element “of building the consumer trust and the market certainty needed to make Canada a world leader in electronic commerce” (p. 3).

Documents Held By Public Bodies and the Protection of Personal Information, S.Q. 1982 (L.R.Q. c.A-2.1); Saskatchewan: *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c.F-22.01, *Privacy Act*, S.S. 1990-91, c.P-24. Quebec was the only province with private sector legislation: *An Act Respecting the Protection of Personal Information in the Private Sector*, S.Q. 1993, c.17.

In response to these concerns, Canada passed the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2000 (R.S.C. 2000, c. 5). PIPEDA is based on the *Model Code for the Protection of Personal Information* (CAN/CSA Q-830) developed by the Standards Council of Canada in 1996. The Model Code was the result of negotiations between industry, government and consumer group stakeholders. Like the *Privacy Act* before it, PIPEDA contains a long list of exceptions to the application of FIPs, to ensure that FIPs do not reduce the efficiency of conflicting goals, such as policing, research or administration.

When the Government of Canada began to consider the need for PIPEDA in the late 1990s, there was a parallel process initiated by the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities (HURAD). HURAD conducted hearings and public consultations to explore legislative options which could account for the effect of new technologies on privacy broadly understood as a human right and social value. HURAD's consultations brought together 248 Canadians representing a wide range of perspectives to participate in a series of facilitated discussions with members of Parliament regarding the effect of technologies (such as genetic testing, biometrically coded smart cards and video surveillance) on their understanding and experience of privacy. The dialogic nature of the consultations provided HURAD with a window on the social expressions of privacy emerging in the Canadian public. After in-depth discussions in six different cities across the

country, the Committee concluded that:

Canadians see privacy not just as an individual right but as part of our social or collective value system... Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others – either with trust, openness and a sense of community, or with distrust, fear and a sense of insecurity (Canada, 1997, p. 6).

HURAD argued that, although the data protection legislation contemplated by Industry Canada was “clearly a critical part of the spectrum of privacy interest, in a world of increasingly intrusive technologies, it is by no means the only game in town” (Canada, 1997, p. 24); and that truly effective privacy protection can only be sustained if the social value of privacy is given greater weight than the economic benefits of what former Privacy Commissioner of Canada Bruce Phillips called “the traffic in human information” (Phillips, 1996, pp. 12-13). In effect, the Committee sought a legislative mechanism that would privilege the social meaning of privacy over the imperatives of managerialism and technological innovation. To this end, HURAD recommended that the Government of Canada enact a privacy rights charter that would provide privacy rights with quasi-constitutional status and require all federal legislation to respect everyone’s “physical, bodily and psychological integrity and privacy; privacy of personal information; freedom from surveillance; privacy of personal

communications; [and] privacy of personal space” (Canada, 1997, p. 45).

The charter was intended to be “umbrella legislation” that would help guide the development and application of all federal laws, including data protection legislation dealing with the collection of personal information by the private sector. By giving the charter precedence over data protection legislation, the Committee hoped to “capture the full breadth of privacy, like a wide angle lens taking in a panoramic view, as opposed to the data protection framework toward which the Industry and Justice Ministers are working that focusses, like a close-up lens, tightly on informational privacy rights” (Canada, 1997, pp. 44-45). The Committee expressly drew on the early work of the United Nations and the Council of Europe:

Ultimately, [the privacy charter] is about taking privacy seriously as a human right. To do that, we must invoke recent history and remind ourselves *why* the right to privacy was entrenched in the *Universal Declaration of Human Rights* and subsequent human rights instruments. Otherwise, we may be seduced into believing that privacy is simply a consumer rights issue that can be fixed by a few codes of conduct and some new, privacy enhancing technology (Canada, 1997, p. 72).

There was very little interaction between HURAD and Industry Canada as PIPEDA worked its way through the legislative process. Shortly after the Department of Justice and Industry Canada released their joint discussion paper

(Canada, 1998c) in 1998, Justice dropped out of the process due to disagreements with respect to how to draft the Bill, and the Minister of Industry carried the legislation through Parliament alone. Privacy advocates appearing before the Senate and the House Committees examining PIPEDA did argue that fair information practices needed to be contextualized within a broader understanding of privacy as a social and democratic value, and urged Parliament to expressly provide for: (1) protection of privacy as a fundamental human right; and (2) a limitation on the purposes for which information may be collected (Canada, 1998a; 1998b). In response, legislators incorporated the following clause into what was then Bill C-54:

The purpose of [the Act] is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances (PIPEDA, s. 3).

PIPEDA evidences the dynamic nature of the ongoing negotiation between the social meaning of privacy and the managerial agenda. Although this clause expressly recognizes that individuals have “the right of privacy”, that right is limited to informational privacy and contextualized by the “need” of administrative organizations to implement surveillance. In fact, the first draft of the clause

balanced the individual's right against a concurrent "right of organizations to collect" information; this corporate "right" was only changed to a "need" when advocates pointed out that corporations have no legal right to demand information from customers. However, as this chapter has demonstrated, by bracketing the right to privacy with "rules to govern the collection" of information, PIPEDA subordinates the social meaning of the right to privacy to managerial and technical imperatives by privileging instrumental demands to access the private sphere in order to control and manage risk. This has not been accidental. Canadian legislators have been reluctant to give teeth to privacy legislation because of concerns about constraining bureaucratic efficiency and the technical innovation that is said to drive the information economy. When MPs first considered a limitation on purposes clause for PIPEDA, they rejected constitutional language designed to situate privacy as an essential social and democratic value. Rather than limit surveillance to those "purposes which are demonstrably justified in a free and democratic society" (Canada, 1998b), they enacted the reasonable and appropriate standard in order to accommodate the fears of government intervenors that privacy protection would hamper both the public and the private sectors' ability to operate efficiently.

The Department of Justice made this argument expressly in 2000 when a *Privacy Rights Charter* (Bill S-21, 37th Parliament) modelled on HURAD's recommendations was introduced in the Senate of Canada by Senator Sheila

Finestone²⁴. During hearings before the Senate Standing Committee on Social Affairs, Science and Technology, Senior General Counsel Elizabeth Saunderson spoke strongly against the Bill because the legal recognition of privacy as a social value would place many of the government's information collecting programs in jeopardy. Although she assured the Committee that the Department is "sympathetic" with the social and democratic value of privacy, she argued that legislation that protects this broader understanding of privacy "would create a good deal of uncertainty and quite possibly may pose obstacles to many government programs and policy":

Let me give you a concrete example where the bill could affect departmental legislation and operations. Citizenship and Immigration Canada (CIC) collects a great deal of personal information relating to immigration applications and to the enforcement of deportation orders and immigration offences. Bill S-21 would potentially require CIC to defend its information gathering and sharing activities in court ... In conclusion, while Bill S-21 can be praised as intending to enhance the privacy of Canadians, the devil may be in the detail. Changes could come *at the expense of certainty, public safety, operational efficiency and fiscal responsibility* (Canada, 2001, emphasis added).

The history of the development of data protection legislation demonstrates that

²⁴ Senator Finestone had chaired HURAD during its privacy study before being appointed to the Senate.

the consensus behind FIPS is built on conflicting goals and agendas, and that legal protections for the social experience of privacy have consistently given way to competing public and private sector interests in efficiency, trade, security, and economic and political integration. Typically, privacy advocates have supported data protection regimes because they purport to give the individual control over his or her information, in keeping with Westin's definition of privacy as informational control²⁵. However, whenever individual control conflicts with other goals, those elements of FIPs that do not promote the managerial interest in data integrity have been weakened or dropped from the legislative toolbox.

As privacy has been "balanced" against competing interests, much of the social meaning of privacy contained within Westin's theory of informational control has been lost. Without broadening the theoretical basis for privacy protection beyond information rights, the social meaning of privacy will continue to be constrained by privacy-invasive practices on the part of the public and private sectors. Accordingly, effective privacy policy is predicated upon broadening the theoretical understanding of privacy beyond data protection, to account for the social experience of privacy in the lifeworld. The next chapter revisits Westin and identifies the social elements contained within his theory of privacy, as a first step towards building a theoretical framework that can account for the lived

²⁵ See the interventions of the Consumer Association of Canada and the Public Interest Advocacy Centre before the House of Commons Standing Committee on Industry with respect to Bill C-54, for example (Canada, 1998b).

experience of privacy in the lifeworld.

Chapter 4 – Exploring the Social in Westin’s Theory of Privacy

Westin’s seminal work, *Privacy and Freedom* (1967), is based on a thorough review of the sociological literature on privacy, and encompasses both a theoretical and empirical concern with emergent social issues revolving around the use of new technologies. However, at its heart, *Privacy and Freedom* is a legal project that expressly aims to inform policy making. It grew out of the Association of the Bar of the City of New York’s Committee on Science and Law, which was formed in 1959. The Committee was unusual in many ways, not least in its interest in a broad understanding of the interrelationships between science, people and society. Committee Chair Oscar Ruebenhausen recalls how the Committee’s interest in “embryonic issues that might later mature into problems” (Ruebenhausen, 1970, p. viii) was rooted in a desire to promote “a climate of understanding out of which public decisions could wisely evolve” (p. ix). The Committee’s proceedings led them to question:

If, as it seemed, the new technology was on a collision course with the values of personal privacy and human dignity, could the collision be averted? Could a system be devised to identify and permit beneficial uses of the new technology and yet, at the same time, preclude those uses that most men would deem intolerable? (*ibid*).

To explore these issues, the Committee undertook a formal study on privacy and technology early in 1962, and the result of that study, *Privacy and Freedom*, was

published eight years later.

Westin was accordingly specifically tasked with finding legal and policy responses that would maximize the benefits of new technologies while minimizing the risks. In Westin's words, "The real need is to move from public awareness of the problem to a sensitive discussion of what can be done to protect privacy in an age when so many forces of science, technology, environment, and society press against it from all sides" (Westin, 1967, p. 3). This emphasis on finding legal solutions is woven into his discussion of privacy theory. For example, his theoretical framing of privacy functions "helps to clarify the important choices about individual privacy that American law may have to make in the coming decade" (p. 32). In like vein, his exploration of the effect of surveillance technologies on American privacy norms "may help to guide American policy makers" (p. 4).

Westin's analysis of the law is not uncritical, and he seeks to reinvigorate "disappointing" legislative and common law responses (p. 364) that have failed "to bring technological surveillance under constitutional control" (p. 344). To this end, he articulates, for the first time, a list of fair information practices designed to ensure that the individual retains control over the collection, use and disclosure of her personal information:

- Accountability (pp. 325, 235);
- Identification of purpose (p. 377);

- Knowledge and consent (pp. 325, 375);
- Limitation of collection (p. 377);
- Limitation of use (p. 377);
- Retention (p. 376);
- Accuracy (p. 325);
- Security (p. 324);
- Openness (p. 325); and
- Right of access and correction (p. 325).

Although Westin's work is remarkable for its comprehensiveness and often prophetic analysis of emerging privacy issues, its success as a legislative programme is unparalleled. As Chapter Three indicates, his set of fair information practices has been incorporated into law both internationally and at the domestic level in 43 countries to date, and his definition of privacy as informational control continues to dominate the development of privacy policy¹. However, *Privacy and Freedom* contains a number of other policy recommendations that have not been incorporated by legislators. These "forgotten" prescriptions imply the law should provide some kind of oversight

¹ Professor Westin himself remains a key player in the policy process. He is the Director of Privacy Exchange (an organization put together by public and private sector stakeholders in the EU and the US to facilitate the exchange of cultural and legal perspectives on privacy and data protection), President of the Center for Social & Legal Research (a public policy think tank on privacy issues), and President of Privacy & American Business (a highly influential report and information service on privacy issues). He has been the academic advisor for over 15 public opinion surveys on privacy attitudes – the latest being the Consumer Privacy Activism Survey released in August 2004 – and continues to be a frequent intervenor in domestic and international legislative forums. For a detailed biography, see <http://www.pandab.org/whoswho.html>.

before invasive technologies are put into place to ensure that the purpose for surveillance is socially appropriate.

Recovering these forgotten prescriptions is the task of this chapter. I begin by returning to Westin's full legislative programme, and examine how it sought to constrain surveillance practices in order to protect and advance the social value of privacy. I then examine Westin's theoretical framework and unpack the sociological elements of his thinking. Westin's conception of privacy is rich in sociality, because it is rooted in the broader sociological tradition of Georg Simmel, Robert Park, Kurt Lewin and Erving Goffman. However, I argue that Westin failed to fully develop the sociality of privacy because of his focus on information flow. By conceiving of privacy as a counterpoint to social interaction, he creates two competing poles of privacy and sociality. Since the private is rooted in social withdrawal, privacy protection is defined as the ability to control the flow of personal information from the complete privacy of solitude to increasing levels of exposure as the individual leaves solitude for intimate and communal interaction. This places the individual's need for privacy in conflict with both his or her need for sociality and the community's need to invade privacy for the purposes of social control.

Westin's legislative programme

Westin introduces his legislative programme by arguing that "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” (p. 370). Westin suggests that there are five steps in such a process:

1. measuring the seriousness of the need to conduct surveillance;
2. deciding whether there are alternative methods to meet the need;
3. deciding what degree of reliability will be required of the surveillance instrument;
4. determining whether true consent to surveillance has been given; and
5. measuring the capacity for limitation and control of the surveillance if it is allowed (*ibid*).

Fair information practices are only introduced at the last stage of the inquiry, and only come into play if the organization seeking to use surveillance first meets the burden to prove that the surveillance should be “allowed”.

As discussed in Chapter One, Westin has been criticized for pitting the individual right to privacy against competing social goals, in effect creating a zero sum game in which privacy rights must be “balanced” or traded off against the social interest in efficiency and security. There is some merit to this criticism. Westin's analysis is firmly rooted in American liberal legal tradition and the Millian view of society as an aggregate of atomistic individuals who seek to establish a sphere of autonomy independent of and in tension with the collective. From this perspective, privacy is necessary to control the invasive powers of the state and to ensure that individuals can make rational, self-interested decisions with

relative autonomy (Bennett, 1995, p. 4). As such, the need to restrict surveillance is part of the individual's ongoing "struggle for liberty" (Westin, 1967, p. 67), and technologies are problematic precisely because they erode the "libertarian equilibrium among the competing values of privacy, disclosure, and surveillance" (*ibid*) established by the framers of the American constitution in 1789. Westin argues that the role of law is to control the flow of new technologies by articulating a "balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance" in order to maintain the conditions necessary for individual autonomy and democratic governance (Westin, 1967, p. 24). If this balance is understood to place the individual's need for privacy against society's need to advance the public good, then privacy is indeed a zero sum game which is open to communitarian attack.

However, as Regan notes, Westin's work is "rooted in the social context" (Regan, 1995, p. 27); and his legislative framework suggests much more than an instrumental balancing of individual vs. social needs. Indeed, Westin sees surveillance as a social issue which must be subjected to public judgment. The first step in his inquiry is to establish whether or not the need for surveillance is "serious enough to overcome the very real and presently rising risk of jeopardizing *the public's confidence* in its daily freedom from unreasonable invasions of privacy" (*ibid*, emphasis added). Although organizations often seek to use surveillance to:

... solve problems of genuine social importance... police forces ... to solve

crimes, corporations to control theft, employers to select more successful employees, educators to identify personality problems in school children, behavioral scientists to observe real-life situations... if all that has to be done to win legal and social approval for surveillance is to point to a social problem and show that surveillance would help to cope with it, then there is no balancing at all, but only a qualifying procedure for a licence to invade privacy (p. 370).

Westin argues that some collective benefit is not a sufficient reason to invade privacy; the importance of the benefit can only be determined by honestly evaluating the impact of the surveillance on relationships of social power and discrimination in society at large (pp. 370-371). From the start, Westin's program accordingly questions whether or not surveillance should be tolerated by the public because of its effect on social relationships. And to pose that question requires some kind of legal control over purposes, an ability to say no to surveillance when it is not socially appropriate².

Chapter Three demonstrates that data protection legislation has constrained sociological concerns about privacy in order to serve the instrumental needs of the systems world. However, Westin's analysis is sensitive to the pressures that instrumental thinking places on privacy – i.e. that organizations must penetrate

² Regan argues that Westin's model fails to protect privacy from the communitarian attack because he leaves the right to say no in the hands of the individual (Regan, 1995, p. 27). This is consistent with the third stage in Westin's balancing process, which asks whether the individual being watched has given informed consent to the surveillance in question. I deal with this issue in the discussion of boundaries below.

private boundaries to collect data to manage risk. Westin alludes to this danger when he warns:

The classic eighteenth- and nineteenth-century information theory was of rational individual action based on personal interest... Beginning in the early twentieth century, we have moved steadily toward a more behavior-predictive theory of information, which assumes the need for much psychological and organizational data in order to make the decisions of social science, business, and government. The more computers offer opportunities to simulate behavior, forecast trends, and predict outcomes, the more pressure is generated for personal and organizational information to be collected and processed. In a way we sometimes only dimly grasp, this is one of the great changes in modern society (p. 322).

In addition, his discussion of psychological testing (p. 385) leads him to conclude that the law should prohibit the use of certain psychological surveillance technologies, such as personality testing and polygraphs, because the use of these technologies for the instrumental goal of hiring productive employees violates social norms. He notes that "American society is unequivocally committed to the idea that religious notions are *private* and that no governmental or quasi-governmental authority (such as the corporation or the secular private university) should decide what is 'reasonable' in religious belief" (p. 276), and concludes that "society has a right, if it wishes, to forgo the 'penetration' of projective tests in what are, realistically, compulsory tests for government and industrial employment" (p. 277). He does not rely upon fair information practices

or individual consent to constrain these technologies. Instead, he argues that the law should expressly provide that they are prohibited because they violate “the general right of public employees to be free from unreasonable invasions of privacy” (p. 385). Legislation is required to establish “a broad standard in the tradition of the common-law right to privacy or the quasi-constitutional approach”³ (*ibid*) by which to judge whether or not the use of psychological surveillance is consistent with social objectives, including the “high social goal in American society” of “preserving an attitude of non-confession towards authorities” (p. 373).

As such, the first stage in Westin’s policy inquiry calls for public evaluation of whether or not a proposed surveillance scheme is consistent with the normative understanding of privacy that is embedded in social norms and values. The second and third stages are equally concerned with the social value of privacy. They place the burden of proof on organizations seeking to implement surveillance systems to establish that there are no less invasive alternatives to the proposed technology and that the proposed technology actually works *before* implementation can be considered. This is not an instrumental test. Westin argues that the case for surveillance should be articulated “in terms that the educated public could judge” (p. 371) and, once the burden is met, the public

³ This kind of legal standard is reminiscent of the constitutional arguments which were used to constrain the Icelandic national health sector database to mitigate the social ramifications of the surveillance, in spite of the fact the database complied with a legislated set of FIPs, as discussed on pp. 64-67 above.

must then decide whether or not the surveillance “should be permitted even though it *is* wholly scientific” (p. 374).

In Habermasian terms, this inquiry would limit the autonomy of instrumentalism by subordinating purposive rational action to social judgment⁴. However, the review of data protection legislation in Chapter Three demonstrates that Westin’s full legislative program has been neglected, and the almost exclusive legislative focus on fair information practices⁵ has allowed instrumentalism to constrain and restructure the sociological meaning of privacy as it is lived in the lifeworld.

Although privacy is still a contested notion, as can be seen by the controversies generated by the 1987 German census and the Icelandic health sector database, the law has failed to develop much of the social meaning of privacy contained in Westin’s framework, and data protection has been susceptible to being reconstituted along instrumental lines.

Interestingly, Westin’s definition of privacy has met a similar fate in the privacy

⁴ As discussed in Chapter Two, this is precisely the kind of legislative outcome that the Canadian Department of Justice sought to avoid when it argued against the *Privacy Rights Charter* before the Senate Standing Committee on Social Affairs, Science and Technology. General Council Elizabeth Saunderson stated that provisions placing the burden of proof on the organization using surveillance technology, and requiring the organization to demonstrate that its objective could not be achieved by any other less intrusive means would throw government and private sector practices into confusion. Therefore privacy protection must take a back seat to certainty and government efficiency.

⁵ As discussed in Chapter Two, the exception is the United States which continues to put a number of privacy issues under legislative scrutiny. Although the success of its privacy protection has been mixed, it is interesting that the one Western country that continues to engage with privacy in the legislature does not have comprehensive data protection policy.

literature. Westin is most often quoted for 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” (p. 7).

However, the definition continues:

Viewed in terms of the relation of the individual to social participation, 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 (p. 7).

Just as Westin’s broader legislative program has been eclipsed by data protection, the second part of his definition of privacy, the social part, has been dropped from policy discourses. The next part of this chapter revisits Westin’s theoretical approach to privacy in order to identify the social elements contained in that definition.

Social elements in Westin’s conception of privacy

As stated above, *Privacy and Freedom* is in essence a legal project which seeks to reinvigorate the mechanisms of democratic governance by enunciating legal protections for privacy. However, Westin expressly roots this project in the social psychological literature and seeks to explore privacy’s “psychological, sociological, and political dimensions ... on the basis of leading theoretical and empirical studies” (p. 3). He starts by drawing on Edward Hall’s *The Hidden*

Dimension and Robert Ardrey's *Territorial Imperative* and concludes that privacy is rooted in human evolution (p. 8) and that privacy norms are present "in virtually every society" (p. 13). Although these norms vary according to "each culture's conceptions of sensory relations" (p. 30), "a complex but well-understood etiquette of privacy is part of our social scenario" (p. 39). From this perspective, then, privacy is inherently social; it is part of the way in which social beings interact.

The social nature of privacy is evident throughout Westin's discussion of privacy states. For example, small group intimacy is essential to achieve the "basic need of human contact" which is expressed through "close, relaxed, and frank relationships between two or more individuals" (p. 31). Anonymity is constructed socially by the recognition on the part of others that the anonymous person should not be "held to the full rules of behavior that would operate if he were known to those observing him" (p. 31). In like vein, the state of reserve is defined as "a psychological barrier against unwanted intrusion", which is dependent upon the interaction between the individual seeking privacy and the others with whom she is interacting: "The manner in which individuals claim reserve and *the extent to which it is respected or disregarded by others* is at the heart of securing meaningful privacy in the

**Table 11 –
Westin's Privacy States
and Functions**

States:

1. Solitude
2. Intimacy
3. Anonymity
4. Reserve

Functions:

1. Personal autonomy
2. Emotional release
3. Self-evaluation
4. Limited and protected communication

crowded, organization-dominated settings of modern industrial society and urban life” (p. 32, emphasis added).

As such, Westin’s theoretical model is rich in sociality. But this sociality does not come out of a theoretical vacuum. Westin’s intellectual pedigree is drawn from a core group of sociologists who provide touchstones for his thought. He draws heavily on Georg Simmel, particularly in defining the privacy states of anonymity and reserve. For Westin, anonymity is an essential part of Simmel’s “phenomenon of the stranger” (p. 31). Westin uses Simmel’s insight that strangers “often received the most surprising openness – confidences which sometimes have the character of a confessional and which would be carefully withheld from a more closely related person” (Simmel, 1950, p. 408) to explain how anonymity allows a person to “express himself freely” because he knows he will not be “held to the full rules of behavior and role that would operate if he were known to those observing him” (Westin, 1967, pp. 31-32).

Reserve, or “the creation of a psychological barrier against unwanted intrusion” (p. 32) is rooted in Simmel’s concept of “mental distance” – the combination of “reciprocal reserve and indifference” which is exhibited during social interaction to “protect the personality” (*ibid*). Westin notes that his own conceptualization of privacy as the tension between the individual’s desire to withhold or disclose information was earlier identified by Simmel as the tension between “self-revelation and self-restraint”, and between “trespass and discretion” (*ibid*).

Westin's sociological roots are also evident in his articulation of privacy functions. He uses the work of Simmel, Robert Park, Kurt Lewin and Erving Goffman to ground his first function, autonomy, as an aspect of the core self which interacts with others in a series of concentric circles moving outward from solitude to intimacy to general social interaction (p. 33). Westin expressly adopts the description of the self as developed by these thinkers, i.e.:

[The] core self is pictured as an inner circle surrounded by a series of larger concentric circles. The inner circle shelters the individual's 'ultimate secrets' – those hopes, fears, and prayers that are beyond sharing... The next circle outward contains 'intimate secrets', those that can be willingly shared with close relations... The next circle is open to members of the individual's friendship group. The series continues until it reaches the other circles of casual conversation and physical expression that are open to all observers (*ibid*);

and uses Park's and Goffman's understanding of social masks to explain why forced exposure is so devastating to the individual:

If this mask is torn off and the individual's real self bared to a world in which everyone else still wears his mask and believes in masked performances, the individual can be seared by the hot light of selective, forced exposure ... [O]nly grave social need can ever justify destruction of the privacy which guards the individual's ultimate autonomy" (pp. 33-34).

Westin's description of the second privacy function, emotional release, is based

on Goffman's work on social roles. Westin writes:

Like actors on the dramatic stage, Goffman has noted, individuals can sustain roles only for reasonable periods of time, and no individual can play indefinitely, without relief, the variety of roles that life demands. There have to be moments "off stage" when the individual can be "himself" (p. 35).

Westin argues that, from this perspective, privacy is essential because it provides moments when individuals can "lay their masks aside to rest. To be always 'on' would destroy the human organism" (p. 35). He draws on Goffman's work on total institutions to support this, and concludes that the privacy function of release allows us "respite from the emotional stimulation of daily life" (*ibid*) and space in which to manage bodily and sexual functions (p. 36).

The privacy function of self-evaluation is based on Park's argument that reflective solitude is necessary to provide the individual with an opportunity "to anticipate, to recast, and to originate" (Park & Burgess, 1921, p. 231). For Park, solitude, like religious contemplation, is a time for "organizing the self" (Coe, quoted in Park & Burgess, 1921, p. 237). Westin argues that such contemplation enables the individual "to integrate his experiences into a meaningful pattern and to exert his individuality on events." He concludes that, "To carry on such self-evaluation, privacy is essential" (p. 36).

In his discussion of the last privacy function, limited and protected

communication, Westin draws heavily from the work of Simmel and Goffman. Westin begins by asserting that, "In real life, among mature persons all communication is partial and limited, based on the complementary relation between reserve and discretion that has already been discussed" (p. 37) in connection with Simmel's work on self-revelation and self-restraint. He then notes that "limited communication is particularly vital in urban life" (pp. 37-38) and, in support of this, refers to Simmel's work on the role of reserved communication in preserving the self in the metropolis. Westin continues to explore two general aspects of limited communication. The first aspect, which provides for the sharing of confidences in relationships of trust, relies on Goffman's ethnographic studies of every day social relationships, and on Simmel's analysis of the confessional aspect of sharing confidences with strangers. The second aspect, which "serves to set necessary boundaries of mental distance in interpersonal situations" (p. 38), is drawn directly from Simmel's discussion of the need to create mental distance in a successful marriage, and Goffman's studies of the ways in which facial expressions, gestures, jokes and conversational conventions (such as changing the subject) are used to signal the need to withdraw from others.

Westin is therefore steeped in the sociological literature, and draws from a body of intellectual resources that focuses on the sociality of daily interaction. What then accounts for the ways in which his theory has been used to truncate the social understanding of privacy to informational control? Chapter Three

indicates that privacy has been constrained by both the valorization of technology and the managerial interest in efficiency and control. However, I argue that part of the answer also lies in Westin's focus on the control of personal information. For reasons discussed below, this focus leads to the conclusion that privacy is either a-social or anti-social. Accordingly, the social roots of Westin's conceptualization of privacy states and functions, like the social elements of his legislative program, disappear from view.

The disappearing social dimension

Regan argues that Westin fails to develop the social meaning of privacy fruitfully because he anchors the concept to a "personal adjustment process" (Westin, 1967, p. 7) in which the individual decides, "with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public" (Westin, 1967, p. 42). In this way, the individual is extracted from the social and placed in conflict with the collective, as he seeks to resist social demands for exposure.

The juxtaposition of the individual and the social is built into Westin's inquiry at an early stage. The Association of the Bar of the City of New York's Committee on Science and Law tasked Westin with explaining the "interaction of [privacy] and the competing claims of society" (p. xii) in the context of "their underlying, adversary values" (xi), and the liberal conception of the atomistic individual is imported through Westin's legal analysis. Moreover, Westin continually refers to

the tension between the individual's right to privacy, on one hand, and society's interest in invading privacy on the other hand⁶, and Regan's critique (1995) that this makes privacy vulnerable to communitarian attack is a cogent one.

However, when Westin speaks of competing interests in privacy, disclosure and surveillance, the disclosure side of the equation is not imposed by the collective on the individual in order to affect social ends; social control is brought about through surveillance which can, in turn, be resisted by the individual through withdrawal and reserve. Disclosure, on the other hand, is the result of the *individual's* choice to seek out and participate in social interaction as opposed to the collective choice to invade. Westin writes, "the individual in virtually every society engages in a continuing personal process by which he seeks privacy at some times and disclosure or companionship at other times" (p. 13). Moreover, the desires for privacy and disclosure are co-equal: "Individuals have needs for disclosure and companionship every bit as important as their needs for privacy" (p. 39).

Westin, quoting Murphy, calls the process of balancing these competing interests one of the key "dialectical processes in social life" (Murphy, 1964), and sets the stage for Altman's development of privacy as a boundary control mechanism. However, Westin immediately limits his insight into the social

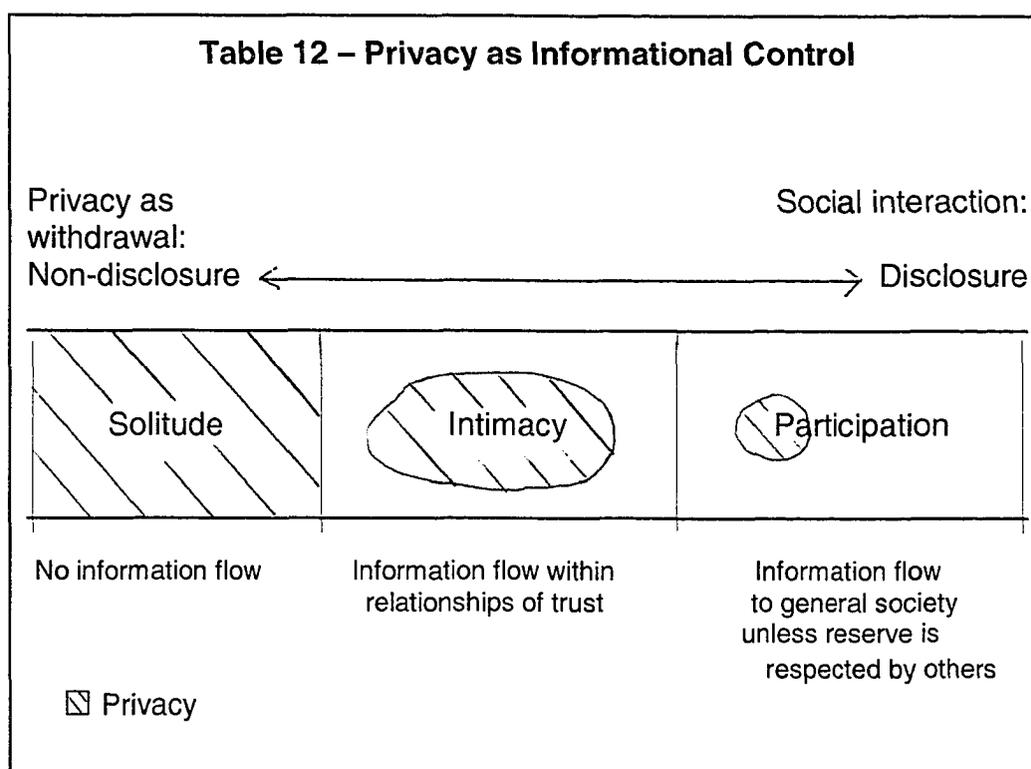
⁶ See, for example, Westin, 1967, pp. 12, 13, 22, 24, 28, 39 and 42.

nature of privacy in two related ways. First, as Regan argues, he leaves it up to the individual to adjust the balance by himself, in isolation of others. He states, "Although it is obviously affected by the cultural patterns of each society, the process is adjusted in its finer degrees by each individual himself" (p. 13). Accordingly, the individual is burdened with the sole responsibility of protecting his privacy, just when technology is permeating traditional boundaries. This leads to the result in the *Tessling* case, where individuals who wish to remain inscrutable are required to take extraordinary measures to retain their body heat within the physical limits of their dwelling house so it cannot be captured by infra red technologies⁷.

Second, by defining privacy as the opposite of social interaction, Westin shifts the focus of his inquiry to the flow of information across the boundary between private spaces and public spaces, rather than on the boundary itself. If privacy is "the withdrawal of a person from the general society" (p. 7), then the fullest form of privacy is social isolation. In Westin's words, "solitude is the most complete state of privacy that individuals can achieve" (p. 31). But if this is so, then privacy is a-social, existing on one pole on a continuum in tension with social interaction on the other pole. As the individual seeks to satisfy her competing interest in privacy and in social participation, she must develop mechanisms that allow her to control the consequences of her interactions in ways that do not

⁷ See pp. 63-64 above.

disclose more than she is willing to reveal as she moves out of solitude. Accordingly, as the individual moves further from “perfect privacy” through interactions with intimates to general social participation, privacy shrinks and “restricting information about himself and his emotions [becomes] a crucial way of protecting the individual in the stresses and strains of social interaction” (p. 13). (See Table 12).



Westin accordingly interprets social mechanisms to protect privacy within the context of the disclosure of information. For example, he argues that kinship rules “present individuals with a need to restrict the flow of information about themselves to others and to adjust these regulations constantly in contacts with

others” (p. 14). “Covering the face, averting the eyes, going to one’s mat, or facing the wall” are seen as ways of “restricting the flow of information about oneself” in the intimacy of the household (pp. 15-16). Reserve “expresses the individual’s choice to withhold or disclose information – the choice that is the dynamic aspect of privacy in daily interpersonal relations” (p. 32).

Once the focus shifts to the flow of information, privacy is no longer grounded in the social interaction of subjects, but located in the individual’s unilateral control over keeping information on the internal side of the boundary. As Westin says, “deciding when and to what extent to disclose facts about himself – and to put others in the position of receiving such confidences – is a matter of enormous concern in personal interaction, almost as important as whether to disclose at all” (p. 37). From this perspective, privacy is no longer a-social; it becomes anti-social. Since disclosure is dependent on the trustworthiness of intimate others and the sensitivity of the general public to respect the individual’s reserve, any social interaction poses a risk to privacy and privacy can only be fully protected by a withdrawal from others.

The focus on informational control also leads to the anomalous result that personal information may be restricted even when disclosure does not violate the individual’s lived sense of privacy. For example, some Canadian hospitals no longer tell the chaplain when a patient who has self-identified as a member of a particular religion is in the hospital because that requires the disclosure of

information. But the purpose of self-identification is to signal your belonging to and participation in a social group for the purposes of obtaining social support in a time of stress, and individuals who do not want to interact with the particular chaplain can simply choose not to do so. Cutting off the information flow disrupts the individual's enjoyment of intimate social discourse and support, isolating the individual. Similarly, some Canadian school principals refuse to reveal personal information about a child who was involved in a fight to the parents of the other child, claiming that the disclosure of that information would violate the child's privacy. The two children are left in a social void and the ability of intimate others to help them resolve a social problem is hampered because the social flow of information is artificially restricted. This is the opposite side of the coin we examined in Chapter Three, when fair information practices failed to restrict collections that violated the lived expectation of privacy, in Germany during the 1983 census or in Canada during the longitudinal labour force database controversy, for example. Either way, whether we are left with overly restrictive constraints on the flow of personal information during social discourse or with rules that privilege organizational access in spite of social demands to be left alone, Westin's insights into the sociality of privacy are lost because of his focus on the flow of information.

The next chapter will seek to recover and reconstitute those insights, by putting Westin into conversation with George Herbert Mead. I turn to the work of George Herbert Mead because he picks up on themes introduced by his

contemporaries Simmel and Park, and uses them to develop a comprehensive theoretical understanding of the emergence of the self through social interaction. In addition, Mead's work on symbolic interactionism and social psychology forms the foundation upon which Lewin and Goffman built. Accordingly, his thinking is at the base of the sociological tradition upon which Westin builds.

Chapter 5 – Applying Mead, Altman and Habermas to Privacy Theory

To have a whole life, one must have the possibility of publicly shaping and expressing private worlds, dreams, thoughts, desires, of constantly having access to a dialogue between the public and private worlds. How else do we know that we have existed, felt, desired, hated, feared? (Azar Nafisi, 2003).

This chapter seeks to extend Westin's conceptualization of privacy by applying the work of George Herbert Mead, as it has been applied and extended by Irwin Altman and Jurgen Habermas. Although Westin does not draw specifically on Mead in his formulation of privacy states and functions, Westin's primary sources – Simmel, Park, Lewin and Goffman – are all connected to Mead and the school of social psychology he founded. Simmel, like Mead, concentrates on the emergence of the social through interaction in the local situation. Simmel's view that "society consists of an intricate web of multiple relations between individuals who are in constant interaction with one another" (Cosser, 1977) and that, "Society is merely the name for a number of individuals, connected by interaction" (Simmel, 1950, p. 3-23) resonates with Mead's symbolic interactionism and understanding of language as an exchange of significant gestures. Robert Park was a colleague of Mead's at the University of Chicago, and both Kurt Lewin and Erving Goffman appropriated Mead's work on social psychology to develop field theory and ethnomethodology, respectively. Mead is

therefore important because he lies at the base of the body of the intellectual resources upon which Westin builds his theory of privacy.

I begin by comparing Westin's theory of privacy with Altman's work on personal space and territoriality. Like Goffman and Lewin, Altman uses Mead's conceptualization of social psychology to explore the issues which interest him. Altman's is therefore the most complete attempt in the literature to incorporate and apply a Meadian perspective to the questions Westin raises. However, Altman stops short of developing a "full-blown theory" (Altman, 1975, p. 4) and so, after examining Altman's contribution, I return to the source of the social psychological perspective, George Herbert Mead.

Mead's work is a useful counterpoint to Westin's perspective because it dissolves the apparent conflict between the individual and the social and recasts privacy as a boundary negotiation process, as Altman (1975) saw. However, I argue that a complete corrective requires radicalizing Westin's conception of the individual by applying a Meadian/Habermasian understanding of the emergence of the self through communication. From this perspective, privacy is the boundary between the self and the other, both externally (as Altman argued) and internally through discourse with the generalized other. Privacy is therefore a social construction rooted in language that sits at the core of inter-subjectivity and self-reflexivity. As such, it cannot be traded off in exchange for some other benefit, like efficiency or convenience. I conclude that privacy is a flashpoint for

social struggle precisely because instrumental reason negates the conditions necessary for inter-subjectivity by objectifying the self and collapsing the boundaries between social roles. As such, privacy policy will only be effective if it goes beyond data protection and constrains instrumental imperatives with legal mechanisms designed to protect the conditions necessary for inter-subjective dialogue.

Altman's appropriation of Westin

Altman is able to capture and develop the social elements of Westin's theory by recasting privacy as a boundary control mechanism. Privacy is no longer in tension with social interaction; instead, it is negotiated through social discourse.

Altman is attracted to Westin's approach because Westin locates privacy in complex social settings, and suggests how a variety of mechanisms operate to create various "degrees of privacy" (p. 18). In addition, both argue that privacy is a cultural universal that encompasses interaction between a number of diverse social actors, including individuals and groups. But Altman places special significance on Westin's insight that, "individuals and groups seek a balance between openness and closedness. Furthermore, too much or too little separation is undesirable" (p. 19). For example, Westin argues that, "To be left in privacy when one wants companionship is as uncomfortable as the inability to have privacy when one craves it" (Westin, 1967, p. 39), and, "Either too much or too little privacy can create imbalances which seriously jeopardize the

individual's well-being" (p. 40).

Altman takes the "dialectic and optimizational approach to privacy implied by Westin" and makes it a "central feature of [his] theoretical approach" (Altman, 1975, p. 19). However, Altman is able to do this without stripping privacy of its social core. Unlike Westin, who puts privacy and social interaction at opposite poles, Altman juxtaposes openness and closedness to others; privacy becomes the negotiated line between the two. Altman accordingly defines privacy as:

... an *interpersonal boundary process* by which a person or a group regulates interaction with others. By altering the degree of openness of the self to others, a hypothetical personal boundary is more or less receptive to social interaction with others. Privacy is, therefore, a dynamic process involving selective control over a self-boundary, either by an individual or a group (Altman, 1975, p. 6).

In this model, privacy is not equated with social withdrawal, but defined as "an interplay of opposing forces – that is, different balances of opening and closing the self to others" (p. 11). Altman therefore does not anchor privacy to the individual's control over the disclosure of information. Instead, he argues that privacy is a bi-directional process that involves both inputs from and outputs to others (pp. 11, 18). People have a satisfactory result when their desired state of privacy matches the achieved state. This implicates others in the ways in which privacy is constructed and experienced – privacy becomes "an interpersonal

event, involving relationships among people” (p. 22). Accordingly, the individual seeking privacy is no longer isolated from social praxis and privacy can be obtained in a full range of social situations, from solitude to public participation, so long as the individual is able to negotiate a comfortable boundary between the self and others.

Altman’s approach captures many of the insights Westin has into the relationship between privacy and self identity, and theorizes them within a fully social framework. For example, Altman draws on Westin’s insight that privacy is an essential part of self-evaluation because it is necessary to enable the individual “to integrate his experiences into a meaningful pattern and to exert his individuality on events” (Westin, 1967, p. 36). However, Altman expands on this by placing it into the context of a Meadian understanding of identity. He writes:

We use other people to help label our feelings and define our perceptions. It might be said, therefore, that one function of privacy is to assist in the social-comparison process – at the interface of the self and others. As such, privacy regulation may enable the person to decide on courses of action, to apply meanings to various interpersonal events, and to build a set of norms or standards for interpreting self/other relations. (Altman, 1975, 47)

Thus, Westin’s conclusions that solitude is central to the ongoing dialogue between the self and its conscience (Westin, 1967, p. 31), and that reserve is necessary “to protect the personality” (p. 32) are brought into a deeper

theoretical dialogue regarding the emergence of the self. In like vein, Altman uses Westin's functions of personal autonomy and emotional release to explore the importance of privacy to the interface between the self and other.

Altman concludes that privacy has three functions or goals (pp. 47-48):

1. the regulation of interpersonal boundaries;
2. the development and management of interpersonal roles and dealing with others; and
3. self-observation and self-identity.

All three are tied to the emergence of the self:

In my view, self-identity is central to human existence. For a person to function effectively in interaction with others requires some understanding of what the self is, where it ends and begins... The essence of this discussion is that privacy mechanisms defines the limits and boundaries of the self. When the permeability of those boundaries is under the control of a person, a sense of individuality develops... If I can control what is me and not me, if I can define what is me and not me, and if I can observe the limits and scope of my control, then I have taken major steps toward understanding and defining what I am. Thus privacy mechanisms serve to help me define me (p. 50).

Altman's work therefore points to a theoretical framework that has the potential to subsume Westin's theory as Margulis suggests (Margulis, 2003a, p. 422), and

to capture and develop Westin's insights into the sociality of privacy. However, as an environmental psychologist, Altman's primary interest is the relationship between human social behaviour and the physical environment (p. 1). Privacy is important to Altman because it is a "key link among the concepts of crowding, territorial behavior and personal space" (Altman, 1975, p. 4). In his own words:

I will offer the idea of self/other boundary regulation as an important theoretical process necessary to understanding certain features of environment-behavior relationships. Thus, although I will not state a full-blown theory in the usual sense of the term, I hope to take several necessary steps preliminary to the development of a sophisticated theory of environment and behavior relationships (*ibid*).

To take Altman's work on privacy forward, the next part of the chapter returns to Mead, and begins to lay the groundwork for a theory of privacy that encompasses and supports Altman's analysis. My inquiry is divided into three sections. First, I examine Mead's conceptualization of the self as social emergent, the role of privacy in the formation of identity, and how role-taking explains the social value of privacy in a modern society. Second, I explore how Habermas has extended Mead's work in the context of communication and democratic autonomy. Last, I use a Meadian/Habermasian framework to posit that privacy is a social emergent of language that sits at the core of inter-subjectivity and self-reflexivity.

Applying Mead to privacy theory

Privacy and the social self

Mead, like Westin, was writing at a time when technology was challenging traditional social and political relationships. At the turn of the century, industrialization and rapid growth had led to the disintegration of small communities, and atomistic individualism was unable to reorient a public which was overwhelmed by the conditions of modern life. The Chicago School's critique of the technological and economic consequences of modernity, and the attendant concentrations of economic and political power which threatened the democratic project, convinced Mead and his colleagues that the social sciences should seek to ascertain the current state of society, and make society visible to itself (Peters, 1986, 531). Accordingly, they sought to re-theorize social interaction in a conscious effort to create the self-reflexive conditions necessary for the workings of modern democracy.

As such, Mead was occupied with the same question as Westin: how to theorize democratic relationships so that new technologies do not derail the democratic project. For Mead, the answer to this question is grounded in the nature of the individual and the community. He argues that individuals are reflexive, intelligent beings capable of knowing themselves and the world. However, the act of knowing – indeed the emergence of the self itself – is a social process. For Mead, the self emerges through social communication, and self-consciousness entails a recognition of the necessity of social dependence upon others. The

apparent tension between the individual and the collective dissolves, because the social is antecedent to and constitutive of the individual:

The difficulty is that [contemporary psychology] presupposed selves as antecedent to the social process in order to explain communication within that process, whereas, on the contrary, selves must be accounted for in terms of the social process, and in terms of communication; and individuals must be brought into essential relation within that process before communication, or the contact between the minds of different individuals, becomes possible. The body is not a self, as such; it becomes a self only when it has developed a mind within the context of social experience (Mead, 1934, pp. 49-50).

Unlike the communitarians, Mead does not give the social precedence over the individual. Rather, the social is a prior condition to the emergence of the self that nonetheless allows each individual to develop her own unique, autonomous personality. Mead writes:

The fact that all selves are constituted by or in terms of the social process, and are individual reflections of it – or rather of this organized behavior pattern which it exhibits, and which they prehend (*sic*) in their respective structures – is not in the least incompatible with, or destructive of, the fact that every individual self has its own peculiar individuality, its own unique pattern... In other words, the organized structure of every individual self within the human social process of experience and behavior reflects, and

is constituted by, the organized relational pattern of that process as a whole; but each individual self-structure reflects, and is constituted by, a different aspect or perspective of this relational pattern, because each reflects this relational pattern from its own unique standpoint; so that the common social origin and constitution of individual selves and their structures does not preclude wide individual differences and variations among them (p. 201).

As such, Mead's conceptualization of the self as social emergent accounts for both the social nature of private experience *and* the potential for individual autonomy so important to Westin; although the self emerges from social interaction, it is not determined by the social. From this perspective, the tension between the social and the individual which is so problematic in Westin's theory dissolves.

But how can one account for the emergence of privacy itself? Mead suggests that language is the basic mechanism through which social processes occur because it is what calls forth the appropriate social response during interaction. During any social act, language allows for an adjustment in the actions of one actor to the actions of the other because gestures "act as specific stimuli calling forth the (socially) appropriate responses of the second organism" (p. 9). Thus, if the boundary between the self and others is located in symbolic interaction, then that boundary becomes both dialectical and fluid, as Westin and Altman suggest. Mead writes, "No hard-and-fast line can be drawn between our own

selves and the selves of others, since our own selves exist and enter as such into our experience only in so far as the selves of others exist and enter as such into our experience also" through language (p. 164). It is therefore possible to theorize privacy within the context of the emergence of identity through language.

Privacy and identity

Mead argues that the self can only emerge if it becomes an object to itself, and that can only occur through language: "I know of no other form of behavior than the linguistic in which the individual is an object to himself, and, so far as I can see, the individual is not a self in the reflexive sense unless he is an object to himself" (p. 142). The significant symbols that are used in language call out in the listener the same response as they do in the speaker. Accordingly, language enables each actor to view his own gestures from the perspective of the other, and to see himself as the other sees him, as a social object (Habermas, 1992, p. 176). Language also enables the individual to become conscious of a generalized other:

... to the extent that those responses can be called out in the individual so that he can answer to them, *we have both those contents which go to make up the self, the "other" and the "I."* The distinction expresses itself in our experience in what we call the recognition of others and the recognition of ourselves in the others. We cannot realize ourselves except in so far as we can recognize the other in his relationship to us. It is as he

takes the attitude of the other that the individual is able to realize himself as a self (Mead, 1934, p. 194, emphasis added).

The self therefore emerges through the recognition of the other and the I. Privacy, as the boundary between the two, is placed at the centre of identity because it allows the self to become reflexive. Mead implies this when he distinguishes between the “private” nature of subjective experience that is withheld from others, and the “private” nature of reflexivity that is made possible through the internalization of the dialogue between the social me and the undetermined I. He argues that both subjective and reflective experiences are private, in the sense that they are only accessible to the individual. However, the:

... common feature of accessibility does not necessarily give them the same metaphysical status ... the self has a sort of structure that arises in social conduct that is entirely distinguishable from this so-called subjective experience of these particular sets of objects to which the organism alone has access – the common character of privacy of access does not fuse them together (Mead, 1934, p. 167)

The first meaning of “private” resonates with Westin’s understanding of privacy as the withholding of information by an isolated individual. However, the second meaning of “private” implies that privacy is social because it is embedded into the emergence of identity through symbolic interaction between social actors. Because it delineates the boundaries of the self, privacy is a necessary condition

for reflexivity and inter-subjective dialogue. In Westin's terms, "Every individual needs to integrate his experiences into a meaningful pattern and to exert his individuality on events. To carry on such self-evaluation, privacy is essential" (Westin, 1967, p. 36).

Habermas notes that, for Mead:

... individuation is pictured not as the self-realization of an independently acting subject carried out in isolation and freedom but as a linguistically mediated process of socialization and the simultaneous constitution of a life-history that is conscious of itself. The identity of socialized individuals forms itself simultaneously in the medium of coming to an understanding with others in language and in the medium of coming to a life-historical and intrasubjective understanding with oneself. Individuality forms itself in relations of intersubjective acknowledgement and of intersubjectively mediated self-understanding (Habermas, 1992, 153).

Accordingly, "the self of an ethical self-understanding is dependent upon recognition by addressees because it generates itself as a response to the demands of an other in the first place" (p. 170). Because of this, privacy cannot shelter the atomistic ego from social interaction, as Westin posits; rather the line between self and other is inter-subjectively constituted through communication. Privacy is a potentiality across Westin's spectrum from solitude to social participation because it is central to the distinction between self and other which enables the self to see itself as social object.

Privacy and role-taking

Mead argues that taking the perspective of the other extends to the assumption of a variety of social roles. Since the vocal gesture “call[s] out the response in one form that is called out in the other, [the] child plays the part of parent, of teacher, or preacher” (Mead, 1934, p. 96). By “putting himself in the role of the person who is speaking to him, then he has the meaning of what he hears, he has the idea: the meaning has become him... The individual takes this attitude not simply as a matter of repetition, but as part of the elaborate social reaction that is going on” (p. 109).

Since role-taking is in essence a social phenomenon, privacy is essential because it allows the social actor to construct lines between roles. It is privacy that enables her to function in one role separate and apart from another role. Surveillance is problematic because it collapses the boundaries between roles and makes the actor accountable for all his actions – independent of the context or the role he is playing – to the same people. Goffman (1961) calls this “looping.” During his study of mental hospitals, he noted that patients were unable to keep their various roles separate because they were always under observation; their actions in the context of one role were never separated from their actions in the context of other roles. They were accordingly “constantly confronted with inconsistencies in their behavior and were fully accountable to the same people for all aspects of behavior” (Altman, 1970, p. 40). Altman

concludes that this type of boundary violation “may well be a deterrent to rehabilitation, because [it] exposes the self, eliminates a number of normal self-boundary processes, and makes the person extremely vulnerable to others” (*ibid*).

Locating privacy within a Meadian understanding of role-taking therefore explains Westin’s insight that privacy serves to relieve the self of emotions which build up because the self plays a multiplicity of social roles (Westin, 1967, p. 35). It also provides a theoretical foundation for Westin’s concerns about surveillance. He argues that placing people under surveillance is dehumanizing because “the person-to-person factor in observation – with its softening and ‘game’ aspects – has been eliminated” (Westin, 1967, p. 59). In Habermasian terms, surveillance is problematic because it is uncoupled from communicative interaction and an inter-subjectively generated understanding. It is, by definition, non-reciprocal; the actor’s actions and words are captured by the watcher without any opportunity for inter-subjective interpretation. Accordingly, Westin’s warning that the “reproducibility of speech acts” means that private communications may be taken out of context and used against the speaker can also be theorized by placing privacy at the core of communication. Once the statements are captured and used for instrumental purposes, they are removed from the intersubjectivity which grounds the identity.

Privacy and autonomy

Once privacy is cast as the boundary between the self and other, the boundary is internalized through the conversation of the socially constituted me and the emergent and therefore free I. Privacy so conceived is therefore essential to autonomy because it is a pre-condition of the undetermined nature of the I. For Mead, the self's response to the social environment is active, not passive. The "me" is the "conventional, habitual individual" (Mead, 1934, p. 197) which internalizes "the organized set of attitudes of others which one himself assumes" (p. 175) through taking the perspective of the other. However, the self is not totally determined by the "me" it encounters through social interaction, because the self retains a moment for a creative response, or "novel reply" (p. 197) to the attitudes of others. Mead calls this aspect of the self the "I".

The "I" is not known in the present as it is the self's undetermined response to the attitudes which the social self has taken from others. Accordingly, the "I" can only be known by the "me" after the self has exercised autonomous choice and become part of the "me's" memories. Mead writes, "If you ask, then, where directly in your own experience of the 'I' comes in, the answer is that it comes in as a historical figure" (p. 174). In this sense, the "I" becomes part of the "me" as the "symbolized object in our consciousness of our past actions" (Cronk, 2001). However, since the "I" emerging in the present implies a change in the "me" in the future, the "I" remains autonomous because it can only be determined after the change has occurred.

Mead's understanding of the self is further developed in his theory of temporality. He argues that temporality is created by the emergence of the unexpected event. Without the resulting disturbance, "there would be merely the passage of events" (Mead, 1938, p. 346); it is only when action is inhibited by the emergent that the present is separated from the future, and experience becomes possible. The emergent therefore constitutes a problem to be overcome through human action (Cronk, 2001). But it also poses a problem for reason. For Mead, reason is the search for continuity in experience. Since the emergent creates discontinuity, reason requires that its understanding of experience accommodate and explain the emergent event. In order for the self to do this, the "I" must remain bounded and set apart from the social self, since, if the "I" collapses into the "me", the "I" is no longer undetermined and autonomous of the attitudes of others which are internalized through the "me". Autonomy, therefore, is located in the boundary between the undetermined "I" and the generalized other.

If privacy is the boundary between self and other, then Mead's insights into autonomous action can potentially explain the relationship between privacy and autonomy which is so central to Westin's thinking. To develop this further, I now turn to Jurgen Habermas, who appropriates Mead's work to formulate a more complete explanation of the relationship between communication and democratic autonomy.

Applying Habermas to privacy theory

Privacy and communicative action

Habermas appropriates Mead's work on the self as social emergent in order to ground communicative rationality as an alternative to the instrumentalism of the systems world, to open up spaces for undetermined, autonomous action. Since language is embedded with notions of inter-subjectivity and reciprocity, the emergence of the self becomes a reflexive process in which the individual's understanding of the self moves from the concrete/particular to the abstract/general. Habermas argues that this progression from the particular to the general is a cultural trait of modernity, and that modern societies are marked by institutional differentiation and a proliferation of roles. Individuals are able to adapt to these conditions because, through communicative interaction, we move from an understanding of self and dominant others, to self and significant others, to self and general others (Winseck, 2001).

Habermas's conception of communicative action enables "mutual understanding, conceived of as a process of reaching agreement between speaking subjects to harmonize their interpretation of the world" (Deflem, p. 2). As such, Habermas's "post-metaphysical" conception of reason is not "an immediate source of prescriptions"; in other words, "it is not a subjective capacity that would tell actors what they *ought* to do." Rather, it "intersects" with normativity by making "an orientation to validity claims possible" (Habermas, 1999, pp. 4-5). This is central to Habermas's desire to reinvigorate the potential of reason to inform social

judgment, and articulate principles that will support democratic forms of discourse in modern conditions of increasing complexity without returning to the philosophy of consciousness.

To accomplish this, Habermas must extend the intersubjectivity contained within the relation to the self to a “level of intersubjectivity that is communicatively generated, consolidated in the medium of linguistic symbols, and secured finally though cultural tradition” (p. 10). Habermas argues that Mead fails to do this because he looks at taking the attitude of the other from one side only, the intersubjective relations contained within the relation to the self. However, symbolically mediated interaction can arise only if the causal relationship between stimulus and response is replaced by an interpersonal relationship between speaker and addressee in which both discursive participants can differentiate success-oriented actions from actions oriented towards reaching mutual understanding.

Accordingly, intersubjectivity grounded in language also has consequences not only for the self, but for the system as a whole: “This is not merely a question of the emergence of the relation-to-self that is reflected in itself ... It is a question of the emergence of a higher-level form of life characterized by a linguistically constituted form of intersubjectivity that makes communicative action possible” (pp. 9-10). The process of coming to mutual understanding therefore “makes possible a transition from symbolically mediated to normatively guided

interaction" (Habermas, 1981, p. 5). This, in turn, has consequences for Habermas's articulation of the "principle of democracy" (Habermas, 1999, p. 121), as discussed below in the context of private and public autonomy.

Although Habermas does not address questions of privacy in a comprehensive way, his appropriation of Mead has consequences for privacy theory. He argues that "meaning embodied in social action is something non-external; at the same time, as something objectivated in symbolic expressions, it is publically accessible and not, like phenomena of consciousness, merely internal" (p. 4). He then draws on the following paragraph from Mead: "There is a field within the act itself which is not external, but which belongs to the act, and there are characteristics of that inner organic conduct which do not reveal themselves in their own attitudes, especially those connected with speech" (Mead, quoted in Habermas, 1999, p. 4). This potentially links privacy theory to language theory because language becomes the bridge between that inner experience and the social nature of the self that is expressed through communication.

The boundary between self and other is implicitly addressed when Habermas examines the transition from the language of gestures to symbolic interaction. In order to explain how instinctual communication evolves into a language of meaning in the Meadian sense, he applies Wittgenstein's concept of rules which is, in turn, tied to Wittgenstein's famous argument that there can be no private language. Habermas accordingly imports the position that private experience

necessarily involves public expression – the a-social private can have no meaning because meaning is created only through linguistic interaction with another subject.

Privacy and democratic discourse

In addition, by importing Mead's distinction between the subjective and the social aspects of the self's private experience into his theory of communicative action, Habermas opens a door to explain how privacy as the boundary between self and others is implicated in democratic discourse. In many ways, Mead, Westin and Habermas address the same core issue – Mead is concerned about the potential for democracy in an era of mass communication, Westin hopes to maintain a democratic space at a time when technology is shrinking our experience of freedom, and Habermas seeks to reinvigorate the democratic project in the conditions of modernity. By appropriating Mead's insight that language "has constitutive significance for the socio-cultural form of life" (Habermas, 1981, p. 4), Habermas grounds socialization and social integration in language. However, Habermas extends Mead's analysis to explore ways in which a community of people can come to rational judgment.

Indeed, since the *Structural Transformation of the Public Sphere* was first published in 1962, Habermas has sought to develop a normative theory of democracy that is grounded in the participation of reasoning citizens (Bohman, 1994, p. 897). Although Habermas's project has been motivated by his belief

that the transformative potential of Kant's notion of procedural rationality (the ability to base judgment on reasons) has not yet been exhausted (Calhoun, 1999, p. 2), he is deeply aware that, as economic and bureaucratic systems have been uncoupled from the influences of the lifeworld, the ability of rational communication to shape modern life has been supplanted by the exigencies of the non-linguistic media of money, power and science. In *Between Facts and Norms*, Habermas applies the methodology of the "rational reconstruction" of democracy to combine normative and sociological analyses of contemporary social practices (Bohman, 1994, p. 913).

Because Habermas is seeking to develop a counterfactual which is grounded in both social facts and a moral perspective which can be maintained in a pluralistic society, he moves away from a social contract model of law and adopts a consensus-driven perspective based on a procedural understanding of communicative rationality. Unlike strategic action, in which actors see others as potential instrumentalities, communicative action is oriented to reaching a common understanding about the "rightness of the norms under consideration" (Rosenfeld, 1995, p. 1169). As such communicative action is embedded with the normative constraints of discursive practice: all actors are given an equal opportunity to present their arguments; all interests are considered as a precondition of reaching consensus; and there is a mutual commitment that the better argument will be the sole basis for persuasion (Habermas, 1999, pp. 3-4).

Accordingly, “actors engaged in communicative action would only accept as legitimate those action norms upon which all those possibly affected would agree *together* to embrace on the basis of good reasons” (Rosenfeld, 1995, p. 1169). As such, democratic participation in the legislative process provides the normative justification for the social fact of coercively enforced laws. This “principle of democracy” is derived from the “interpenetration” of communicative rationality and the legal form. Interpenetration occurs when the conditions for a “discursive exercise of political autonomy” are institutionalized in law as a “*system of rights*” (p. 121), including guarantees of private autonomy (i.e. negative liberties, rights of membership in voluntary associations, and legal rights of due process) and guarantees of public autonomy (rights of participation, and social welfare rights to ensure factual equality) (pp. 122-123). Indeed, the key to his proceduralist understanding of law is that “a legal order *is* legitimate to the extent that it equally secures the co-original private and public autonomy of its citizens; at the same time, however, it *owes* its legitimacy to the forms of communication in which civic autonomy alone can express and prove itself” (Habermas, 1998, p. 19).

Public and private autonomy are therefore central to the proceduralist paradigm. They are “co-original”, or “equiprimordial”, because they are mutually dependent, and exist in a circular relationship that is manifested through the process of legitimation:

... legitimate law emerges from, and reproduces itself only in, the forms of

a constitutionally regulated circulation of power, which should be nourished by the communications of an unsubverted public sphere that in turn is rooted in the associational network of a liberal civil society and gains support from the core private spheres of the lifeworld (p. 18).

In this sense, private and public autonomy both flow from Habermas's consociates' "commitment to each other as free and equal participants in a common life, a commitment which is both presupposed by and made possible by the legal order of the democratic ... state bound by the rule of law" (Dyzenhaus, 1996, p. 135).

Habermas's work on law, therefore, highlights the connection between privacy, autonomy and democracy, and mitigates against a legal model that frames privacy solely as a possession of an isolated individual. It also opens up questions about the meaning of autonomous action on the part of those participating in public dialogue, and the need for an autonomous sphere of action for private individuals outside of solitude. This resonates strongly with the human rights perspective, in which privacy is seen as a central element of human dignity and autonomy, and a key component of the democratic process.

Habermas has been criticized for producing a functionalist account of democratic discourse that focuses unduly on institutions. Honneth, for example, argues that his sharp distinction between system and lifeworld provides a reified account of the continual collective, interhuman struggle over identity, meaning and value

which occurs in social life. He concludes that the differentiation between system and lifeworld as two autonomous spheres of action in which these two principles of societal integration reside produces “two complimentary fictions ... (1) the existence of norm-free organizations of action and (2) the existence of power-free spheres of communication” (Honneth, 1991, p. 298). As a result, we are left with “purified ideal-types” of public and private spheres of action which are “stripped of the inherent ambiguity of real social life in which understanding and control are inextricably intertwined” (Feenberg, 1995a, p. 79). Similarly, Shallin has argued that Habermas has privileged consensus and determinancy over dissensus, indeterminacy and uncertainty, and accordingly lost Mead’s crucial insights into the value of experience (Shallin, 1992).

A proceduralist approach to privacy protection is limited, as demonstrated in Chapter Three. If privacy is a social value, then procedural rules such as fair information practices reify what is an ongoing negotiation between real social actors and accordingly privilege the a-social needs of the systems world.

However, Habermas’s discussion of law also points to the inter-subjective nature of both private and public autonomy. By extending Mead’s analysis beyond the emergence of the self to the system as a whole, he defines democratic action as inter-subjective. This has significance for privacy theory because it demonstrates that invasive practices weaken the conditions necessary for democratic discourse because they interfere with the boundary negotiation process which enables a subject to emerge.

More precisely, the instrumental collection of personal data conflicts with the democratic meaning of privacy precisely because the data creates an objectified self which is removed from inter-subjective dialogue. Unless the data is kept open to inter-subjective input and control, the data is concretized and alienated from the individual because the social context which gives it meaning is lost. The instrumental use of the data in those circumstances becomes an exercise in power, and autonomy is lost. As Habermas argues:

Under conditions of strategic action, the self of self-determination and of self-realization slips out of intersubjective relations. The strategic actor ... makes decisions solely according to the standards of subjective preference. He does not rely therein upon recognition by others.

Autonomy is then transformed into freedom of choice (*Willkürfreiheit*), and the individuation of the socialized subject is transformed into the isolation of a liberated subject who possesses himself (p. 192).

This “liberated subject who possesses himself” resonates with Westin’s model of the liberal individual who protects his privacy by social withdrawal and freedom of choice regarding the disclosure of his personal information. The first part of Westin’s definition, stripped of the sociality of the second part, accordingly privileges instrumentalism by recasting privacy as control over objectified data. This fails to capture the lived experience of privacy precisely because:

An ego-instance shorn of all normative dimensions and reduced to cognitive achievements of adaptation does indeed form a functional complement to the subsystems that are steered by media; but it cannot

replace the individuals' own socially integrative accomplishments, which a rationalized lifeworld expects of them (p. 197).

[and]

The decision structure required by media-steered subsystems misses the mark when it encroaches on the private and public core domains of the lifeworld. The independent performances that are here demanded from the subjects consist of something different than rational choices steered by one's own preferences; what these subjects must perform is the kind of moral and existential self-reflection that is not possible without the one taking up the perspective of the other (p. 199).

However, once privacy is rooted in language, it sits at the core of inter-subjectivity and self-reflexivity because it defines the boundary between self and other both externally and internally. As such, it cannot be traded off in exchange for some other benefit, like efficiency or convenience, and remains a flashpoint for social struggle because, as instrumental reason has become uncoupled from the lifeworld, the conditions necessary for inter-subjectivity have been negated through objectification of the self and the collapse of boundaries between social roles.

Privacy as a social emergent of communication

Applying a Meadian/Habermasian perspective to privacy then, allows one to conceptualize privacy within the context of the self as a social emergent of

communication. Altman argued that privacy is a boundary control mechanism that externally allows social actors to negotiate the boundary between self and other. However, through taking the perspective of the other, privacy is also internalized in the dialogue between self and Generalized Other because it is this dialogue that enables the self to become visible to itself and emerge through discursive interaction. Accordingly, privacy sits at the core of intersubjectivity and self-reflection. Privacy is no longer confined to solitude or procedural control over personal information; instead, it is inter-subjectively constituted through communication. This conceptualization captures the sociality of privacy as it is experienced in the life world because privacy is no longer reified but grounded in social interaction.

Accordingly, privacy can be conceived of as the boundary between the self and other which is negotiated through discursive interaction between two or more social actors. As such, it is a dynamic process which is exhibited by the core self *in social interaction with others*, as the self withdraws from others into solitude or moves from solitude to intimacy and general social interaction. Privacy is no longer juxtaposed against social interaction, as Westin posits, but is a potentiality throughout the full range of human experience. For example, an individual desiring low contact with others is able to obtain privacy through solitude. However, if others invade that solitude, the individual experiences a sense of trespass, as he or she is unable to negotiate the desired level of aloneness. On the other hand, as both Westin and Altman indicate, there is a difference

between privacy and isolation; the latter is experienced when the closedness to others is not satisfying to the self. Accordingly, the conception of privacy as social emergent captures the dialectical nature of privacy identified by earlier theory, without inappropriately collapsing it into solitude as Westin does.

This conception also allows us to better theorize the various privacy states that become possible as the individual leaves solitude and engages in social interaction. From the Westinian perspective, social interaction poses risks to privacy that must be managed by the individual by seeking to maintain control over the flow of his or her personal information. The onus of privacy protection therefore shifts to the individual in isolation of others, and the self is left to protect itself through extraordinary measures, much like *Kyllo* seeking to restrict the flow of his body heat to sensors outside his home. However, as Westin first noted, a multiplicity of privacy states become available as the individual becomes more open to others. If privacy is negotiated between social actors, then one can also identify a number of *invasive states*. This focuses questions of privacy protection on the quality of interaction between social actors (including the state and corporations) rather than the reified flow of information.

There are a number of negotiated states that potentially optimize the desired need for privacy as the individual becomes more open to others. For example, an individual who moves through public spaces in high proximity with others but who remains relatively closed to them can achieve privacy through anonymity or

reserve. Excessive crowding may impinge on these states but, as Westin's work indicates, societies that experience physical crowding develop psychological mechanisms to maintain social distance (Westin, 1967, p. 12), much like the Mehinacu man who shares a house with his mother-in-law but is socially forbidden from speaking to her (Altman, 1977, p. 79). Privacy is accordingly not dependent on physical separation but on the negotiated interaction between social actors.

Surveillance invades the individual's sense of privacy precisely because it identifies him when he wishes to move through public space free of others' recognition. More specifically, the lack of anonymity is perceived of as invasive when the watcher does not ignore what he sees but actively seeks to manipulate or control the watched. Accordingly, a surveillance camera in a bank that does not seek to identify customers is more readily accepted than police who take pictures of the faces of people who gather to hear a political speech or employers who use surveillance cameras in the street to record how long people spend smoking cigarettes during the workday. What defines each incident as invasive is the *social action taken by the other*. Anonymity is achieved when *others* agree to respect the individual's wish to remain unidentified. Anonymity, like all privacy states, is dependent upon the social negotiation of a desired boundary between self and other; it cannot be achieved by the individual in isolation. In like vein, an individual who expresses reserve feels invaded by those who fail to respect the social cues he sends and rudely pursue discursive

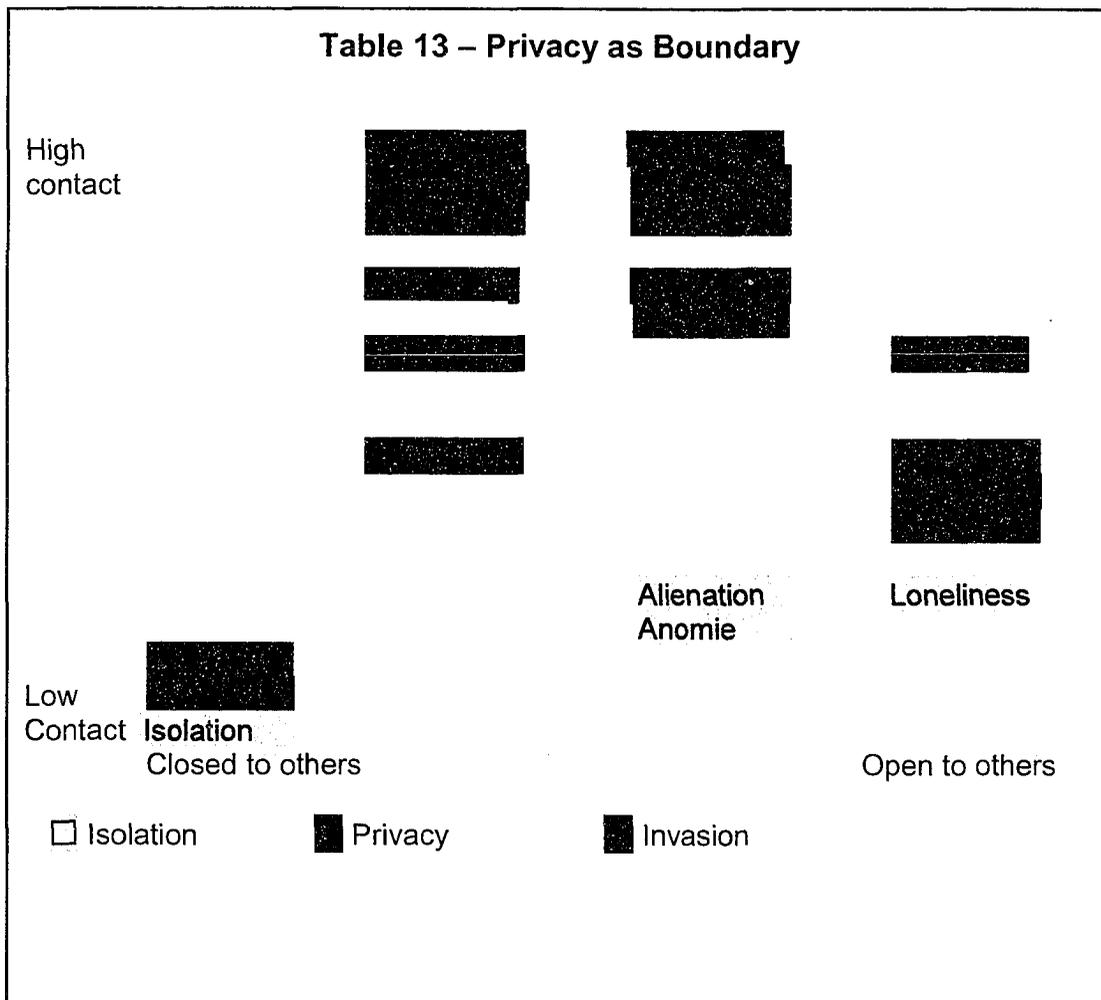
interaction which is too personal or exposing of the self.

As the individual becomes more open to others, she more willingly enters into public activities, including forms of civic participation. However, civic participation is also contextualized by a social agreement regarding the boundary between self and other. There is an unwillingness to accept surveillance in voting booths and public fora because, even though both involve participation in a public process, being watched in these circumstances severely restricts the individual's autonomy. Surveillance of both is perceived to invade the private citizen's democratic space, even though the latter takes place in public. Accordingly, there is an inherent connection between autonomy, privacy and democratic action. On the other hand, individuals who wish to participate in public activities but are unable to negotiate the desired levels of privacy and participation are subject to feelings of alienation and anomie.

The individual who is most open to others seeks interaction within relationships of intimacy. If there is too much contact with non-intimate others in these circumstances, the intrusion into intimate space is a privacy violation because it impinges on the boundary both between the self and unwanted others and between intimates and others. In other words, the intrusion of others into intimate exchanges interferes both with the inviolability of the exposed self and with the social interaction between the self and intimate other. Intimacy can be maintained within a broad range of contact levels precisely because others are

willing to withdraw from intimate interaction and allow intimates social space that recognizes their closeness, much as people do when they avert their eyes when romantic couples exchange a kiss. When the other does not withdraw, the intimates feel intruded upon. On the other hand, an individual seeking intimacy who is unable to enter into intimate interactions with others feels loneliness.

Conceptualizing of privacy as a social emergent of language therefore enables us to theorize the ways in which privacy states are negotiated throughout a range of social interactions, in situations of low to high contact with others, as Table 13 illustrates.



The task, as Westin makes clear, is to devise new legal rules that facilitate privacy throughout this spectrum by constraining invasion and opening up spaces for democratic discourse. Indeed, that is the intent of Westin’s legislative program, to provide policy makers with a framework to assess the social appropriateness of particular surveillance practices in order to protect democratic autonomy. Once the social elements in Westin’s thinking are grounded in a theory of privacy as a social emergent of language, the policy questions are no

longer trapped in an abstracted set of information practices. Instead, policy makers are called upon to assess the impact of invasive practices on the lived experience of privacy in the lifeworld and the exercise of democratic choice. The next chapter tests whether or not this approach can inform more effective privacy policy, by examining the ways in which corporate web sites collect children's information, and contrasting corporate practices with children's perception and use of online communications. I will evaluate whether or not a data protection response can provide an effective remedy for invasive practices, and contrast the kinds of solutions that data protection proposes with those remedies that flow from a broader understanding of the need to protect privacy because it is an essential part of identity formation and inter-subjective dialogue.

Chapter 6 – Testing the Framework: A Case Study on Children’s Online Privacy

They’re going to slap that baby’s bottom, then slip an ID chip in their neck or between their shoulders so you can keep track of your kid (Sun Microsystems’ CEO Scott McNealy, quoted in Vance, 2004).

In the early 1990s, Canada committed itself to networked communications in order to remain competitive in the emerging information marketplace (Canada, 1994; Manley, 1999). As part of that economic agenda, the federal government had wired every public school in the country to the Internet by the end of the decade (Manley, 1999). Remarkably, three years later, 73 per cent of households with children under 18 living at home were also connected to the Internet, a figure which is almost 20 percentage points higher than the number of Canadian households with an online connection (Statistics Canada, 2003). Over one-quarter (26%) of the children living in wired homes access the Internet using their own computer, as opposed to a communal family machine (CTF, 2003).

Canadian children are now among the most wired in the world¹. Shade, Porter and Santiago argue that, “For many Canadian families the Internet has quickly become a domestic utility, used alongside (and sometimes more than) television,

¹ Studies indicate that 99 per cent of Canadian children between the ages of 9 and 17 use the Internet regularly (MNet 2001b). American research indicates that younger children are also incorporating the Internet into their lives; as many as 35 per cent of toddlers surf regularly (American Corporation for Public Broadcasting, 2001).

radio and newspapers” (Shade et. al., 2004, p. 1). Parents have encouraged their children to use the Net because they believe that it will help them succeed at school and prepare for the workplace (Allen & Rainie, 2002; MNet, 2001a), but children overwhelmingly see the Net as a place to play and socialize (Gunter et. al., 2003; Kline, 2001; Abbott-Chapman & Robertson, 2001; MNet, 2001b). Typically, they are playing and socializing on commercial sites. And one of the “defining characteristics” of these sites “is that personal information is aggressively collected from users, both directly and surreptitiously” (Steeves & Tallim, 2003). Given the invasive nature of many of these sites, public interest groups began to call for regulation to protect children’s online privacy as early as 1996 (Montgomery, 1996; Linn, 2004, pp. 200-201).

This chapter provides an overview of the ways in which privacy-invasive practices are incorporated into commercial web sites targeting children, and contrasts corporate practices with children’s perceptions and use of online communications. I begin by examining the types of information practices commonly used by online marketers by surveying sites which have been identified by children and youth as “favourites” (Shade et. al., 2004; Fillion, 2003; MNet, 2001b; Montgomery, 1996, 1999). I use examples drawn from these sites to illustrate the ways in which the collection of personal information structures children’s online play spaces. The methods of collection I discuss have been documented in a series of reports published by the Center of Media Education, including *Web of Deception* (Montgomery, 1996), *CME Assessment of Data*

Collection Practices of Children's Web Sites (Montgomery, 1999) and *teensites.com* (Montgomery, 2001), and are representative of the ways in which children's personal information is collected for commercial purposes. I then examine how data protection principles have been implemented to protect children from online invasions of privacy, and assess their effectiveness in dealing with the policy concerns raised by these practices. Lastly, I analyse whether or not the communication-based understanding of privacy articulated in Chapter Five can provide a stronger basis for effective policy in this context.

I argue that data protection principles are ineffective in protecting children's online privacy because consent-based mechanisms are easy to circumvent and fair information practices fail to take young people's experiences and social needs into account. By focussing attention on procedural rules, data protection also constrains the potential for a broader debate on the social value of aggressive online marketing to children. A communicatively based understanding of privacy reopens this question, and enables policy makers to examine the impact of marketing practices on children's identity formation and social relationships. This perspective reinvigorates Westin's full legislative programme, and reconnects questions of privacy policy to the formation of public judgment in the lifeworld.

A snapshot of children's online environment

The following analysis indicates that the child's online environment is structured by commercial imperatives which have been built into the sites they visit and the functionalities they use. Children typically select commercial sites when they seek to play or socialize online. For example, when asked to identify their favourite places on the Net in surveys, children have consistently listed commercial sites (Shade et. al., 2004; Fillion, 2003; MNet, 2001b; Montgomery, 1996, 1999) such as:

- newgrounds.com (gaming site)
- addictinggames.com (gaming site)
- shockwave.com (gaming and movie site)
- candystand.com (branded gaming environment - Lifesavers)
- neopets.com (virtual pet playground)
- Barbie.com (branded virtual playground - Matel)
- Sponge Bob Squarepants (branded playground - Nickleodeon)
- alloy.com (teen enterainment environment)
- bolt.com (entertainment site for teens)

These sites have been highly successful at attracting and retaining a large audience of young people. Candystand, for one, is popular with children between the ages of 9 and 17 (MNet, 2001b). All of the games and contests on this site feature Lifesaver products. Children playing Mini Motocross, for example, select an avatar named for a Lifesaver flavour and get bonus points for picking up Lifesaver candies throughout the race.

Corporations create Web sites for children for a number of reasons. Since the Net is a public medium, these sites provide marketers with a unique opportunity to watch children as they play and record their actions. Now that children conduct their private lives on a public network, “their interests, their preferences, their behaviour and their most intimate communications are monitored, collected, and sliced and diced for someone else’s profit,” in effect turning the Net into a continuous feedback loop for market research (Steeves & Tallim, 2003).

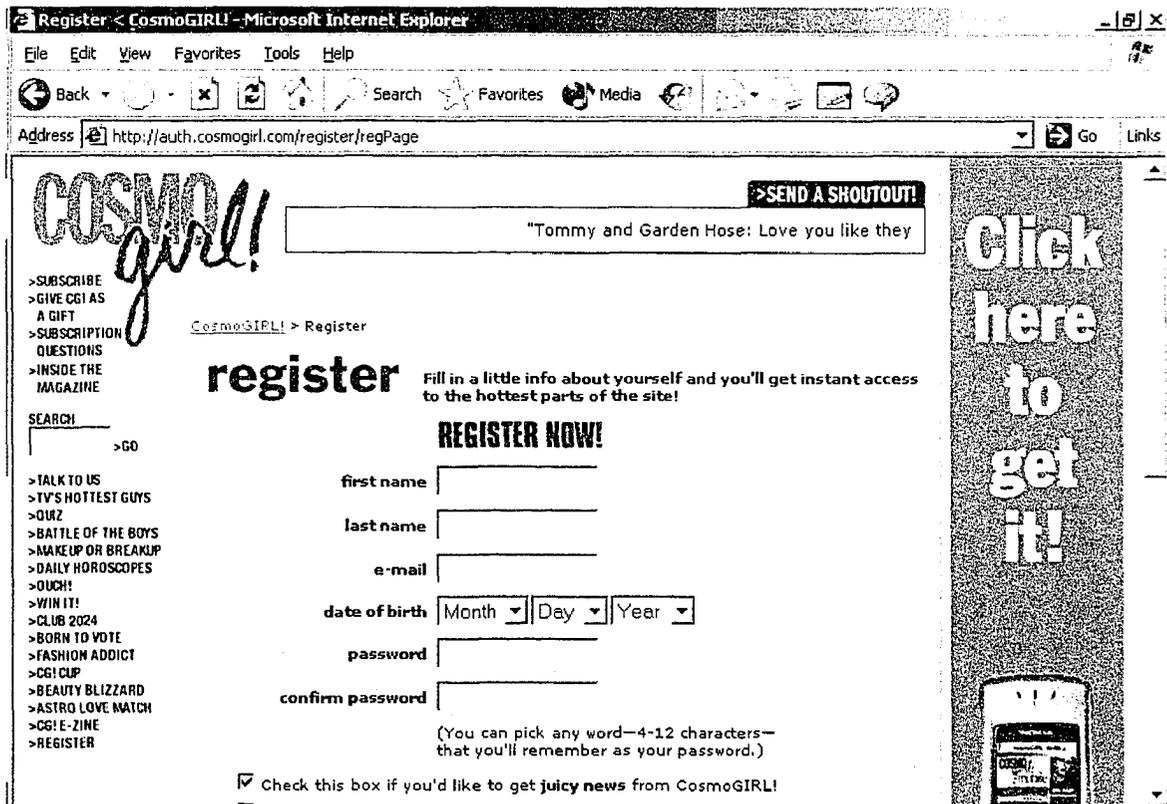
Children are the ideal target for this type of surveillance because they stay online for longer periods of time, they are more likely to access the Net from a variety of locations, and they participate in a wider range of online activities than adults (Forrester Research, 1999). In addition, by building brands into play environments, marketers create what they call “sticky traffic”; unlike traditional advertising, which retains the reader’s attention only for a short time, children will play with branded products for extended periods, exponentially increasing the ad’s impact.

Corporations are also interested in children because they exercise a great deal of spending power. YTV’s annual Tween Report indicates that Canadian children between the ages of nine and 14 spend a total of \$1.7 billion per year of their own money, and influence approximately \$20 billion per year in family spending (YTV, 2002). Corporations seeking to capitalize on this market create web sites that offer games, quizzes, chat environments and advice, in order to encourage children to provide them with personal information which can then be

used to target the children with advertising. Typically, these children's sites play into their developmental needs in order to encourage kids to talk about themselves (Linn, 2004, p. 24). For example, research indicates that older children use the Net to obtain independence from parents and family, to communicate with their peers, to try on new identities and to express their opinions, so commercial sites provide plenty of opportunities to do so (CME, 2001). Girls are particularly attractive to marketers because, unlike boys who use the Net primarily for entertainment recreational purposes, their online use patterns predispose them to communication, sharing, and expressiveness (Brunet et. al., 1998).

Many popular girls' magazines, including *Seventeen*, *Cosmogirl*, *Teen* and *YM*, publish an e-version. The e-magazines mirror much of the content of the real world versions – horoscopes, contests, and articles on beauty, fashion, dating and celebrities – and offer opportunities to interact and communicate, through chat rooms, hotlinks to advertisers, online shopping links, advice columns and email. The public nature of the Net means that the publishers can monitor the teens that come to the site and record their interests, preferences, communications and behaviour, creating a continuous feedback loop for market research. But to maximize the value of the information they collect, the magazines encourage the children to identify themselves by providing personal information. For example, *Cosmogirl* urges them to, "Fill in a little info about yourself and you'll get instant access to the hottest parts of the site!".

Illustration 1 – Cosmogirl Registration Page



Many of these sites, like Emode.com², use personality tests to collect information from, and market to, individual girls. These quizzes ask detailed questions about the child's personality, preferences, hopes and aspirations. Since children have to register with the site before they can access the quizzes, the marketer is able to record the child's responses linked to his or her first and last name, zip/postal code, email address, gender, marital status (and whether he or she has children) and level of education. This information can also be matched against the data trail that the child generates as she surfs through the site, selecting articles, chatting online about boys and playing games.

Emode also uses the information they collect to target girls with personalized advertisements. For example, after 14-year old Jenna took the "Ultimate Personality Test," she was told she values her image so Emode recommended that she visit e-diets, one of their advertisers, to "prep her body for success" (Steeves & Tallim, 2003). Although many corporations, like Emode, use media stereotypes to reinforce social messages about body image and gender roles (Signorelli, 1997), the affect of these stereotypes is "magnified in a surveillance environment that enables marketers to embed them in personalized communications with an individual child" (Steeves & Tallim, 2003).

Neopets, a popular site among young girls, uses empowering language to

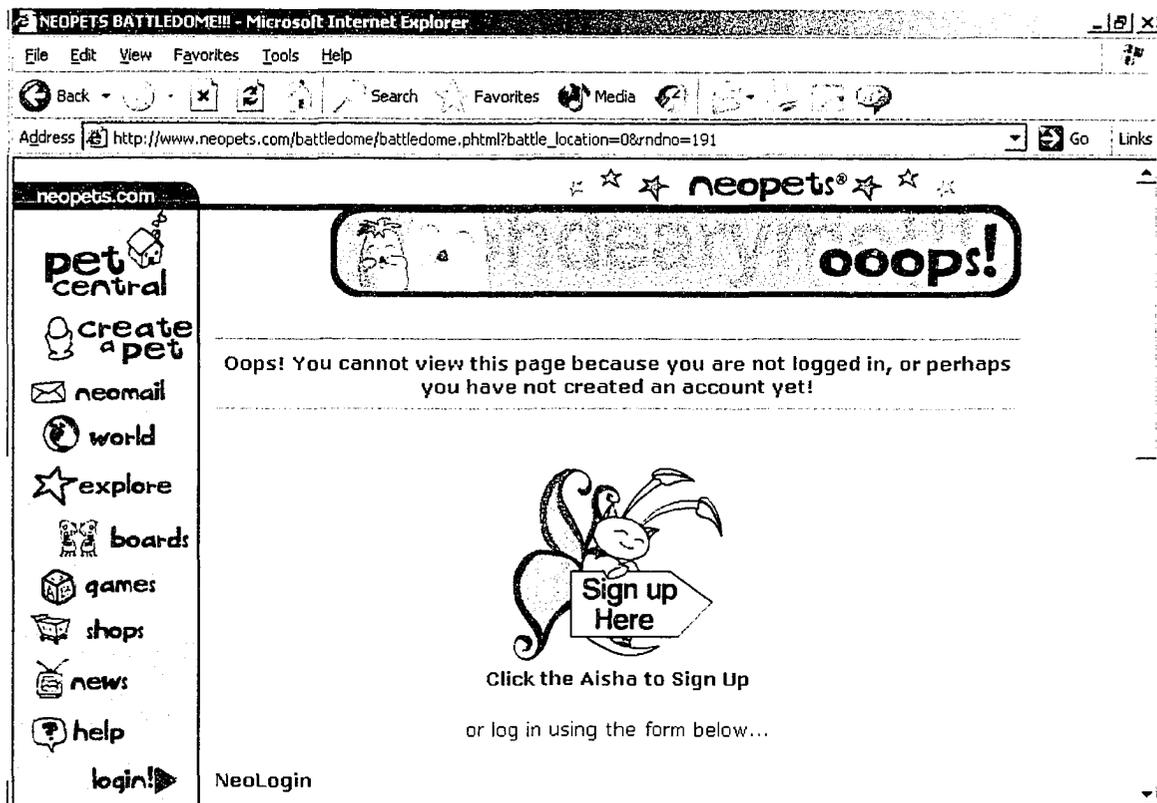
² Emode has since been taken over by Tickle, an online social environment for teen girls, with quizzes, dating information and chat areas.

encourage children to fill out market surveys and earn Neopoints, so they can buy things for their virtual pets: “You will be able to tell the producers, designers, etc., what should be improved, what sucks, what’s great and actually make a difference!” One survey posted in 2002 focussed on food, and asked kids about their:

- favourite chocolate bars and cereal brands;
- breakfast habits;
- name, age, gender and email address;
- education level;
- country and zip code;
- ethnic background; and
- Internet use.

It also asked children to select things that interested them from 60 items, including gambling, beer and liquor (Steeves & Tallim, 2004).

Illustration 2 – Neopets Registration Reminder Page



Like other children's sites, Neopets encourages users to identify themselves. If a child tries to access a game or a contest without registering on the site, he or she will be told, "OOPS! YOU ARE NOT LOGGED IN! You are not currently logged into Neopets, so you will NOT be able to earn any Neopoints for playing this game (but it'll still be fun!) Either Log In, or Sign Up with Neopets and you can start earning Neopoints straight away!" The site tells kids registering is "simple, fast and FREE!", although the sign-up process involves accepting Terms and Conditions³ that are 18 screens long, and the default setting on the sign-up form commits them to installing "GloPhone, so I can call anyone, anywhere for Free (GloPhone to GloPhone) right from my computer. Get 500 NP [Neopoints] for signing up!" Children are also encouraged to sign up for Return Path: "Who might be looking for you at your old e-mail address? Stay in touch with friends at your current e-mail. Enter your old e-mail address to register for Return Path's free service. Get 250 NP for signing up!" Return Path (2004) is a corporation that helps email marketers "[navigate] the ever-changing email landscape. Our solutions protect brands, increase efficiency, and improve results... Return Path helps you [the email marketer] increase ROI [return on investment] by continually improving your email communications."

The seamless blend of commercial content, entertainment and play in the child's

³ The Terms and Conditions protect the site's copyright, prohibit children from selling their Neopets or Neopoints to others or profiting from the site in any way, and set out acceptable use conditions concerning language etc.

online environment also provides an opportunity to disguise marketing as empowerment. The zip4tweens site is designed for “‘tween’ kids - not quite teens but definitely not children!” and tells its visitors that, “We're here to help you have fun - and build a strong mind and body.” In the Parents Section of the site, it states, “The zip4tweens.com Web site is designed to help tween girls (about 8 to 12 years old) see the value of eating smart and being physically active. Content and activities on the site can also help them feel good about themselves and confident in what they can accomplish both physically and mentally”. But if you read the fine print, you see that the site is owned by the Cattlemen’s Beef Board, the National Cattlemen’s Association and Circle 1 Network. The Circle 1 Network:

... specializes in marketing to kids and tweens, and marketing to families through interactive strategies including educational games, games for kids, online promotions, edutainment and advergaming. We publish properties for kids of all ages, teens, tweens and parents that help with reaching and advertising to kids, and we help develop kid advertising (Circle 1 Network, 2004).

The site is clearly a marketing tool designed to create product loyalty among girls who have embraced vegetarianism in record numbers⁴. As tweens talk together

⁴ Girls Incorporated (1994), an American non-profit youth organization, tells the girls who visit its site that, “Vegetarianism is no passing fad. According to the Vegetarian Resource Group, the number of vegetarians is on the rise. In fact, the organization estimates that one million school-age kids have adopted a meat-free diet!” Girls Inc. Encourages girls to “make an informed decision”, and identifies non-meat sources of iron and protein.

about “popularity, dating, and more” in the chat areas, play games like “Burger Boggle”⁵ and “Grillin’ and Chillin’”, or “go to the party zone to make invitations for [their] next burger birthday bash,” they are surrounded by marketing messages about beef. For example, ZIP (which stands for Zinc, Iron and Protein) is the only game on the site that does not incorporate images of hamburgers.

However, girls must answer trivia questions such as, ““Which of the following is one of the best dietary sources of iron? (A) Beef (B) Metal (C) Crunching on tin cans (D) Cotton candy.” If the child clicks on (B), (C) or (D), the program laughs. After the child selects (A) for beef, the screen flashes, the program plays exciting, prize-winning music, and the child advances to the next level of the game. When the game is over, the child is told:

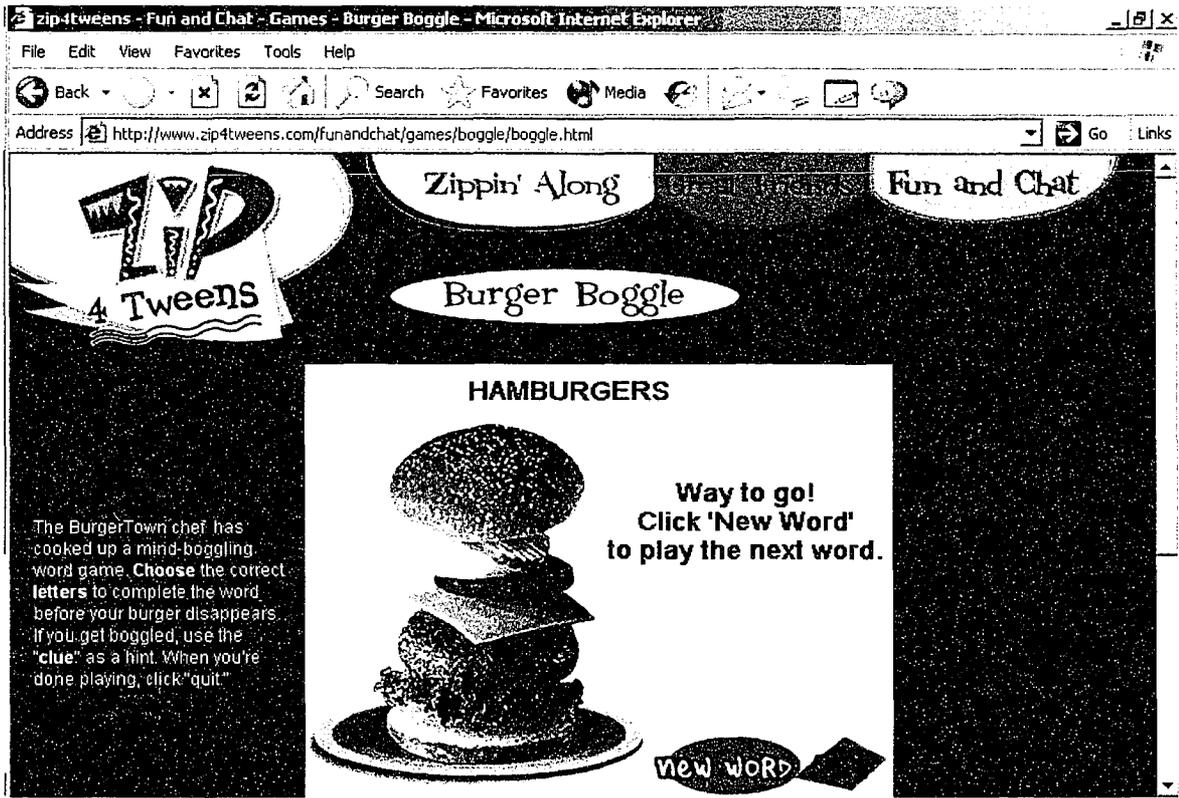
Now that you've conquered the Zonks by energizing the Zips, how about giving yourself more energy? Did you know that the nutrients contained in the foods you eat give you energy? Who wants to be tired all the time - so, think energy when *choosing your favorite foods, like tacos, spaghetti and hamburgers*. Next time you're looking for something to eat, think about foods that give you these key nutrients: Zinc, Iron and Protein (emphasis added).

Beef tops the list of preferred foods in each category.

⁵ Burger Boogle is a Hangman-type game where kids spell out words like “Kebobs” and “Hamburger”. Incorrect answers mean you lose a layer of your hamburger.

In like vein, the site's Smart Eatin' section provides 17 recipes for things like Beef on Bamboo and Easy Beef Chill. Fourteen of the recipes feature beef or dairy products; the remaining three are fruit, salad or tomato-based recipes and do not include any competing meat products, like chicken or fish. In the Smart Eatin' section Swap Out of the Ordinary, kids are told, "After the millionth tuna sandwich for lunch, turn to lean beef instead! Beef has nutrients like zinc, which improves your memory and helps you grow. Just three ounces of roast beef has the same amount of zinc as almost 35 ounces of canned tuna!" The section also advises them that people who think turkey has less fat than beef are wrong, and chicken provides less zinc, iron and vitamin B-12 than beef.

Illustration 3 – zip4tweens Burger Boogle Game



Online marketers, like the Beef Board and Circle 1 Network, typically encourage children to play with products in order to create a “personal relationship” between the child and the product. This is particularly true of brands (Lindstrom & Seybold, 2003). The Barbie site provides girls with an opportunity to design and dress their own Barbies, do a Barbie make-over, sing along with Barbie as she sings “Friends like we are” to the child, or “Make Happy Family Memories” with the Barbie’s “friends” Alan, Midge, their son Ryan, Midge’s parents, and Midge’s new baby⁶ (who the child gets to name when she fills out the Birth Certificate). The site actively encourages girls to buy Barbie products. For example, each child can record their purchasing preferences in their “Wish list”, and email it to their parents. As Barbie says:

Making your wish list is easy and fun! Here’s how to do it:

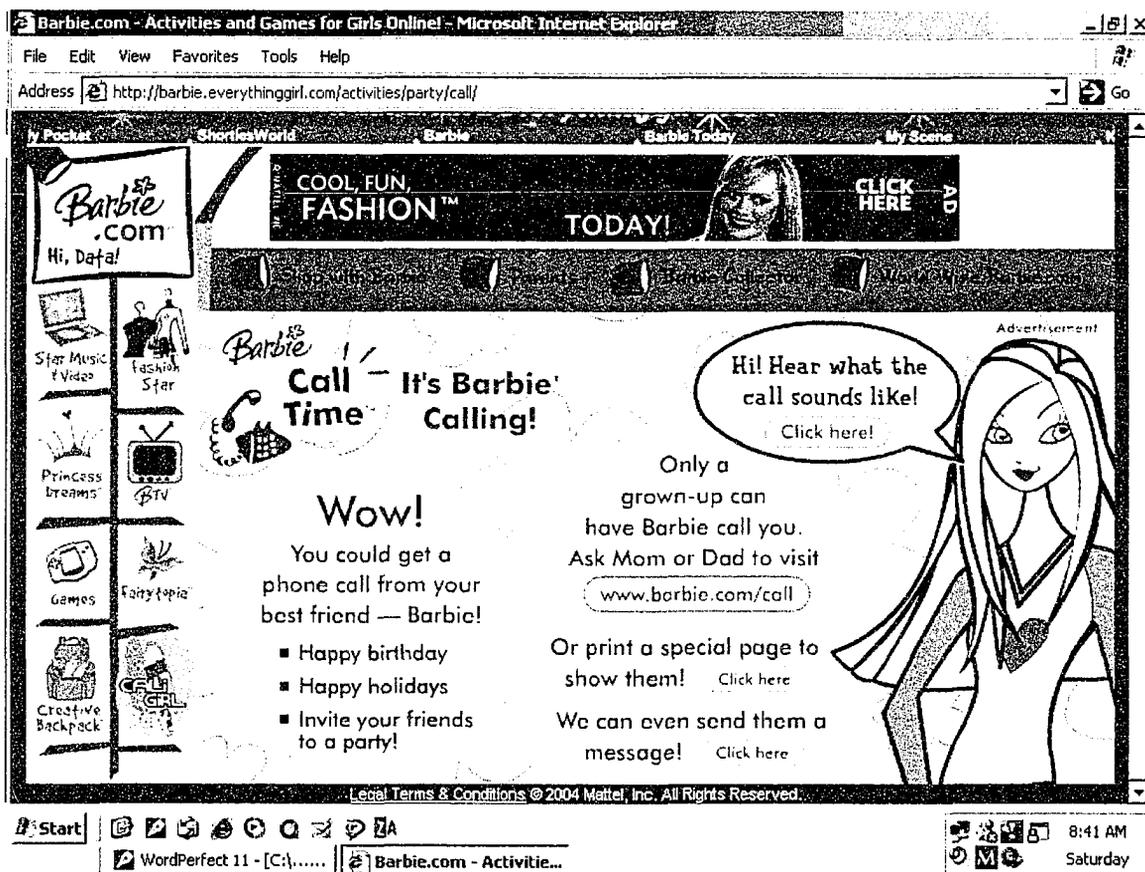
1. Click Shop Now! To check out the cool stuff in Shop with Barbie.
2. When you see something you like, click to add it to your wish list.
3. When you’re done shopping, print your wish list, email it to family or friends, or save it for later.

The site also embeds trailers for the latest Barbie movie, and tells girls, ““If you had [the doll version of movie character] Serafina now, you could hear her talk and meow!” But the site incorporates more than a sales pitch – it reinforces the “friendship” between the child and the brand itself. After taking a car trip into the city to help Cali (a doll) get ready for a party, the screen tells her, “We’re totally

⁶ Alan, Midge, Ryan, the grandfather, the grandmother and the baby are all available to purchase. Alan, Midge and Ryan are registered trademarks.

glad your chillin' with our Cali girl crew!" For \$1.99 (US), Barbie can also call the child directly on the phone. The site tells girls, "Wow! You could get a call from *your best friend-Barbie!*" (emphasis added). For American Thanksgiving, Barbie tells the girls in audio, "Hi! It's Barbie! I think this is such a special time of year. Don't you? I've got a wonderful wish for you. I'd love to call you and tell you! Or just say Hello. Ask your mom or dad if it's okay. Oh, I hope to talk to you soon!" Barbie will also call to wish them Happy Birthday, invite their friends to a party at their house, or tell them a bedtime story. Through interacting with a product in a web environment, children learn to "trust" brands like Barbie and consider them their "friends" (MNet 2001b, 2003).

Illustration 4 – Barbie Call Time Page



Advergaming sites like Barbie.com that encourage children to play with branded products have proven to be an excellent way to engage young people. Forrester Research projects that the advergaming industry will be worth over \$1 billion per year by 2005 (Steeves & Tallim, 2003). But branded game environments are not restricted to dolls and candy. Many advergaming sites seek to create product loyalty between children and adult products, such as cars, gambling and alcohol. Lifesaver's Candystand, for example, includes Video Poker and Poker Puzzler. In the first, children bet credits on hands which are dealt in a slot machine environment. When they win, they hear the sound of coins clinking as the number of credits increases. Poker Puzzler is another casino-style game. The cards are dealt onto a casino table and the computer plays lounge music while the children play. When they win, they hear slot machine sounds.

Beer.com is an industry site designed to create product loyalty for beer in pre-teen and teenaged boys. It combines games, music, sports, party talk, chat and advice with erotic, sexualized images of young women. Like sites aimed at girls, Beer.com tells boys to, "Join now and get access to the best on the Web for free! The Pub Club is where we keep Beer.com's premium content. You'll find beer.com's famous Beer Girls, contests, incredible features, the best beer ads and other awesome vids. And when we create something unbelievably cool, you'll find it in the Pub Club." Encouragements to join up are embedded in the site. For example, visitors are advised to, "Log-in to see two girls kissing and a bunch of other kickass beer ads." To register, users provide their name, email

address, age, gender, country, and zip/postal code, and answer the question, “How many beers do you drink per week?” by selecting 0, 1 to 2, 3 to 6, 7 to 12, or 13+. If teens under 18 try to register, they are advised that, “You must be of legal drinking age to join.” However, simply changing the birth date on the registration form allows them to complete the registration process, even though they have already identified themselves as underage users.

Like many other sites targeted at teens, Beer.com offers advice to its visitors. The Center for Media Education reports that just under half of teen sites include interactive advice columns, because teens are often seeking opportunities to learn more about issues that interest them and to discuss their problems without fear of being exposed to those people in their immediate social circle (Montgomery, 2001). In Beer.com’s advice column on sexual fantasies, their sex expert, Dr. Date, advises young men to select from the list of “Top Ten Female Fantasies”, including “sex with a stranger ... male dominance, lez action, offering sex for hire, guy-guy threesome [and] being taken”. As Dr. Date encourages boys to incorporate these fantasies into their dates, she assures them that, although girls fantasize, they don’t “have the courage to do it for real”.

Illustration 5 – Beer.com Home Page



The highly eroticized or soft pornography images used on Beer.com are not uncommon on sites targeted at older children. A growing number of mainstream marketers use erotic pictures of young people to sell product. Abercrombie & Fitch is perhaps the most notable. Michigan Attorney General Jennifer Granholm has called its clothing catalogue "Playboy for kids". The Christmas 1998 Quarterly featured teens undressing each other, four girls in bed with a male holding his boxers, and a nude teen girl riding an elephant. It also contained recipes for alcoholic drinks in an article entitled "Drinking 101", but the article was removed after protests from Mothers Against Drunk Driving. The Spring Break 99 Quarterly included a centerfold of a nude boy and girl carrying a surfboard, a picture of a topless girl suggestively embracing another girl, and three nude boys on the beach. The 2003 Christmas Quarterly featured a series of pictures of a large group of nude young people by a river, illustrating stories on group sex. One article argued, "A pleasant and super safe alternative to [group sex] is group masturbation - sometimes called a circle jerk or Jack-and-Jill-Off." Another article, the A&F "sexpert" column, included advice on "sex for three" and told readers that "go[ing] down" on a date at the theatre is acceptable, "just so long as you do not disturb those around you". A companion column compared the difference between sleeping with young school girls and having sex with women to the experience of biting into "fresh apple right off the tree" as opposed to the "store-bought variety that sit on the shelf wrinkled and bruised from the handling" (WorldNetDaily, 2003).

Children report that pornography, gambling and alcohol marketing is so prevalent, both online and off, that it forms the wallpaper of their lives in both their public and their private spaces (MNet, 2003). However, there is a dearth of research on the effects of immersing children in this material. The Australia Institute reports that 80 per cent of 16 and 17 year old boys visit hard core pornography sites, and argues that exposure to pornography “will inform young men’s belief that it’s okay to pressure a girl into sex ... in particular taking up sexually aggressive and sexually harassing behaviours” (Flood & Hamilton, 2003). The Japanese National Police Agency reports that the geometric growth of teens using online dating sites between 2001 and 2002 led to a 300 per cent increase in child prostitution, a 15 percent increase in child rapes and a 313% increase in blackmail. Eighty-six percent of the victims were children (Kioka, 2003). Since 95.6 per cent of the criminal cases arising out of dating sites involved the use of an i-mode cell phone⁷, plans to build global positioning satellite (GPS) capability into cell phones world-wide poses special risks to children.

The online environment has also generated some disturbing behaviour on the part of some teens, particularly those who commodify themselves in exchange for gifts or money. Cam girls⁸ post photos of themselves on the web and then

⁷ These cell phones can access the Internet through a wireless connection. In Japan in 2002, there were 3,401 dating sites which were accessible through an i-mode cell phone, compared to 2,038 which were accessible by PC (Kioka, 2003).

⁸ And some cam boys, though the vast majority of sites involve girls.

ask online admirers to send them gifts from wish lists posted on sites like amazon.com and MSN. In 2001, cam kids participated in a contest called Survivorcam where girls, some claiming to be as young as 14, competed by performing tasks in front of their cameras. The Survivorcam motto was: "Outpose. Outshine. Outwhore." Fifteen year old Brandi, who called herself "an underaged piece of ass" on her cam site listed 4 Sailor Moon dolls on her wish list (Mieszkowski, 2001).

Invasive marketing practices and the commodification of children's social spaces have generated public debate for the past four decades⁹. In the mid 1990s, public attention became focussed on the issue on electronic marketing databases after a number of investigative reports demonstrated how easily strangers could buy information from marketers to locate individual children¹⁰. In 1996, the Centre for Media Education (CME) published its report, *Web of Deception: Threats to Children from Online Marketing* (Montgomery, 1996). The report documented, for the first time, the types of privacy-invasive practices embedded in commercial web sites targeted at children. The CME argued that young children cannot differentiate between online content and advertising, and

⁹ As Linn notes, debate around online marketing is contextualized by the broader movement to regulate children's advertising as a whole. This movement began in the 1960s and continues today (Linn, 2004, p. 200).

¹⁰ In December, 1995, CNN reported that 900-number locator services could be used to determine the physical location of individual children. In May of the following year, the San Francisco Examiner published a story about how a Los Angeles television station purchased the names and addresses of over 5,500 children living in Pasadena from a Chicago-based marketing firm for \$277 even though the TV reporter identified himself by the name of a notorious child killer (EPIC, 2003).

do not understand the consequences of revealing their personal information to marketers. Accordingly, the CME called for regulation to protect children's online privacy.

Children's experience of online privacy

However, a closer examination of children's online behaviour reveals a more complex set of dynamics. Typically, early research concluded that children do not care about their online privacy, since they are willing to give away personal information to win a contest or join a club (eg. Montgomery, 1996; MNet, 2001b). However, recent studies have indicated that online privacy is an active concern for children, particularly in the context of their social relationships with concrete others in their immediate social networks. Livingstone and Bober surveyed 1,511 British children aged of nine and 19 and concluded that, "While often naive about threats to their privacy from external sources, children are fiercely protective of their privacy in relation to their parents" (Livingstone & Bober, 2003, p. 4). Two thirds (69 per cent) of the survey participants said they minded if their parents restricted or monitored their Internet use, and report taking steps to protect their online privacy from family members:

- 38 per cent had deleted emails so they could no longer be read;
- 38 per cent had closed or minimized a Window when someone came into the room;
- 17 per cent has deleted the history file in their browser;
- 17 per cent had deleted cookies files;

- 12 per cent had intentionally misnamed or hidden a file; and
- 12 per cent had used another person's password without permission in order to avoid exposure (p. 46).

Qualitative interviews found that children equated online monitoring by their parents to having their pockets searched or being stalked (Livingstone & Bober, 2003, p. 26). Older teens especially reported that they had a right to their privacy and their privacy should be respected: "You don't want your mum spying on you and knowing everything about you," and "Because you want your independence, really, you don't want your mum looking over your shoulder checking what you're doing all the time" (p. 27).

Children consciously choose media in order to regulate their privacy and manage their relationships with others (Livingstone & Bober, 2004; Oksman & Turtianinen, 2004; MNet, 2003). Abbott-Chapman and Robertson's study of Australian teens found that young people's online and offline activities focus mainly on "friendship building in the immediate locale" (2001, p. 485), and Gunter reports that the Internet has emerged as an important way for kids to stay in touch and gossip with family and friends (Gunter et. al., p. 203). Particularly because networked communication removes children from embodied, face-to-face interaction, children feel a greater sense of control over how they present the self to others within their immediate social network when they use mediated communication such as text messaging (Oksman & Turtianinen, 2004) or instant messaging (Shade et. al., 2004). Shade reports that MSN makes children feel

more confident and is perceived to be “less scary” (p. 15) than other forms of conversation. Oksman & Turtianinen note that, “A less than successful attempt at this type of communication can easily be passed over by referring to the playful quality of text messaging thus, to employ the Goffmanian term, elegantly withdrawing from the stage” (p. 326). Livingstone’s work supports this conclusion; she reports that “talking in a private online space enabled friends to be more open with each other, an important factor in girls’ friendships. Face-to-face communication, in this context, is too visible and, thus, subject to peer pressure” (Livingstone & Bober, 2003, p. 18). For both boys and girls, the Net creates “a protective distance which enables them to think more about what they are going to say and avoid embarrassing situations that would occur on the telephone or face-to-face” (p. 19). Accordingly, children prefer to use email to exchange secrets because it is more private since no one can overhear the conversation (p. 18), and text messaging is considered to be as private as a letter for the same reasons (Oksman & Turtianinen, 2004, p. 326).

Children’s construction of online privacy is also implicated in the development of their sense of identity. Teens in particular seek out private spaces “in which to withdraw and reflect [and] ... for safe seclusion or group activities with close friends as part of the process of construction of self as a reflexive and symbolic object” (Abbott-Chapman & Robertson, 2001, p. 485). Their use of media is dialectical, and intricately involved in identity formation (Steele & Brown; Oksman & Turtianinen, 2004). Indeed, children report they consciously “pretend to be

someone else” (Livingstone & Bober, 2003, p. 16) online in order to “try on” different identities and to gain access to an otherwise closed adult world (MNet, 2003).

An empathic reading of children’s online experiences of privacy therefore supports a Meadian framework that explains privacy as a dynamic boundary mechanism that is an essential element of identity formation and inter-subjective communication. Young people’s sense of privacy is inherently social; they do not experience privacy in an abstract way, but feel invaded if and when their concrete interests in self-expression and social interaction are at stake within the context of their relationships with others in their immediate social networks. This is not dissimilar from adults who typically do not react to unreflexive monitoring of their behaviour until the invasion become visible, as it did in the case of the Canadian government’s Longitudinal Labour File. Once the invasion becomes concrete, it steps out of the background and people take action to reassert a more comfortable boundary between self and others.

A Habermasian framework also sheds light on the ways in which children accept commercial surveillance while actively and vigorously opposing invasive behaviour on the part of the adults in their lives. Habermas appropriates Piaget’s work on human development when he argues that people move from the concrete/particular to the abstract/general as identity is formed. Younger children are accordingly developmentally more attuned to the actions of concrete

others within their immediate social experience; and, as children age, they become more aware of privacy in the abstract. For example, older teenagers prefer to talk face-to-face because they recognize that real world communication is, in fact, more secure than online communication. In order to avoid being “spied” on, they do not participate in intimate exchanges in open media:

Hazel [age 17]: If you wanted to have a private conversation, then I’m sure you’d talk to them face-to-face rather than using the internet, because if you know they can be listened to, or someone else can see what you’re doing, then I wouldn’t have thought that you’d want that to happen. So you’d therefore talk to them, meet up and talk to them face-to-face.

Stephanie [age 17]: Exactly. ‘Cause that friend could be with someone anyway. Or they can cut and paste ytour conversation into someone else’s internet conversation. So that is – *I don’t think anyone would be that silly to discuss their private [life] on MSN* (Livingstone & Bober, 2003, p. 19, emphasis added).

As children mature, then, they are more likely to develop an abstract understanding of privacy, although, as Shade (2004) and Livingstone (2004) point out, this in part depends on being educated about the nature of the online spaces they inhabit.

There is also some evidence that an awareness of constant monitoring makes children more fearful that those in authority will deny them privileges. Children in

Canada report that they worry that pornographic pop-ups will be recorded by school and home monitoring software and, in spite of the fact the pop-ups appear through no fault of their own, they will be unable to convince parents and teachers of their innocence (MNet, 2003). This may have implications for their exercise of autonomy as citizens in the future by predisposing them to self-censor in order to avoid repercussions on the part of those in authority.

However, others report that young people are often confident that they can avoid detection by “outsmarting” adults who are seeking to control their online behaviour (Livingstone & Bober, 2004). In this way, they continue to renegotiate the boundary and reassert their privacy in the context of their interactions with both concrete and abstract others.

The data protection response

Legislative responses to invasions of children’s online privacy have typically failed to explore the social context of children’s online lives. For example, American legislators began to look for a legislative response shortly after the CME report was published. However, from an early point in their inquiry, the issues were redefined in data protection terms, and questions about the potential harm that flows from commercializing child’s play were dropped from the debate. When the Electronic Privacy Information Center¹¹ (EPIC) testified before Congress in September 1996, they called for the introduction of fair information

¹¹ EPIC is a Washington-based public interest research centre that lobbies for the protection of privacy, free speech and constitutionalism.

practices, arguing that “current practices, which ignore standard privacy procedures followed in other industries and other market sectors, pose a substantial threat to the privacy and safety of young people” (EPIC, 1996). The CME supported this approach as well (*ibid*). The Federal Trade Commission conducted an inquiry and, in March of 1998, testified before Congress in favour of a data protection model (EPIC, 2003). Four months later, Senators Richard Bryan and John McCain introduced a bi-partisan bill and on October 21, the *Children's Online Privacy Protection Act of 1998* (15 U.S.C. §§ 6501-6506) (COPPA) was enacted.

COPPA requires that operators of commercial web sites directed to children¹² that collect personal information from children under the age of 13¹³ comply with a set of fair information principles¹⁴. First and foremost, operators are required to obtain parental consent before collecting information from a child (Principle of Knowledge and Consent). The parent’s consent must be “verifiable” – in other words, the operator must take reasonable steps to ensure that the parent receives notice of the operator’s information practices and consents to them.

¹² To determine whether or not a site is directed at children, the Federal Trade Commission looks at the “subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features” (US, 2004b).

¹³ Sites that are not directed at children but have actual knowledge that they do collect information from children are also subject to the Act.

¹⁴ The full list of fair information practices is set out on pp. 49-50 above.

The FTC informs operators that “if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others, the situation presents greater dangers to children, and a more reliable method of consent is required”¹⁵. Internal purposes include “marketing back to a child based on his or her preferences or communicating promotional updates about site content” (US, 2004b). Accordingly, the law assumes that placing children under surveillance as they play, and collecting their personal information in order to market product to them, is inherently benign and poses only a slight risk of harm.

The primary method for the operator to inform parents of its practices is to post a Privacy Notice in a prominent place on its site (Principle of Openness). The Notice must set out:

- operator’s name and contact information, including a contact who can respond to queries regarding the sites privacy policy (Principle of Accountability);
- how and what information will be collected from the child (Principle of Knowledge and Consent);
- the purpose of the collection (Identification of Purposes Principle);
- if the child’s personal information will be disclosed to third parties and, if so, for what purpose (parental consent is required for disclosure) (The

¹⁵ This provision is scheduled to sunset on April 21, 2005 (US, 2002).

Finality Principle);

- that the operator may not require that a child disclose more information than is reasonably necessary to enable the child to participate in that activity (Limitation of Collection Principle);
- parental right to access the child's record (Access Principle); and
- parental right to have the record deleted (Retention Principle).

In addition, the operator must make reasonable efforts to ensure the information is secure and kept confidential (Principle of Security).

Canadian legislators have not dealt specifically with children's privacy and the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) is silent with respect to children. However, the Office of the Privacy Commissioner's Guide for Businesses and Organizations indicates that consent for a minor may be obtained from a legal guardian (Canada, 2004). Under the common law, a minor has a diminished capacity to enter into a contract¹⁶. Accordingly, it is likely that a court would hold that a person under the age of 18 in Canada cannot legally consent to disclose his or her personal information for the purposes of PIPEDA without parental consent¹⁷.

¹⁶ "Generally speaking infants (minors) are not bound by their contracts which are either void or voidable" (*Toronto Marlboro Major Junior "A" Hockey Club et al. v. Tonelli et al.*, (1977) 18 O.R. (2d) 21 (Ontario Court of Justice).

¹⁷ This assumes that the offer to provide online services is accepted and the consideration to make the contract binding is the child's provision of personal information.

Some Canadian children's sites take steps to inform parents by email that their children have registered with the site and to obtain parental consent for the collection of their personal information. For example, the YTV.com registration process advises children that:

All members to YTV.com must be between the ages of 6 -18 and must live in Canada. Parental permission is also required for membership. As part of the registration process, we collect some personal information. All of your information is kept in a secure database and will never be seen by anyone outside of YTV.com staff (check out our Privacy section for more details). It's also necessary for us to collect parent's email addresses for those between the ages of 6 -15. We send an email to the Parents letting them know that their child has registered for a membership with YTV.com.

The implication of the first two sentences is that all children under 18 must obtain parental permission to register, but YTV only contacts parents if the child is 15 or under. Later in the registration process, the child is advised, "Because we collect personal info, we need to know your parent says it's okay for you to join.

Consent is given by checking the box below". Children are asked to check a box that indicates, "My parent/guardian gave me permission to have a YAP!

Membership." YTV.com also includes a "Safety and Privacy" link at the bottom of each page that links children to the YTV privacy policy.

TVOKids.com, on the other hand, does not have an icon or link to a privacy policy and a search for "privacy" using the site's search engine yields no results.

Although there is no registration process on the site, children are asked for personal information. For example, a child entering the Toronto Zoo's Name the Baby Giraffe contest must provide her name, city, age and telephone number in order to enter. There is nothing on the site to indicate how the information will be used and whether or not it will be retained after the contest is over. It is arguable that TVO does not fall under PIPEDA because it is not involved in commercial activity, but the site is embedded with sponsor pages, includes branded game environments for commercial products like littlerobots.com, and links to commercial sites, such as artattack.com, that sell product to children. The site also incorporates commercial marketing practices, such as encouraging kids to send email messages to their friends, which provides the site with the child's name and email and the name and email of their friend. When kids email TVO directly, they are asked to provide their first name, age, email address, and the names of their favourite TVOKids show TVOKids.com web page.

Illustration 6 – TVOKids Sponsor Page



As stated above, public interest groups called for the regulation of commercial sites targeting children because young children cannot differentiate between online content and advertising, and do not understand the consequences of revealing their personal information to marketers. Under both COPPA and PIPEDA, there are two primary mechanisms to protect children in these circumstances: the provision of (parental) consent¹⁸; and the presence of online privacy policies so parents and older children can make informed decisions about whether or not to release personal information. However, both of these mechanisms are problematic, even within a data protection framework. First, they assume that parents (and children 13 and over in the US) actually read and understand online privacy policies. Turow (2003) reports that 57 per cent of adults incorrectly believe that the mere presence of an online privacy policy ensures that any personal information that the site collects will not be shared with other organizations. Although 47 per cent say they think privacy policies are easy to understand, two-thirds of the people who believe this also – incorrectly – believe a site will not share their data. Turow warns that:

... the overwhelming majority of US adults who use the internet at home have no clue about data flows—the invisible, cutting edge techniques whereby online organizations extract, manipulate, append, profile and share information about them. Even if they have a sense that sites track

¹⁸ Although PIPEDA is silent with respect to children, it applies to the collection of all personal information in the course of a commercial activity and so captures the online collection of children's information. Since it is likely that minors cannot consent to the collection of their personal information, for the purposes of this discussion I am assuming a court would require the site first obtain parental consent.

them and collect individual bits of their data, they simply don't fathom how those bits can be used. In fact, when presented with a common way that sites currently handle consumers' information, they say they would not accept it (*ibid*).

Moreover, parents are no different from other adults: "Like the others, most parents are concerned, confused, and conflicted about internet privacy" (*ibid*). Most children, on the other hand, are unlikely to read a privacy policy because they are long and boring (MNet, 2003) and they simply consent to provide the information because they want to enter a contest or win a prize (MNet, 2001b).

COPPA and PIPEDA are also limited by narrow statutory language. Since COPPA only applies to sites directed at children, other sites, like Amazon.com, argue that COPPA does not apply to them even though they have an online Toy Store¹⁹. PIPEDA is limited to information collected in the course of commercial activity (s. 4(1)); commercial activity is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character" (s. 2). Accordingly, sites like TVOKids may be able to argue that PIPEDA does not apply to their activities because they are not primarily commercial in nature. Artificial distinctions that exempt some sites from regulation and capture others fail to account for the way that children flow easily from site to site, blending them

¹⁹ On April 22, 2003, 12 consumer organizations filed a complaint with the FTC that Amazon.com was in violation of COPPA. The complaint had not been resolved at the time of publication.

together into a continuous online social environment.

Similarly, distinguishing children based on age, like COPPA does, draws an “arbitrary line between teenagers and younger children”. Allen argues that, “No justification exists for perceiving the age of 13 as more capable of using computers without adult supervision. Some children above the age of 13 may still need parental control and vice versa” (quoted in EPIC, 2003). From a child's point of view, the age limit is incredibly easy to sidestep. If a 12 year old really wants to collect those Neopoints, play a game on Candystand, or chat on beer.com, all she has to do is change her age. On Candystand, for example, a child who registers an age less than 13 is asked for a parent's email address so the site can ask for the parent's permission to register the child. But if the child simply goes back to the registration page and changes her age, she is registered automatically. Unless every user's age can be authenticated, age limitations are virtually unenforceable, but reliable authentication would paradoxically lead to a massive invasion of online privacy (EPIC, 2003) forcing every user to identify himself to prove that he is not a child.

Perhaps most telling is the fact that, from a practical point of view, both Acts have failed to slow the sale of children's personal information. EPIC (2003) concludes that, “Despite COPPA's protections, there is a thriving list brokerage industry that targets children” and points to a “pre-school list advertisement, where marketers can purchase one million names for only \$5”. Shade, Porter

and Santiago conclude that, “Canadian Internet policy has so far tended to ignore how children and teens have become a viable and integral online market, which is a startling omission when considering the overall political economic framework of the Internet” (Shade et. al., 2004, p. 17). The review of children’s sites earlier in this chapter provides evidence that commercial sites targeting children pose dangers to their privacy and their sense of identity, and yet data protection policy has been unable to respond to these dangers because it focusses attention on the narrow question of informational control. The more difficult questions to ask, however, have to do with the social consequences of treating kids as fair game in a market economy that is based on commodifying their privacy.

Surveillance is now built into the social environments in which children play, learn and socialize. Students attending the Venerable Bede High School in Sunderland, England submit to iris scans when they pick up their food from the cafeteria and take out books from the school library (Leyden, 2003). Enterprise Charter School in Buffalo, New York requires students and staff to carry a radio-frequency identification chip which controls their access to the school and monitors their attendance (Scheeres, 2003). CCTV cameras are common in schools across Canada, and children submit to breathalyzers to get into school dances (Albrecht, 1998). The online environment works to naturalize these kinds of surveillance, because it trains children at an early age to identify themselves and allow themselves to be monitored. As data protection has been built into

business networks, corporations have in effect constructed a social environment for children that opens up their private lives in unprecedented ways and structures their social interactions for profit. At the same time, data protection has constrained the potential for a broader debate on the social value of aggressive online marketing to children by misdirecting the attention of policy makers to narrow questions of procedure. A communicatively based understanding of privacy reopens this question, and enables policy makers to examine the impact of marketing surveillance on children's identity formation and social relationships.

The policy potential of a communicatively-based understanding of privacy

In Chapter Five, I argued that privacy is the boundary between the self and other. Since the self emerges by internalizing the other's view of the self as a social object, privacy is located at the centre of identity formation. From this perspective, the most troubling aspect of commercial sites targeting children is the way in which web operators intentionally invade children's privacy to manipulate their sense of self for profit. The money at stake is substantial. Barbie alone generates over \$1 billion per year in gross revenues for Mattel Incorporated (Acuff, 1997, p. 5).

Dan Acuff, the president of Youth Market Systems, explains the relationship between children's identity and profit. He argues that to "maximize [the] opportunity for success" and create a "seismic impact on a company's bottom-

line profits”, corporations seeking to sell to children need:

... a thorough and *integrated* approach to product and product development that has *knowing the targeted consumer* at the core – knowing his/her brain development, needs, motivations, and wants, and the way he/she perceives the world... Most central to this systematic approach is a deep and profound understanding of the underlying abilities, motivations, needs, and behaviours of the young target (pp. 5-6).

Acuff’s Youth Market Systems approach operationalizes the work of Piaget, Erickson, and Kohlberg, to obtain “an in-depth understanding of the child consumer” because that is what “provides the only real access to approximating a ‘winning formula’ for the development of products and programs that succeed with kids (*ibid*). Marketer Rachel Geller (1998) bases her tips on how to market to children on “intensive work with psychologists” and encourages marketers to capitalize on teen’s narcissism because, “Playing off teen insecurities is a proven strategy.” Global marketing research agency Millward Brown surveyed several thousand children from more than 70 cities in 15 different countries (including the Americas, Europe and Asia) to determine “their life priorities, hopes and dreams and [reveal] the true drivers of kids’ trends by analyzing teen-minority groups, communities and clubs” (Lindstrom & Seybold, 2003).

Psychologist Susan Linn concludes that “The marketing industry, with the help of psychologists, targets its campaigns to hook children by exploiting their developmental vulnerabilities – the ways that their cognitive, social, emotional, and physical development influence decision making, likes, dislikes, interests, and activities” (Linn, 2004, p. 24). For example, when Cosmogirl! asks girls, “Do

you and your boyfriend have a problem you'd like help solving? If you're both willing to tell your side, we've got a therapist who can help! Tell us NOW!" they are intentionally playing upon teen's interest in advice in general, and relationships in particular. The question is also surrounded by four flashing ads and, if girls choose to seek the therapist's advice, they first get a pop-up containing a fifth ad. The global firm Saatchi and Saatchi advises marketers to exploit tween's developmental need to belong by changing "their goal to selling a community experience, instead of selling a product... to creating a hip, community experience" (quoted in Linn, 2004, p. 25), like the beef-friendly chat rooms and message boards on ZIP4tweens.com. Online teen communities like Alloy and Bolt add a good helping of what marketers like to call "edge". Geller explains that, "Teens are more difficult because they are an oppositional subculture, interesting in shutting out the adult world. However, there are enormous opportunities for the marketer who is able to understand both the reality and fantasy of teen life" (Geller, 1998, p. 1). Beer.com's use of soft porn images and questionable sex advice is a clear example of playing to teenaged boys fantasies in order to build brand loyalty for an adult product.

From this perspective, the online invasion of privacy is not merely a question of collecting personal information from children without their, or their parent's, consent. Rather, it involves the opening up of the child's private world to the eye of the marketer, who not only watches the child but reconstructs the child's environment in order to manipulate the child's sense of self and security. The

“self” that the child internalizes through its discussions with the “other” is removed from inter-subjective dialogue and confronted by the imperatives of an instrumental interest in creating a compliant consumer. This process is intentional on the part of the marketer. For example, as soon as the industry realized more than half of the world’s urban children have access to the Net and 10 per cent have their own web pages, marketers “made the adjustment” and began to plant false Web sites designed to look like amateur sites developed by tweens so they could embed surreptitious advertising into the online environment (Lindstrom & Seybold, 2003). This is called “stealth marketing”, and is described as:

... an unconventional strategy used to attract consumers, using "under the radar" promotional tactics that essentially go unnoticed by your non-target audience, as well as your competition. In fact, engaging in stealth marketing can be thought of as going to war with your competitors without your competitors knowing they are at war (OnPoint, 2004).

By constructing the child’s online environment to advance the instrumental interest in profit, corporations also limit the inter-subjectively generated identities available to the child. For example, MSN’s Privacy Policy indicates that a user’s registration information is used “to operate the site, for demographic statistics, and to display appropriate individualized advertisements.” MSN Instant Messaging has emerged as one of the primary communication tools used by Canadian tweens and teens (MNet, 2003), and just under half (49 per cent) of 12

to 17 year olds report they use it almost daily (Filion, 2003). When I registered on MSN as 16 year old Sue Laurier in 2003, my MSN page was changed to reflect MSN's idea of what interests a 16 year old girl – links to world news and weather were replaced by the latest celebrity gossip and information on dieting.

The massive collection of the minute details of children's online behaviour – their hopes and dreams, product preferences, crushes, or answers to questions like Cosmogirl's, "Have you ever taken a drug and had a bad experience?" or "What do you call your vagina?" (Cosmogirl.com's talk to us page) – combine into a continuous feedback loop that provides marketers with ammunition to sell specific products to individual children, and to finetune the child's online social environment to make the child more vulnerable to advertising messages. This invades the child's privacy because it artificially manipulates the line between the child's sense of self and other by embedding consumer messages into the "organized community or social group which gives to the individual his unity of self" (Mead, 1934, p. 154) in an attempt to steer the emergence of the self to facilitate a business agenda; this is particularly problematic because children have difficulty in distinguishing between advertising and content in the online world (Montgomery, 1996).

In addition, online marketing interferes with the child's social relationships by reconstructing the child's view of family life in order to make the child more vulnerable to marketing messages. In Habermasian terms, the systems world

colonizes the family and treats it as an asocial object to be manipulated and controlled according to the dictates of instrumental logic. For example, Linn discusses the impact of the “nag factor” on family life. In order to increase sales, marketers target advertising for products to children because “you want that nag factor so that seven-year-old Sarah is nagging Mom in the grocery store to buy Funky Purple [ketchup]. We’re not sure Mom would reach out for it on her own” (Heinz manager Kelly Stitt, quoted in Linn, 2004, p. 35)²⁰. To expand this “pester power” beyond the point of sale, companies engage in “relationship mining” to “understand family forces ... [and uncover] the motivations of different family members and the reasons for particular outcomes when conflicting needs occur” (Linda Neville, quoted in Linn, 2004, p. 36). Linn argues that, “Families are perceived as a repository (the mine) containing valuables that are there for the extracting – and exploiting” (p. 36), with the end result being an “effective assault on the fabric of family life” (p. 35).

This assault is facilitated by “deliberately undermin[ing] parent/child relationships both by encouraging children to nag and by portraying parents and adults as either absent or incompetent” (p. 197). For example, an ad for GloPhone on alloy.com reads, “Blah, blah, blah. Sick of hearing the 'rents [parents] complain about your yapping habits? Get a GloPhone account today and talk to anyone,

²⁰ The nag factor accounts for 46 per cent of sales of businesses that target children (Linn, p. 34); and influences 78 per cent of total grocery purchases, generating \$10 billion of food and beverage sales per year (Hauser, 2003).

anywhere, anytime -- for FREE!" The child is encouraged to avoid "annoying" parental supervision of the amount of time spent on the phone by embedding a product onto their desktop that will coincidentally deliver targeted advertising and collect personal information from them. Alloy.com is geared for teenagers (although GloPhone is also advertised on Neopets, which attracts a younger user group), and feeds into children's developmental need to be in control. Linn argues that marketing "exacerbates an ongoing, normal tension in family life that arises as children move from the total dependence of infancy to the independence of adulthood ... the need for autonomy" (p. 37). That parents do not like a product is *part* of the sales pitch. As Neville explains with respect to Kraft Lunchables, "Parents do not fully approve – they would rather their child ate a more traditional lunch – *but this adds to the brand's appeal among children because it reinforces their need to feel in control*"(quoted in Linn, p. 37, emphasis added).

At the same time that marketers seek to interfere in the child's relationships within the lifeworld, they attempt to create a "relationship" between the child and the product. However, this artificial relationship is removed from intersubjectivity, as there is no other "self" at the other end of the discursive interaction. Although children can interact with fictional characters in ways that attribute subjectivity to the fiction, that is an internal process which is

contextualized by the child's experiences in the lifeworld²¹. The relationship between the child and a brand is created externally, and involves a conscious manipulation on the part of the corporation to insinuate the brand itself into the child's thinking processes in order to manipulate the child's preferences. Thus, Barbie is no longer an object, but an artificial "subject" with which the child can enter into a relationship based on trust.

Bot programmes take this type of marketing to a new level. Bots are designed to electronically communicate with people in ways that simulate human behaviour. ELLEGirlBuddy, for example, was a bot that was programmed to interact with girls electronically and steer them towards the ELLEGirl.com web site (Kerr, 2004, p. 313). ELLEGirlBuddy represented herself as a 16 year old red head who "lives" in San Francisco with her parents and older brother, "likes" kickboxing, the colour periwinkle, the book *Catcher in the Rye*, and the music of No Doubt, and wants to be a handbag designer and a foreign correspondent when she "grows up". She was programmed to chat with girls about celebrity gossip, the weather and the bot's virtual life, "occasionally throwing in a suggestion or two about reading ELLEGirl magazine" (p. 313). Ian Kerr warns:

These electronic entities are being employed to assist in a rather slick form of misdirection. Like Hollywood's finest directors, who are able to steer their audiences' attention away from the false assumptions that they

²¹ For example, children use imaginary friends to help explore their subjective world and externalize the role-taking that enables the self to emerge.

have so skillfully engendered, some software programmers are applying principles of cognitive science to develop electronic entities that garner consumer trust. Unfortunately, some e-businesses are exploiting these applications to garner trust where no such trust is warranted (p. 288).

Even though girls interacting with ELLEGirlBuddy knew she was a bot, the program was able to create a “relationship” with girls because the interaction developed “trust through a form of friendship” (p. 315). Steve Klein, CEO of ActiveBuddy Inc., explains “these agents will become, for all intents and purposes, actual *friends* of the people that interact with them ... [so] the agent’s recommendation to me will be taken on a par with, for instance, your recommendation to me that I buy a Volvo” (quoted in Kerr, p. 315). The “illusion of friendship” is maintained because the programme creates “enormous personal profiles” of the girls which are “used to affect (as well as effect) their subsequent interactions” (p. 316).

The use of bots, particularly bots targeting children, raises serious questions about the nature of communication which is stripped of inter-subjectivity. It constitutes an invasion of privacy because the corporation penetrates the child’s private spaces and extracts data for instrumental purposes by manipulating the child communicatively. The interaction is, by definition, non-reciprocal; the child’s words are captured by the watcher without the filter of inter-subjective interpretation. The child is no longer situated as a consumer interacting with a salesperson, but as a friend talking to a friend, and the boundary between roles

– friend, consumer, anonymous member of civil society – collapses. This is a far cry from Simmel's discourse with the stranger because the conversation is initiated by a stranger *precisely* to use the child's private thoughts against her; the stranger fully intends to "continue in his life" and to exert "authority or restraint over the individual" (Westin, 1967, p. 32). That is the point of the whole exercise.

Westin, using language that resonates with a Meadian understanding of the emergence of the self, warns that this kind of invasion can have serious consequences on the development of a child's identity:

... what information about an individual is put in his files becomes part of his estimate of himself; it is how the wise and the powerful forces in his life see him. It takes a very strong personality, especially among children being recorded in the new information-worshipping society, to reject or fight the recorded judgment of who he or she 'is'. (Part of the value of privacy in the past was that it limited the circulation of recorded judgments about individuals, leaving them free to seek self-realization in an open environment) (p. 323).

Data protection policy is unable to protect this type of self-realization because it does not inquire into the social validity of the purposes for which data is collected. For example, as noted above, the Federal Trade Commission rules under COPPA assume that internal marketing of product to children is inherently benign and therefore calls for less stringent regulation than simple disclosure of

data to a third party. But a communicatively based understanding of privacy connects information practices to social consequences because it recognizes that privacy is tied to the formation of identity and healthy social relationships. This perspective reinvigorates Westin's legislative programme because it enables policy makers to confront the ways in which privacy invasions reconstitute the social environment.

Accordingly, when Westin's five-steps are applied, policy makers must first measure the seriousness of the need to conduct surveillance. Privacy is no longer on the defensive (to use Regan's term) because it is no longer situated as an individual right that must give way to social benefits. Instead, it is at the core of inter-subjectivity and, as such, central to social structure. Westin quotes Robert Merton in this regard:

'Privacy' is not merely a personal predilection; it is an important functional requirement for the effective operation of social structure. Social systems must provide for some appropriate measure, as they would say in France, of *quant-à-soi*—a portion of the self which is kept apart, immune from social surveillance (Merton, quoted on p. 58).

The argument that online surveillance of children helps advance an economic agenda is no longer freed from the inter-subjectively generated understanding of the lifeworld because, as Westin says, merely pointing to a social need that can be met through surveillance "is no balancing at all, but only a qualifying procedure for a licence to invade privacy. The need must be serious enough to

overcome the very real and presently rising risk of jeopardizing the public's confidence in its daily freedom from unreasonable invasions of privacy" (p. 370). Once the broad-ranging impact of invasive marketing techniques on the development of a child's identity and social relationships is brought into the privacy debate, it becomes much easier to conclude that the form of surveillance is not socially appropriate. It is no longer a question of tinkering with process, but of coming to social judgment about substance.

Moreover, under the second step of Westin's inquiry, the burden lies on the marketer to establish that other less invasive techniques are not available to meet the need (p. 371). Market research can occur in focus group situations where children – and their parents – know that they are being asked about a product. Companies can obtain feedback on their efforts to create products that are timely and relevant without systematically reconstituting the child's social environment and surreptitiously lifting the veil of her private life for their own purposes. Similarly, online market research can occur in transparent ways, rather than masking as "chat" and "play".

Such transparency will also help to make the research instrument more reliable, which addresses Westin's third step. Privacy, understood as a social construction rooted in language, is "not static; [boundary control mechanisms] change over time and have feedback loops that permit readjustments" (Altman, 1975, p. 43). Surreptitious market surveillance mitigates against a fair exchange

of views on products because it is predicated on misleading the child as to the nature of the interaction. Reasserting the boundary between the child's private life and the marketplace would protect the inter-subjectivity necessary to the formation of communicatively generated understanding and push back instrumental incursions which seek to objectify social experience and submit it to instrumental control.

A communicatively based understanding of privacy also provides a deeper context with which to apply Westin's "controlling principle" of consent. He argues that, "Neither law nor public opinion should force anyone to have privacy if that person, assuming he is an adult of sound mind, wants to give up his privacy for ... commercial ... reasons" (p. 374). The corollary is that children do not have the capacity to consent to commercial surveillance, because their identities are still vulnerable to the "recorded judgment of who he or she 'is'" (p. 323). Surveillance of children necessarily limits their freedom "to seek self-realization in an open environment" (*ibid*) because it interferes with the internalization of the conversation with the generalized other.

As such, theorizing privacy as the boundary between self and other provides policy makers with a stronger understanding of the sociality of privacy and the social consequences of invasion in the context of children's online privacy. This approach refocuses the debate on Westin's primary legislative question – is surveillance socially appropriate? – and reconnects the law to the meaning of

privacy as it is lived by real social actors in the lifeworld. Solutions such as increased monitoring of children's actions by parents and teachers can be critically evaluated, because they are placed into social context. As Livingstone notes, "An explicit negotiation of the balance between children's safety and children's privacy is important to the trust relationship between parents and children" (Livingstone & Bober, 2003, p. 4). Increased surveillance makes it less likely that children will be able to develop relationships of trust with significant adults in their lives. Good privacy policy must be sensitive to children's developmental needs, *including* their need for privacy and the role that privacy plays in fostering trusting relationships with intimate others. Rather than focussing on narrow issues of parental consent, policy informed by a Meadian framework can begin to explore the social impact of invasive practices and seek to structure both the online and the offline environment in ways that will promote the social and democratic meaning of privacy.

Chapter 7 - Conclusion

This dissertation has examined the theoretical underpinnings of current privacy legislation, and argued that the narrow conceptualization of privacy as informational control is not robust enough to restrict invasive practices enabled by new technologies. Although Westin's theory of informational control is rich in sociality, the social elements of his theory have been truncated from both policy and theoretical debates. This has served to privilege managerialism and technical innovation over the protection of privacy. In order to reclaim these social elements, I put Westin into dialogue with George Herbert Mead and Jurgen Habermas. I then laid the groundwork for a communicatively based theory that defines privacy as the boundary between the self and the other, both externally (as Altman argued) and internally through discourse with the generalized other. From this perspective, privacy is a social construction rooted in language that sits at the core of inter-subjectivity and self-reflexivity. As such, it cannot be traded off in exchange for some social benefit, such as efficiency or convenience. It also constitutes a flashpoint for social struggle precisely because instrumental reason negates the conditions necessary for inter-subjectivity by objectifying the self and collapsing the boundaries between social roles. Privacy policy will accordingly only be effective if it goes beyond data protection and constrains instrumental imperatives with legal mechanisms designed to protect the conditions necessary for inter-subjective dialogue.

Current privacy policy frameworks privilege a narrow interpretation of privacy as informational control. Laws based on this definition of privacy focus on fair information practices which are based on the individual's right to control the collection, use and disclosure of his or her personal information. Regan argues that this conceptualization as informational control pits privacy as an individual right against the social value to be gained through surveillance. This accordingly creates a zero sum game in which privacy must be "balanced" or traded off against the public good in using personal information to enhance efficiency and security. This masks the nature and importance of privacy as a social value and ensures that privacy protection will continue to give way before institutional arguments in favour of invasion.

A review of the literature makes it clear that the current dominant theoretical understanding of privacy as individual control over personal information is problematic, because it privileges the flow of information to technocratic elites. However, in spite of concerns that data protection is neither resilient enough a concept to protect privacy as a human right, social value and democratic value nor able to account for the role privacy plays in the development of identity, the policy literature continues to be dominated by fair information practices. Regan suggests that the literature may be advanced by recasting privacy as a social value in and of itself. Margulis builds on Regan's insight, and argues that by, revisiting Westin and Altman, one could move the debate forward by expressly incorporating social psychological insights into privacy theory (Margulis, 2003b).

This thesis takes up the task set by both Regan and Margulis, and seeks to reinvigorate the social meaning of Westin's theory of privacy. The historical review of data protection legislation set out in Chapter Three identifies the conceptual core of privacy in several countries, and sets the stage for a theoretical reflection on the nature of privacy as a social value. The similarities and contrasts which are revealed are significant because they identify the problems that need to be reflected upon theoretically.

A review of the broader legal tradition dealing with privacy demonstrates that the law has translated both sociological experience and democratic principles into a number of legal remedies which cluster around three anchors: constitutional and criminal protections against the invasive power of the state; property; and reasonable expectations of privacy. This means that privacy concerns based on historical memory and sociological experience have been sustained right up to the 1970s. Accordingly, privacy is not a response to technological imperatives but a social value with historical and cultural underpinnings. In like vein, privacy concerns which arose in the 1970s were rooted in the sociological experience of World War II and the threat of post-War totalitarianism.

However, in general, constitutional and common law concepts of privacy are grounded in the liberal tradition and, as such, are vulnerable to communitarian attack for the same reasons Regan critiques Westin's conceptualization of

privacy as an individual right. Judicial discourses are also limited because they link protections against surveillance to reasonable expectations of privacy and, as invasive technologies are built into the communication infrastructure, these expectations have necessarily shrunk. Nonetheless, the interaction between data protection legislation and broader judicial discourses regarding autonomy, dignity and social norms is not fixed, and common law articulations of privacy remain in the background because they contain a potential moment of social negotiation outside of the narrow limits imposed by the special interests which came together to shape data protection legislation.

An analysis of the enactment of data protection regimes in early adopting jurisdictions indicates that these special interests included: the protection of personal privacy in the advent of computer technology; the protection of national sovereignty; the resolution of conflicts over the distribution of power within states; the legitimization of information practices adopted by the public and the private sectors; the promotion of public sector and private sector efficiency; the promotion of trade; the promotion of technological development and innovation; the promotion of economic integration; and the promotion of political integration. These concerns were often contradictory and in tension with each other. Generally, legislation was legitimized by appeals to human rights concerns flowing from the European experience of totalitarianism but, as data protection became entrenched, the sociological meaning and experience of privacy was constrained by two technical and institutional brakes: the valorization of

technology; and the managerial interest in modernization. In Habermasian terms, the first sought to maintain technology in an autonomous sphere that was impervious to socio-cultural inputs, and the second sought to constrain and redefine both historical memory and the sociological meaning of privacy by privileging discourses based on instrumental logic, routine practices and administrative control. Data protection legislation accordingly took on a pedagogical function; it endeavoured to reconstruct public concerns in ways that were consistent with the managerial imperative, by “educating” the public about the meaning of privacy and privacy remedies.

Canadian privacy legislation is equally structured by these two brakes.

Moreover, the Canadian experience demonstrates how data protection principles work to privilege invasion when there is a conflict between managerialism and the sociological experience of privacy in the lifeworld, by limiting privacy issues to procedural questions of informational control. As privacy has been traded off in favour of competing interests in efficiency and technical innovation, much of the social meaning of privacy contained within Westin's theory of privacy has been lost.

This dissertation is intended to be an act of recovery in that regard. Westin's work does not flow from a theoretical vacuum. Indeed, his intellectual pedigree is drawn from a core group of sociologists who provide touchstones for his thought, and he draws heavily on Georg Simmel, Robert Park, Kurt Lewin and

Erving Goffman to articulate both the functions and states of privacy. Westin is therefore steeped in the sociological literature, and draws from a body of theory that focuses on the sociality of daily interaction. Drawing on these roots, Westin identifies privacy as one of the central dialectics of social life, and sets the stage for Altman's development of privacy as a boundary control mechanism.

However, he immediately limits his insight into the social nature of privacy in two ways. First, he places control over the boundary in the individual's hands alone, which juxtaposes the individual's interest in privacy against the social interest in surveillance. Second, he defines privacy as the opposite of social interaction, which necessarily shifts the focus of his inquiry from the socially constructed boundary between self and others to the information that flows beyond the privacy of solitude to the sociality of interaction. Together, these factors combine to make privacy a-social and in tension with social interaction, setting the stage for Regan's critique.

By putting Westin into conversation with George Herbert Mead, one can reconstitute Westin's original insights into the sociality of privacy. Mead's work on symbolic interactionism and social psychology sits at the base of the work of Westin's primary sources – Simmel, Park, Lewin and Goffman – and supports Altman's insights into the relationship between privacy, the development of interpersonal roles, and self-identity. Indeed, Altman's ability to capture and develop the social elements of Westin's theory by recasting privacy as a boundary control mechanism, which dissolves the tension between privacy and

social interaction, is based on Mead's understanding of the social emergence of the self. Once privacy is conceived of in this way, it is no longer anchored to the control over the flow of information and the individual seeking privacy is no longer isolated from social praxis.

Altman's work therefore points to a theoretical framework that has the potential to subsume Westin's theory as Margulis suggests (Margulis, 2003a, p. 422), and to capture and develop Westin's insights into the sociality of privacy. Indeed, Mead was occupied with the same question as Westin: how can one theorize democracy so that new technologies do not derail the democratic project. For Mead, the answer lies in the emergence of the self as a social being. The apparent tension between the individual and the collective which is so problematic in Westin's work dissolves, because the social is prior to and constitutive of the individual.

By placing the boundary between the self and others in symbolic interaction, the boundary becomes both dialectical and fluid, as Westin and Altman suggest. Privacy, as the boundary between the two, is central to identity formation because it is internalized through the dialogue between the social me and the emergent I. As such, it is a necessary element of healthy identity formation because it allows the self to become reflexive. Privacy therefore cannot shelter an atomistic individual from social interaction, as Westin posits. Instead, the line between self and other is inter-subjectively constituted through communication in

a number of different social contexts, including solitude, intimacy and participation in public activities. Privacy is a potentiality across Westin's spectrum because it is central to the distinction between self and other which enables the self to see itself as social object.

The instrumental collection of personal data conflicts with the social meaning of privacy precisely because the data creates an objectified self which is removed from inter-subjective dialogue. The collection of data in those circumstances becomes an exercise in power. In Habermasian terms, surveillance is problematic because it is non-reciprocal, and the actor's actions and words are captured by the watcher without any opportunity for inter-subjective interpretation. However, once privacy is rooted in language, it is placed at the core of inter-subjectivity and self-reflexivity because it defines the boundary between self and other both externally and internally. As such, privacy can no longer be traded off in exchange for some other benefit, like efficiency or convenience; and remains a flashpoint for social struggle because, as instrumental reason has become uncoupled from the lifeworld, the conditions necessary for inter-subjectivity have been negated through objectification of the self and the collapse of boundaries between social roles.

Once the social elements in Westin's thinking are grounded in a theory of privacy as a social emergent of language, the policy questions are no longer trapped in an abstracted set of information practices. Instead, policy makers are called

upon to assess the impact of invasive practices on the lived experience of privacy in the lifeworld. This is precisely the shift that occurs when children's online privacy is viewed from a Meadian perspective. Data protection policy has been unable to respond effectively to online invasions of children's privacy because it focusses attention on the narrow question of informational control. However, a communicatively based understanding of privacy enables policy makers to examine the impact of marketing surveillance on children's identity formation and social relationships. Since the self emerges by internalizing the other's view of the self as a social object, privacy is located at the centre of identity formation and policy makers are able to confront the social consequences of invading children's privacy to manipulate their sense of identity for profit.

From this perspective, the online invasion of privacy is not merely a question of collecting personal information from children without consent. Rather, it involves the opening up of the child's private world to the marketer's surveillance, which not only captures information about the child but enables the marketer to reconstruct that world in order to manipulate the child's sense of identity and social belonging. The child's privacy is invaded because the marketer embeds consumer messages into the community from which the child's sense of self emerges. In Habermasian terms, the systems world colonizes the child's world and treats it as an object to be manipulated and controlled according to the dictates of instrumental logic, without the creative tension injected by inter-

subjective dialogue.

Data protection policy is unable to protect children from this type of invasion because it does not evaluate the social appropriateness of the purposes for which data is collected. But a communicatively based understanding of privacy connects information practices to social consequences because it recognizes that privacy is tied to the formation of identity and healthy social relationships. This perspective reinvigorates Westin's legislative programme because it enables policy makers to confront the ways in which privacy invasions reconstitute the social environment. Privacy policy is accordingly liberated from narrow considerations of informational control and policymakers are called upon to decide whether or not the surveillance in question is appropriate.

Accordingly, this dissertation advances the privacy literature by developing the critique immanent in Westin's theoretical framework. Once privacy is conceived of as a social emergent grounded in language, one is able to reclaim Westin's full legislative programme and transform the current policy debate by reconnecting policy to the sociological understanding of privacy as it is lived in the lifeworld.

Appendix – Privacy Provisions in Selected Instruments

Universal Declaration of Human Rights

The United Nations General Assembly adopted the Universal Declaration of Human Rights (General Assembly resolution 217 A (III)) on December 10, 1948. The Declaration expressly provides for the protection of privacy; Article 12 declares, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Privacy is also indirectly protected through Article 3 which protects “the right to life, liberty and security of person,” as well as Article 18 which provides that:

Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 22 of the Declaration lays the groundwork for respect for privacy as a social right tied to the development of personality:

Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of

each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.

European Convention for the Protection of Human Rights and Fundamental Freedoms

The Council of Europe (COE) first passed privacy provisions in 1950 as part of the Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 XI 1950). The COE was established in 1949 by ten Charter members in order to strengthen and defend human rights, parliamentary democracy and the rule of law. The ten Charter members who signed the Treaty of London to establish the Council of Europe in 1950 were Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden and the United Kingdom. In 2004, the Council of Europe's membership had grown to 45 countries, including 21 newly democratizing countries in Central and Eastern Europe.

The Convention was a direct response to the UN Declaration, and incorporated similar language with respect to privacy. Article 8 of the Convention states:

- (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
- (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national

security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Sub-Article 2 sets out parameters for potential invasions of privacy but qualifies the enumerated list with the words, “as is in accordance with the law and is necessary in a democratic society.”

Article 9 of the Convention mirrors the protections for freedom of thought, conscience and religion set out in the UN Declaration, but sub-Article 2 provides a similar qualification:

(2) Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.

As in Article 8, any restrictions on private expression of religious or other beliefs must be lawful and consistent with democratic values and processes.

International Covenant on Civil and Political Rights

The United Nations adopted the International Covenant on Civil and Political Rights (General Assembly resolution 2200A (XXI)) on December 16, 1966. The Covenant entered into force on March 23, 1976, in accordance with Article 49 which provided that it “shall enter into force three months after the date of the

deposit with the Secretary-General of the United Nations of the thirty-fifth instrument of ratification or instrument of accession”). Canada ratified the Covenant on August 19, 1976.

Article 17 mirrored the general provisions of Article 12 of the Universal Declaration of Human Rights with respect to privacy, with the addition of the word “unlawful”, as follows:

No one shall be subjected to arbitrary *or unlawful* interference with his privacy, family, home or correspondence, nor to *unlawful* attacks on his honour and reputation (emphasis added).

Article 18 also closely follows the text of the Universal Declaration of Human Rights with respect to the right to freedom of thought, conscience and religion, including the “freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching”. Article 14 expressly provides that the interest of the private lives of persons before the courts may justify the exclusion of the press and the public from court proceedings.

Swedish Data Act

Sweden passed its Data Act on July 1, 1973. The Act created a licensing and registration system administered by the Data Inspection Board (DIB). The DIB is an independent government agency. Members of its Board of Directors are

appointed for four year terms, and are chosen to represent the political parties in the Swedish legislature, the major labour unions, industry, and the public administration.

The Act only applies to automated data processing, and does not extend to paper records. Under the Act, a public or private sector organization creating a personal file must apply to the DIB for a licence to do so. A personal file is defined as “any file, list or other notes kept by automatic data processing and containing personal data referable to the individual concerned” (s. 1). Under s. 3, the DIB must grant permission to set up and keep a personal file “if there is no reason to assume that ... undue encroachment upon the privacy of registered persons will occur”. The section then enumerates the factors to be taken into account in judging what constitutes undue encroachment. Special attention is to be paid “to the nature and quantity of the personal data to be recorded in the file, to how and from whom the data are to be collected, and to the attitude to the file held, or which may be assumed to be held by, the persons who may be registered”.

Data holders are accountable to the DIB (s. 7a) and to a data subject who reports “a suspicion that personal information is incorrect or misleading” (s.8). The DIB regulates the purpose of the file (s. 5); files can only be kept for that purpose (s. 7(1)) and collection is limited to information which accords with that purpose (s. 7(2)). Information may only be collected, used and disseminated for

the specified purpose (s. 7(3)), and private organizations cannot reveal the personal circumstances on an individual without authorization (s. 13). Data may only be retained as long as it is needed for the purpose of the file (s.12). The data holder is required to ensure that information is not incorrect or misleading (s. 8) and to add information if the file is incomplete (s. 9). The data must be protected from unlawful destruction, alteration or dissemination (s. 7(4)).

(Section 7(4) is similar to the requirement that data holders use security safeguards, although the wording is more general and does not specifically require the use of security systems as many of the succeeding Acts do.) The data subject has a right to access the file (s. 10) and to have it corrected (s. 8). Mandatory licensing and registration ensure that there will be no secret data systems.

Council of Europe Resolution regarding private sector databases

The Council of Europe passed a Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector (COE Resolution (73) 22) on September 26, 1973. Paragraph 6 of the Annex to the Resolution states that the individual has the right to know what information is collected about him or her and the purpose for its collection, although there is no requirement that the data holder obtain the individual's consent to its collection, use and disclosure. The information should be "appropriate and relevant" to the purpose for which it is stored (para. 1), and only used for that purpose unless there is "appropriate authorisation" (para. 5). Authorisation is to be broadly interpreted,

and includes individual consent, a licence from a regulatory authority or a general authorisation permitted by law (Explanatory Report, para. 27). The retention of “certain categories of information” should be limited (Annex, para. 4), inaccurate or obsolete information should be corrected or deleted (para. 7), and data holders should use security systems to restrict and track access (para. 8).

Council of Europe Resolution regarding public sector databases

On September 20, 1974, the COE passed a second Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector (Resolution (74) 29). Governments are required to set out the purpose for which information is collected and used (COE Resolution (74) 29, para. 3(b)) and the individual has the right to know what information is stored about him or her (COE Resolution (74) 29, para. 5), although there is no requirement that the individual first consent to its collection. Information must be “appropriate and relevant to the purpose for which it has been stored” (COE Resolution (74) 29, para. 2(c)). Data cannot be used for other purposes unless expressly permitted by law or a competent authority (COE Resolution (74) 29, para. 3(c)); however, there is no need to obtain the individual’s consent to the secondary purpose. Rules regarding the length of time data can be retained are mandated (COE Resolution (74) 29, para. 4). Information must be accurate and up to date (COE Resolution (74) 29, para. 2(b)). There must be security safeguards in place; safeguards include electronic security systems and rules of conduct governing those individuals who access the data on behalf of the data holder (COE Resolution

(74) 29, para. 6). Lastly, the data holder should regularly inform the public about the “establishment, operation and development” of public sector databases (COE Resolution (74) 29, para. 1).

American Privacy Act of 1973

The United States enacted the Privacy Act of 1974 (5 U.S.C. § 552a) on December 31, 1974. Each agency must inform the individual of the purpose for which the information will be used (s. (e)(3)(B)) as well as the “routine uses which may be made of this information” (s. (e)(3)(C)). “Routine use” is defined as use “for a purpose which is compatible with the purpose for which it was collected” (s. (a)(7)) and, as such, incorporates uses other than the express purpose alone. The agency cannot disclose personal information without the individual’s consent (s. (b)). The Act also provides that an agency can only collect information that is “relevant and necessary to accomplish a purpose” (s. (e)(1)), and that the information must be accurate, relevant, timely and complete (s. (e)(5)). Agencies are required to establish rules of conduct for persons operating record systems (s. (e)(9)) and administrative, technical and physical safeguards to keep the data secure (s. (e)(10)). The individual has a right to access data held about him or her, and to correct data believed to be inaccurate (s. (d)). Data cannot be collected secretly; record system creators must publish a detailed description of the system in the Federal Register (s. (e)(4)).

German Federal Data Protection Law

Germany passed the Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Law) on January 27, 1977. Under the Law, public data holders are accountable to the Federal Commissioner for Data Protection (ss. 24, 37), who has both investigatory and advisory powers. Private sector data holders were required to appoint an internal data protection officer to ensure compliance under s. 36. The provision has since been deleted from the German legislation, although the concept has been picked up by subsequent legislative instruments passed by the Council of Europe, Canada and others.

The data holder is required to advise the data subject of the purpose for collection (s. 4(3)) and can only collect personal information with the individual's consent, unless permitted by law or where the "collection of the data from the data subject would necessitate disproportionate effort and there are no indications that overriding legitimate interests of the data subject are impaired" (s. 4(2)(2.b)). The information can only be used only for the purposes for which they were collected (ss. 14, 28), although there are significant exceptions to this rule. For example, the public sector can use data for other purposes where:

- a legal provision prescribes or peremptorily presupposes this;
- the data subject has consented;
- it is evident that this is in the interest of the data subject and there is no reason to assume that he would withhold consent if he knew of such other purpose;

- particulars supplied by the data subject have to be checked because there are actual indications that they are incorrect;
- the data are generally accessible or the controller would be permitted to publish them, unless the data subject clearly has an overriding legitimate interest in excluding the change of purpose;
- this is necessary in order to avert substantial detriment to the common weal or to protect substantial interests of the common weal;
- this is necessary to prosecute criminal or administrative offences, to implement sentences or measures as defined in Section 11 (1), No. 8 of the Penal Code or reformatory or disciplinary measures as defined in the Youth Courts Act, or to execute decisions imposing administrative fines;
- this is necessary to avert a grave infringement of another person's rights; or
- this is necessary in order to conduct scientific research, scientific interest in conduct of the research project substantially outweighs the interest of the data subject in excluding the change of purpose, and the research purpose cannot be attained by other means or can be attained thus only with disproportionate effort (s. 14(2)).

Personal data must be erased once “knowledge of them is no longer required by the controller of the filing system for the performance of his duties” (s. 20(2)(2)).

Data holders must use technical and organizational measures to secure the data, and individuals have the right of access (ss. 19, 34) and correction (ss. 20,

35).

OECD Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data

The OECD passed voluntary Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data (OECD Doc. C(80)58) on October 1, 1980. The Guidelines are not a legally binding instrument, but are voluntary in nature. The Guidelines explicitly state that a data holder should be accountable for compliance with the stipulated set of information practices (s. 14). The data holder must specify the purpose for collection at or before the time of collection (s. 9), limit the information collected to that which is relevant to that purpose (s. 8), and only use or disclose that information for another purpose with consent or by lawful authority (s. 10). Information should be accurate, complete and up to date (s. 8) and protected by “reasonable” security safeguards (s. 11). Data holders should have a general policy of openness regarding its information practices and policies (s.12) and individuals should have the right to access their information at a charge “that is not excessive” (ss. 13(a) & (b)), and have successfully challenged data “erased, rectified, completed or amended” (s. 13(d)). The Guidelines limit collection to lawful and fair means, but only require that information be collected with the individual’s knowledge and consent “where appropriate” (s. 7).

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

On January 28, 1981, the COE opened its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS NO. 108, Strasbourg, 28.I.1981) for ratification. Signatory states are required to establish sanctions to hold data holders accountable (art. 10). The purpose for collection must be specified (art. 5(b)) and information collected must be relevant to that purpose (art. 5(c)) and retained no longer than is required (s. 5(e)). Information must be accurate and up to date (art. 5(d)) and protected by appropriate security measures (art. 7). Data holders must be open about the existence of a personal data file (art. 8(a)) and provide an individual with access to his or her file (art. 8(b)) and the ability to correct or erase data which have been improperly collected (art. 8(c)).

Table of Statutes, Treaties and Conventions

Access to Information Act, Canada, R.S., 1985, c. A-1.

Act Respecting Access to Documents Held By Public Bodies and the Protection of Personal Information, Quebec, S.Q. 1982 (L.R.Q. c.A-2.1).

Act Respecting the Protection of Personal Information in the Private Sector, Quebec, S.Q. 1993, c.17.

Basic Law for the Federal Republic of Germany, 1949 (Promulgated by the Parliamentary Council on 23 May 1949) (as Amended by the Unification Treaty of 31 August 1990 and Federal Statute of 23 September 1990).

Cable Communications Policy Act, US, PL 98-549, 1984.

Canadian Charter of Rights and Freedoms, Schedule B, Constitution Act, 1982.

Children's Online Privacy Protection Act 1998, 15 U.S.C. §§ 6501-6506.

Civil Code of Quebec, R.S.Q., c. C-12.

Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 4 XI 1950.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS NO. 108, Strasbourg, 28.I.1981.

Criminal Code of Canada, R.S.C. 1985, c. C-46, as amended.

Data Act, Sweden, 1973.

Debt Collection Act, 18 U.S.C. § 2415(i); 31 U.S.C. § 3701, 3711(f), 3716-3719, 1982.

Declaration on Transborder Data Flows, OECD Doc. 11, April 1985.

Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data, European Union, Brussels OJ No. L281 24 October 1995.

Driver's Privacy Protection Act 1994, 18 U.S.C. § 2721.

Electronic Communications Privacy Act 1986, 18 U.S.C. § 2510.

- Fair Credit Reporting Act*, 15 U.S.C. § 1681 et seq.
- Family Educational Rights and Privacy Act*, 20 U.S.C. § 1232, 1974.
- Federal Data Protection Law*, Germany, 1978.
- Freedom of the Press Act*, Sweden, 1949.
- Freedom of Information Act*, Manitoba, S.M. 1985-86, c.6 (C.C.S.M.c.F-175).
- Freedom of Information and Protection of Privacy Act*, Alberta, S.A. 1994 c. F-18.5.
- Freedom of Information and Protection of Privacy Act*, British Columbia, R.S.B.C. 1996, c.165.
- Freedom of Information and Protection of Privacy Act*, Ontario, R.S.O. 1990, c.F-31.
- Freedom of Information and Protection of Privacy Act*, Nova Scotia, R.S.N.S. 1993, c.5.
- Freedom of Information and Protection of Privacy Act*, Saskatchewan, S.S. 1990-91, c.F-22.01.
- Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data*, Organization for Economic Cooperation and Development, OECD Doc. C(80)58, Oct. 1, 1980.
- Health Insurance Portability and Accountability Act 1996*, US, PL 104-191.
- Health Sector Database Act*, Iceland Act No. 139/1998.
- Hesse Data Protection Act*, Gesetz und Verordnungsblatt I (1970), 625.
- International Covenant on Civil and Political Rights*, General Assembly of the United Nations Resolution 2200A (XXI), 16 December 1966.
- Model Code for the Protection of Personal Information*, Standards Council of Canada, CAN/CSA Q-830, 1996.
- Partial Birth Abortion Ban Act of 2003*, US, PL 108-105, 11-5-03.

- Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.
- Privacy Act*, British Columbia, R.S.B.C. 1996, c.373.
- Privacy Act*, Canada, R.S.C. 1985, c. P-21.
- Privacy Act*, Manitoba, S.M. 1970, c.74 (C.C.S.M. c.P-125).
- Privacy Act*, Saskatchewan, S.S. 1990-91, c.P-24.
- Privacy Act of 1974*, US, 5 U.S.C. § 552a.
- Privacy Protection Act, 1980*, 42 U.S.C. § 2000aa et seq.
- Privacy Rights Charter*, Canada, Bill S-21, 37th Parliament.
- Quebec Charter of Human Rights and Freedoms*, R.S.Q., c. C-12.
- Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, Council of Europe, Resolution (73) 22.
- Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, Council of Europe, Resolution (74) 29.
- Right to Financial Privacy Act*, United States, 1978, 12 USC § 3401.
- Right to Information Act*, New Brunswick, S.N.B. 1978, c. R-10.3.
- Right to Information Amendment Act*, New Brunswick, S.N.B. 1995, c.51.
- Safe Harbour Agreement*, 2000.
- Universal Declaration of Human Rights*, General Assembly of the United Nations Resolution 217 A (III), 10 December 1948.
- USA PATRIOT Act of 2001*, HR 3162 RDS .
- Video Privacy Protection Act*, 18 U.S.C. § 2710, 1988.

Table of Cases

Blencoe v. British Columbia (Human Rights Commission), 3 [2000] S.C.J. No. 43.

Census case, German Federal Constitutional Court, 1983.

Godbout c. Longueuil (Ville) (1997), 152 D.L.R. (4th) 577 (S.C.C.).

Guðmundsdóttir v. Iceland, Icelandic Supreme Court, No. 151/2003.

Hunter v. Southam (1984), 152 D.L.R. (4th) 577 (S.C.C.).

Irwin Toy Ltd. v. Quebec (A.G.), [1989] 1 S.C.R. 927.

Kyllo v. USA, (2001) 99-8508 (U.S.S.C.).

R. v. Big M Drug Mart Ltd. (1985), 18 C.C.C. (3d) 385 (S.C.C.).

R. v. Duarte, [1990] 1 S.C.R. 30.

R. v. LeBeau (1988), 41 C.C.C. (3d) 163 (Ont. C.A.).

R. v. Tessling, [2004] 1 SCJ No. 63.

R. v. Wholesale Travel Group Inc. (1991), 67 C.C.C. (3d) 193 (S.C.C.)

R. v. Wong, [1990] 3 S.C.R. 36 (S.C.C.).

Toronto Marlboro Major Junior "A" Hockey Club et al. v. Tonelli et al., (1977) 18 O.R. (2d) 21 (Ont. C.J.).

References

- Abbott-Chapman, J. & M. Robertson. (2001). Youth, leisure and home: Space, place and identity. *Loisir et Société* 24(2): 485-506.
- Acuff, D. (1997). *What kids buy and why: The Psychology of marketing to kids*. New York: The Free Press.
- Albrecht, C. (1998, October 9). Magrath teens may have to face breathalyzer. *Lethbridge Herald*. Lethbridge, Alberta.
- Allen, A.L. (1988). *Uneasy access: Privacy for women in a free society*. Totowa, N.J.: Rowman & Littlefield.
- Allen, K & L. Rainie. (2002). *Parents online*. Pew Internet & American Life Project.
- Altman, I. (1975). *The environment and social behaviour*. Monterey, California: Brooks/Cole.
- _____. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues* 33(3):66-84.
- American Corporation for Public Broadcasting. (2003). *Connected to the future: A report on children's Internet use*. Washington.
- Ardrey, R. (1966). *The territorial imperative*. New York: Atheneum.
- Arndt, H.A. (1949). The cult of privacy. *Australian Quarterly* XXI: 69-71.
- Arendt, H. (1978). *The Life of the Mind*. 2 vols. London: Secker & Warburg.
- Bainbridge, D. (1996). *The EC Data Protection Directive*. London: Butterworths.
- Baumann, R. (1984.) *This week in Germany*. July 6: 6.
- Bennett, C.J. (1988). Different processes, one result: The convergence of data protection policy in Europe and the United States. *Governance: An International Journal of Policy and Administration*, 1(4): 415-441.
- _____. (1992). *Regulating privacy*. London: Ithaca.
- _____. (1995). The political economy of privacy: A review of the

literature. Unpublished paper.

- _____. (1997). Understanding ripple effects: The cross-national adoption of policy instruments of bureaucratic accountability. *Governance: An International Journal of Policy and Administration*, Vol. 10: 213-233.
- Bennett, C.J. & Grant, R. (1999). *Visions of privacy: Policy choices for the digital age*. Toronto: University of Toronto Press.
- Bennett, C.J. & Raab, C. (2002). *The governance of privacy: Policy Instruments in Global Perspective*. London: Barnes and Noble.
- Bigelow, R. (1979). Transborder data flow barriers. *Jurimetrics* 20: 8-17.
- Bohman, J. (1994). Complexity, pluralism, and the constitutional state: On Habermas's *Faktizitat und Geltung*. *Law and Society Review* 28(4): 897-930.
- Bokszanski, Z. (1995). Identity of the Social Actor and Social Change. *Polish Sociological Review* 4(112): 349-360.
- British Computer Society. (1972). *Privacy and the Computer - Steps to Practicality*. London: British Computer Society.
- Bruner, C., D. Bennett & M. Honey. (1998). *Girls and technological desire. From Barbie to Mortal Kombat: Gender and computer games*. J. Cassell & H. Jenkins (Eds.). Cambridge, Massachusetts: MIT Press.
- Bull, H.P. (1989). *The Federal Commissioner for Data Protection*. (Typescript). Bonn.
- Burke, K. (1939). George Herbert Mead. *The New Republic* 11 Jan. 1939: 292-293.
- Burkert, H. (2000). Privacy - Data Protection: A German/European perspective. *Governance of Global Networks in the Light of Differing Local Values*. C. Engel & K. H. Keller. (Eds.). Baden-Baden: Nomos.
- Burnham, D. (1980) *The Rise of the Computer State*. New York: Random House.
- Bushkin, A & S.I. Schaen. (1975). *The Privacy Act of 1974: A reference manual*. McLean, Virginia: System Development Corporation.

Cada, C. (2003, August 9). Librarians are on front lines against easier access to records. *The Boston Globe*. Boston.

Calhoun, C. (1992). The infrastructure of modernity: Indirect social relationships, information technology, and social integration. *Social change and modernity*. H. Haferkamp & N.J. Smelser. (Eds.). Berkeley: University of California Press.

Canada. Department of Communications and Department of Justice. (1972). *Privacy and computers: A report of the task force*. Ottawa.

_____. House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities. 35th Parliament, 2nd Session. (1997). *Privacy: Where do we draw the line?*. Ottawa: Public Works and Government Services Canada.

_____. House of Commons Standing Committee on Industry. (1998a). *Evidence*. Meeting No. 81.

_____. House of Commons Standing Committee on Industry. (1998b). *Evidence*. Meeting No. 88.

_____. House of Commons Standing Committee on Industry. (1999). *Fifteenth Report*. 35th Parliament. 25 March 1999.

_____. Human Resources and Development Canada. (2000). *Press release 00-39*. 29 May 2000.

_____. Industry Canada. (1994, April 19). Manley announces Information Highway Advisory Council members. Press release. <http://www.cinemage.com/news1/may1994/highway.html>

_____. Industry Canada and the Department of Justice. Task Force on Electronic Commerce. (1998c). *Building Canada's Information Economy and Society: The Protection of Personal Information*. Ottawa: Public Works and Government Services Canada.

_____. Privacy Commissioner of Canada. (2000a). *Privacy Commissioner annual report 1999-2000*. Ottawa: Public Works and Government Services Canada.

_____. _____. (2004). *Your privacy responsibilities: A guide for businesses and organizations*. Ottawa: Public Works and Government Services Canada.

- _____. Senate Standing Committee on Social Affairs, Science and Technology. (2001). *Evidence*. Issue No. 25.
- Canadian Broadcasting Corporation. (2003, April 19). 'Big brother' travel database restricted. CBC News.
http://www.cbc.ca/stories/2003/04/09/privacy_030409
- Cassy, J. (2003, February 7). Students cash in on 'human billboards' plan. *The Guardian*.
- Cate, F. (1997). *Privacy in the information age*. Washington, D.C.: Brookings Institute Press.
- Cavoukian, A. & D. Tapscott. (1997). *Who knows: Safeguarding your privacy in a networked world*. New York: McGraw-Hill.
- Cavoukian, A. & T. Hamilton. (2002). *Privacy payoff: How successful businesses build consumer trust*. Toronto: McGraw-Hill Ryerson Limited.
- Child, A. (2001). *Protecting Privacy in Canada: Monitoring Compliance*. Information Systems Audit and Control Association Annual General Meeting. Ottawa. 31 May 2001.
http://www.privcom.gc.ca/speech/02_05_a_010531_e.asp
- Clarke, R.A. (1989). Information technology and dataveillance. *Communications of the ACM* 31: 498-512.
- Collins, R. (1998.) *The sociology of philosophies: A global theory of intellectual change*. Cambridge, Massachusetts: Belknap Press.
- Cook, Gary A. (1993.) *George Herbert Mead: The making of a social pragmatist*. Chicago, Illinois: University of Illinois Press.
- Cooley, T.M. (1888). *Treatise of the law of torts*. Callaghan.
- Coser, L. A. (1977). *Masters of sociological thought: Ideas in historical and social context*. Second edition. New York : Harcourt Brace Jovanovich.
- Council of Europe. (1983). *Legislation and data protection*. Rome.
- Cronk, George. (2001.) George Herbert Mead. *The internet encyclopedia of philosophy*. J. Fieser. (Ed.).
<http://www.utm.edu/research/iep/m/mead.htm>

- Culnan, M.J. & R.J. Bies. (1999). Managing privacy concerns strategically: The implications of fair information practices for marketing in the twenty-first century. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Dawson, C.P. & W.E. Hammitt. (1996). Dimensions of wilderness privacy for Adirondack Forest Preserve Hikers. *International Journal of Wilderness* 2(1): 37-41.
- Deflem, M. (1994). Introduction: Law in Habermas's theory of communicative action. *Philosophy and Social Criticism* 20 (4): 1-20.
- Demirbas, O. & H. Demirkan. (2000). Privacy dimensions: A case study in the interior architecture design studio. *Journal of Environmental Psychology*. 20: 53-64.
- DePaulo, B., C. Wetzel, R. Sternglanz Weylin, & M.J. Walker Wilson. (2003). Verbal and nonverbal dynamics of privacy, secrecy, and deceit. *Journal of Social Issues* 59(2): 391-410.
- Derlega V.J. & A.L. Chaikin. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, 33(3): 102-115.
- Dewey, J. (1927). *The public and its problems: An essay in political enquiry*. Chicago: Gateway Books.
- Dodds, A.E. , J.A. Lawrence, and J. Valsiner. (1997). The Personal and the Social: Mead's Theory of the 'Generalized Other'. *Theory & Psychology* 7(4): 483-503.
- Dunn, R.G. (1997). Self, Identity, and Difference: Mead and the Poststructuralists. *The Sociological Quarterly* 38(4): 687-705.
- Dyzenhaus, D. (1996). "The legitimacy of legality." *University of Toronto Law Journal* 46: 129-180.
- Eger, J. (1978). Emerging restrictions on transnational data flow: Privacy protection or non-tariff trade barriers? *Law and policy in international business* 10:1055-1103.
- Electronic Privacy Information Center. (2003). *The Children's Online Privacy Protection Act*. <http://www.epic.org/privacy/kids/>

- Etzioni, A. (1994). *Spirit of community: Rights, responsibilities and the communitarian agenda*. New York: Simon and Schuster.
- _____. (1999). *The limits of privacy*. New York: Basic Books.
- Evans, G., S.J. Lepore & K.M. Allen. (2000). Cross-cultural differences in tolerance for crowding: Fact or fiction? *Journal of Personality and Social Psychology*. 79(2): 204-210.
- Feenberg, A. (1995). *Alternative modernity: The technical turn in philosophy and social theory*. Berkeley: University of California Press.
- _____. (1999). *Questioning technology*. London: Routledge.
- Filion, F. (2003). *Kids take on media: Students tell us how their media intake affects them*. Ottawa: Canadian Teachers Federation.
- Flaherty, D. (1979.) *Privacy and government data banks: An international perspective*. London: Mansell.
- _____. (1989). *Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press.
- _____. (1999). Visions of Privacy: Past, present and future. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Flood, M. & C. Hamilton. (2003). *Youth and pornography in Australia: Evidence on the extent of exposure and likely effects*. Canberra, Australia: Australia Institute. Discussion Paper No. 52.
- Franklin, U. (1996 September 19). "Stormy weather: Conflicting forces in the information society." Closing Address at the 18th International Privacy and Data Protection Conference. Ottawa.
- Freese, J. (1981). More than seven years of Swedish legislation – Analysis of impact and trends for the future. Monte Carlo: Symposium of Computer Security and Privacy, January 26.
- _____. (1987) Seminar on openness and protection of privacy in the information society: Proceedings. Voorburg, Netherlands: Embassy of Sweden and Netherlands Central Bureau of Statistics.

- Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder: Westview Press.
- Girls Inc. (1994). Veg out! What you need to know about vegetarianism. <http://www.girlsinc.org/gc/page.php?id=1.4.14>
- Geller, R. (1998). A quantitative look at the best grands. *Selling to kids*. Potomac, Maryland: Phillips Publishing International, Inc.
- Gellman, R. (1999). Personal, legislative and technical privacy choices: The case of health privacy reform in the United States. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Globe & Mail. (2000, May 18). Delete Big Brother files, Quebec says Critics across the country blast Ottawa's personal database on Canadians: It's 'quite extraordinary and truly scary'. *The Globe and Mail*. Toronto.
- Goffman, E. (1961). *Asylums*. New York: Doubleday.
- _____. (1971). *Relations in public: Micro-studies of the public order*. New York: Basic Books, Inc.
- _____. (1959). *The presentation of the self*. New York: Basic Books, Inc.
- Great Britain. Home Office. (1972). *Report of the Committee on privacy*. London: Cmnd. 5104.
- _____. (1975). *Computers and privacy*. London: Cmnd. 6353.
- Gunter, B., G. Russell, R. Withey & D. Nicholas. (2003). The British Life and Internet Project: Inaugural survey findings. *ASLIB Proceedings* 55(4): 203-216.
- Habermas, J. (1999). *Between facts and norms: Contributions to a discourse theory of law and democracy*. Translated by W. Rehg. Cambridge: Massachussets: MIT Press.
- _____. (1992). Individuation through socialization: On George Herbert Mead's theory of subjectivity. *Postmetaphysical thinking: Philosophical essays*. Translated by W. Mark. Cambridge, Massachussets: MIT Press.
- _____. (1998a). "Paradigms of law". *Habermas on law and democracy*:

Critical exchanges. Michel Rosenfeld and Andrew Arato. (Eds.). Berkeley, California: University of California Press.

_____. (1998b). *The inclusion of the other: Studies in political theory*. C. Cronin & P. De Greiff, Eds. Cambridge, Massachusetts: MIT Press.

_____. (1989). *The structural transformation of the public sphere*. Translated by T. Burger and F. Lawrence. Cambridge, Massachusetts.

_____. (1981). *The theory of communicative action. Volume 2. Lifeworld and system: A critique of functionalist reason*. Translated by T. McCarthy. Boston: Beacon Press.

Hall, E.T. (1966). *The hidden dimension*. New York: Doubleday.

Hammit, W.E. (1982). Cognitive dimensions of wilderness solitude. *Environment and Behavior* 14(4): 478-493.

_____. (1994). The psychology and functions of wilderness solitude. *International wilderness allocation, management and research: Proceedings of a Fifth World Wilderness Congress Symposium*. J.C. Hendee & V.G. Martin. (Eds.). Ojai, California: International Wilderness Leadership Foundation.

_____. (2000). The relation between being away and privacy in urban forestrecreation environments. *Environment and Behavior* 32(4): 521-540.

Hauksson, P. & S. Sigurdsson. (1999). Icelanders opt out of genetic database. *Nature* 400, 19 Aug. 1999 correspondence: 707-708.

Hauser, R. (2003, August). The 'Nag Factor' nets \$10B in sales. *Natural Foods Merchandiser*. Boulder, Colorado: New Hope.com.

Hloden, O. (2000.) For Sale: Iceland's genetic history. Action Bioscience. <http://www.actionbioscience.org/genomic/hloden.html#Primer>

Honneth, A. (1996). *Struggle for recognition (Studies in contemporary German social thought)*. Translated by J. Anderson. Cambridge, Massachusetts: MIT Press.

Horkheimer, M. & T.W. Adorno. (1972). *Dialectic of enlightenment*. Trans. J. Cumming. New York: Herder and Herder.

- Joas, H. (1985). *George Herbert Mead: A contemporary examination of his thought*. Cambridge, Massachusetts: MIT Press.
- _____. (1997). Mead and the renaissance of pragmatism. *Re-claiming the sociological classics: The state of the scholarship*. C. Camic. (Eds.). Oxford: Blackwell Publishers.
- _____. (2001). The Emergence of the New: Mead's Theory and Its Contemporary Potential. *Handbook of Social Theory*. G. Ritzer and B. Smart. (Eds.). London: Sage.
- Katz, J. (1999). *Connections: Social and cultural studies of the telephone in American life*. London: Transaction Publishers.
- Kaya, N & F. Erkip. (1999). Invasion of personal space under the condition of short-term crowding: A case study on an automatic teller machine. *Journal of Environmental Psychology* 19: 183-189.
- Kaya, N. & M. Weber. (2003). Territorial behavior in residence halls: A cross-cultural study. *Environment and Behavior*. 35(3): 400-414.
- Kioka, Y. (2003). Dating sites and the Japanese experience. Tokyo: National Police Agency. http://www.iajapan.org/hotline/mobilepdf/4_KIOKA.pdf
- Kline, S. (2001). *Media use audit for B.C. Teens*. Burnaby, BC: Simon Fraser University Media Lab.
- Kupritz, V.W. (2000). Privacy management at work: A conceptual model. *Journal of Architectural and Planning Research* 17(1): 47-63.
- Laperrière, R. (1999). The "Québec model of data protection: A compromise between laissez-faire and public control in a technological era. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Laudon, K. (1994). Markets and privacy. *Communications of the ACM*.
- Lemert, C. & S. Branaman. (1997). *The Goffman reader*. Cambridge, Massachusetts: Blackwell.
- Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.
- Lewin, K. (1948). *Resolving social conflicts*. New York: Harper & Row.

- Leyden, J. (2003, January 8). UK school plans retinal scans in the dinner queue. *The Register*. London.
- Lindstrom, M & P.B. Seybold. (2003). *BRANDchild: Insights into the Minds of Today's Global Kids: Understanding Their Relationship with Brands*. London: Kogan Page, 2003
- Linn, S. (2004). *Consuming kids: The hostile takeover of childhood*. New York: The New Press.
- Livingstone, S. & M. Bober. (2003). *UK children go online: Listening to young people's experiences*. London: Economic and Social Research Council.
- _____. (2004). *UK children go online: Surveying the experiences of young people and their parents*. London: Economic and Social Research Council.
- Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk and digital discrimination*. London: Routledge.
- _____. (2001). *Surveillance society*. Buckingham: Open University Press.
- _____. (1994). *The electronic eye: The rise of the surveillance society*. Minneapolis: University of Minnesota Press.
- Macpherson, C.B. (1987). Liberalism as trade-offs. *The rise and fall of economic justice and other essays*. Oxford: Oxford University Press.
- Madgwick, D. (1968). *Privacy Under Attack*. London: National Council for Civil Liberties.
- Manley, J. (1999). *Canada and the Internet revolution: Connecting Canadians*. Washington: The Trilateral Commission.
<http://www.trilateral.org/annmtgs/trialog/trlgtxts/t53/man.htm>
- Margulis, S. (2003a). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*. 59(2): 411-430.
- _____. (2003b). Privacy as a social value and behavioral concept. *Journal of Social Issues*. 59(2): 243-262.
- Marshall, N.J. (1970). Environmental components of orientations toward privacy. *EDRA 2: Proceedings of the second annual Environmental Design Research Association Conference*. J. Archea & C. Eastman.

(Eds.). Stroudsburg, Pennsylvania: Dowden, Hutchinson & Ross.

_____. (1974). Dimensions of privacy preferences. *Multivariate Behavior Research* 9(3): 255-272.

Marx, G. (1999). Ethics for the new surveillance. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.

_____. (1988). *Undercover: Police surveillance in America*. Berkeley: University of California Press.

Marx, G. & N. Reichman. (1984). Routinizing the discovery of secrets: Computers as informants. *American Behavioral Scientist* 27: 423-452.

MacLeod, I. (2000). Federal watchdog says some files hold 2,000 bits of information. *Ottawa Citizen*, Wednesday 17 May 2000.

McDougall, B. (Ed). (1999). *Perspectives on privacy*. Toronto: Zaxis Publishing Inc.

McQuivey, J. (1999). *Net rules for a net-powered generation*. Cambridge, Massachusetts: Forrester Research.

Mead, G.H. (1934). *Mind, self, and society from the standpoint of a social behaviourist*. C.W. Morris. (Ed.). Chicago, Illinois: University of Chicago Press.

_____. (1936). *Movements of thought in the nineteenth century*. M.H. Moore. (Ed.). Chicago, Illinois: University of Chicago Press.

_____. (2000). "Science in social practice" *Social Thought & Research* 2000, 23(1-2): 47-63.

_____. (1964). *Selected writings*. A.J. Reck. (Ed.). Indianapolis, Indiana: Bobbs-Merrill.

_____. (1938). *The philosophy of the act*. C.W. Morris. (Ed.). Chicago, Illinois: University of Chicago Press.

_____. (1959). *The philosophy of the present*. A.E. Murphy. (Ed.). La Salle, Illinois: Open Court Publishing Company.

Media Awareness Network. (2001a). *Canada's children in a wired world: The*

parents view. Ottawa.

_____. (2000). *Parents and youth focus groups, 2000.*
Ottawa.

_____. (2003). *Young Canadians in a wired world: Phase II
focus groups.* Ottawa.

_____. (2001b). *Young Canadians in a wired world: The
student's view.* Ottawa.

Mieszkowski, K. (2001, August 13). Candy from strangers. *Salon Magazine.*

Miller, A. R. (1971). *The Assault on Privacy.* Ann Arbor: University of Michigan
Press.

Montgomery, K. (1999). *CME assessment of data collection practices of
children's web sites.* Washington: Center for Media Education.

_____. (2001). *teensites.com.* Washington: Center for Media
Education.

_____. (1996). *Web of deception: Threats to children from online
marketing.* Washington: Center for Media Education.

Morris, C. (1934). Introduction. *Mind, self, and society from the standpoint of a
social behaviourist.* By G.H. Mead. C.W. Morris. (Ed.). Chicago, Illinois:
University of Chicago Press.

Mulgan, G.J. (1991). *Communication and control: Networks and the new
economies of communication.* New York: Guilford Press.

Murphy, A.E. (1959). Introduction. *Philosophy of the present.* By G.H. Mead.
A.E. Murphy. (Ed.). La Salle, Illinois: Open Court Publishing Company.

Murphy, R.F. (1964). Social distance and the veil. *American Anthropologist* 66:
1257-74.

Nafisi, A. (2003). *Reading Lolita in Tehran.* New York: Random House.

National Academy of Sciences Project on Computer Databanks. (1972).
Databanks in a Free Society. Washington.

Niblett, G.B.F. (Ed). (1971). *Digital information and the privacy problem.*

Informatic Studies No. 2. Paris: OECD.

O'Connor, A.M. (2004). Who wants to know?: Privacy vs. security debated. *Los Angeles Times*. May 30.

OECD. (2004). *Overview of the OECD*. http://www.oecd.org/document/18/0,2340,en_2649_201185_2068050_1_1_1_1,00.html#The_OECD_what_is_it

_____. (1976). Policy issues in data protection and privacy. *Proceedings of the OECD seminar 24-26 June 1976*. Paris: OECD.

OnPoint Marketing. (2004). *Stealth Marketing/Undercover Marketing*. <http://www.onpoint-marketing.com/stealth-marketing.htm>

Packard, V. (1964). *The Naked Society*. New York: David McKay.

Park, R.E. (1950). *Race and culture*. Glencoe, Illinois: The Free Press.

Park, R.E. & E.W. Burgess. (1921). *Introduction to the science of sociology*. Chicago: University of Chicago Press.

Pedersen, D.M. (1996). A factorial comparison of privacy questionnaires. *Social Behavior and Personality* 24(3): 249-262.

_____. (1979). Dimensions of privacy. *Perceptual and Motor Skills* 48: 1291-1297.

_____. (1999). Model of types of privacy by privacy functions. *Journal of Environmental Psychology* 19(4): 397-405.

Persson, G. (1986). Computerized personal registers and the protection of privacy. *Current Sweden* 344: 4.

Peters, J.D. (1986). Institutional sources of intellectual poverty in communication research. *Communication research*, 13(4), 527-559.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, New York: State University of New York Press.

Phillips, B. (1996). Standing Committee on Human Rights and the Status of Persons with Disabilities, 35th Parliament, *Evidence*, Meeting No. 15.

Posner, R. (1978). The right to privacy. *Georgia Law Review* 12: 393-422.

- Prosser, W. (1960). Privacy. *California Law Review* 48: 383.
- Province. Testing firms scour doctors' files for eligible patients. (2004, February 23). *The Province*. British Columbia.
- Raab, C. (1999). From balancing to steering: New directions for data protection. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Regan, P. (1999). American business and the European data protection directive: Lobbying strategies and tactics. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- _____. (1995.) *Legislating privacy*. Chapel Hill: University of North Carolina Press.
- _____. (1996.) Surveillance and new technologies: Changing nature of workplace surveillance. *Computers, surveillance and privacy*. D. Lyon & E. Zureik. Minneapolis: University of Minneapolis Press.
- Rasmussen, D. M. (1994). "How is valid law possible? A review of *Faktizitat und Geltung* by Jurgen Habermas. *Philosophy and Social Criticism* 20 (4): 21-44.
- Rehg, W. (1999). Translator's Introduction. *Between facts and norms: Contributions to a discourse theory of law and democracy*. By J. Habermas. Cambridge: Massachusetts: MIT Press.
- Reidenberg, J. (1999). The globalization of privacy solutions: The movement towards obligatory standards for fair information practices. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Riley, T. (2004). Personal interview. 22 April.
- Rodota, S. (1976). Privacy and data surveillance: Growing public concern. *Policy issues in data protection and privacy*. OECD Information Studies no. 10. Paris: OECD.
- Rosenberg, J.M. (1969). *The Death of Privacy*. New York: Random House.
- Rosenblatt, P. & L. Budd. (1975). Territoriality and privacy in married and unmarried couples. *Journal of Social Psychology* 97: 67-76.

- Rosenfeld, M. (1998). "Can rights, democracy, and justice be reconciled through discourse theory?" *Habermas on law and democracy: Critical exchanges*. M. Rosenfeld and A. Arato. (Eds.). Berkeley, California: University of California Press.
- _____. (1995). "Law as discourse: Bridging the gap between democracy and human rights." *Harvard Law Review* 108: 1163-1189.
- Rosenfeld, M. and A. Arato. (1998). Introduction: Habermas's Theory of Law and Democracy. *Habermas on law and democracy: Critical exchanges*. M. Rosenfeld and A. Arato. (Eds.). Berkeley, California: University of California Press.
- Rotenberg, M. (1996, September 12). *Testimony and Statement of the Record on Children's Privacy Protection and Parental Empowerment Act, H. R. 3508*. House of Representatives, Committee on the Judiciary, Subcommittee on Crime. Washington: Electronic Privacy Information Center.
- Rowe, B.C. (Ed). (1972). *Privacy, computers and you: Workshop of the Data Bank Society Manchester*.
- Rule, J. (1974). *Private lives and public surveillance: Social control in the computer age*. New York: Schocken Books.
- Rule, J., D. MacAdam, L. Stearns & D. Uglow. (1980). *The politics of privacy: Planning for personal data systems as powerful technologies*. New York: Elsevier.
- Rule, J. & L. Hunter. (1999). Towards property rights in personal data. *Visions of privacy: Policy choices for the digital age*. C.J. Bennett & R. Grant. (Eds.). Toronto: University of Toronto Press.
- Samarajiva, R. & P. Shields. (1992). Emergent institutions of the 'intelligent network': Toward a theoretical understanding. *Media, Culture and Society*, 14:397-419.
- Scheeres, J. (2003, October 24). Three Rs: Reading, writing and RFID. *Wired Magazine*. San Francisco, California.
- Shallin, D.N. (1992). Critical theory and the pragmatist challenge. *American Journal of Sociology*, 98(2), 237-279.

- Signorelli, N. (1997). *A Content analysis: Reflections of girls in the media*. Menlo Park, California: Kaiser Family Foundation/Children Now.
- Simitis, S. (1995). From the market to the polis: The EU Directive of the protection of personal data. *Iowa Law Review* 80: 445-469.
- _____. (1987). Reviewing privacy in an information age. *University of Pennsylvania Law Review* 135: 707-746.
- Simmel, G. (1959). Social inquiry and the autonomy of the individual. *The human meaning of the social sciences*. D. Lerner. (Ed.). New York: Meridian Books.
- _____. (1950). *The sociology of Georg Simmel*. K. Wolff. (Trans. & Ed.) New York: The Free Press.
- Shade, L., N. Porter and K.S. Santiago. (2004, July 26-29). Everyday domestic internet experiences of Canadian youth and children. Paper presented at *Digital Generations—Children, Young People and New Media*. London.
- Statistics Canada. (2004, July 8). Household internet use survey 2003. *The Daily*. www.statscan.ca/Daily/English/040708/d040708.pdf
- Steele, J. & J.D. Brown. (1995). Adolescent room culture: Studying media in the context of everyday life. *Journal of Youth and Adolescence* 24(5): 551-576.
- Steeves, V. (1998). Censorship and Privacy Issues as Communications Become Increasingly Digital. *Adapting to New Realities: Canadian Telecommunications Policy*. D. Conklin. (Ed.). London, Ontario: University of Western Ontario Press.
- _____. (2001). Human Rights and New Technologies: The Canadian Charter of Rights and Freedoms: Twenty Years Later. *Electronic Governance*. T. Riley. (Ed.). London: Commonwealth Centre for Electronic Governance.
- _____. (2002.) Privacy and new media. *Mediascapes*. P. Attallah and L. Regan Shade. (Eds.). Toronto: Thomson.
- _____. (1999a). Privacy, Free Speech and Community: Applying Human Rights Laws to the Internet. *Human Rights and the Internet*. S. Hicks. (Ed.). Toronto: MacMillan Canada.

- _____. (1999b). Privacy, Property and Policy: Hidden Implications for the Information Highway. *The Information, Innovation and Impacts Series*, Ottawa: Statistics Canada, Science and Technology Redesign Project..
- Steeves, V. & J. Tallim. (2003). *Kids for sale: Online marketing to kids and privacy issues*. Ottawa: Media Awareness Network.
- Sweden. Committee on Automated Personal Systems. (1972). *Data and Privacy*. Stockholm.
- Sweden. Justice Department. (1972a). *Data and privacy*. Stockholm: Almannas Foraget.
- Sweden. Ministry of Defence. The Secretariat for National Security Policy and Long-Range Defence Planning. (1976). Stockholm.
- Sweden. National Tax Board. (2003). Population Registration in Sweden. Brochure. <http://www.rsv.se/broschyror/711/711b03.html#9>
- Turow, J. (2003). Americans and privacy: The system is broken. Philadelphia: Annenberg Public Policy Center of the University of Pennsylvania.
- United States. Department of Commerce. (2004a). *Safe Harbour overview*. http://www.export.gov/safeharbor/sh_overview.html
- _____. Department of Health, Education and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. (1973). *Records, computers, and the rights of citizens*. Washington, D.C.
- _____. Federal Trade Commission. (2004b). *How to comply with the Children's Online Privacy Protection rule*. <http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>
- _____. National Archives and Records Administration. (2002, April 17). *Federal Trade Commission 16 CFR Part 12*. Federal Register 67(74): 18818.
- Vance, A. (2004, September 30). RFID promoter can't stand being tracked. *The Register*. London.
- Walters, G. (2001). *Human rights in an information age: A philosophical analysis*. Toronto: University of Toronto Press.
- Warren, C. & B. Laslett. (1977). Privacy and secrecy: A conceptual

- comparison. *Journal of Social Issues*, 33(3): 43-51.
- Warren, S. & L. Brandeis. (1890). "The right to privacy". 4 Harv.L.Rev.: 193-220.
- Westin, A. (1980). Introduction. *The politics of privacy, computers and criminal justice records*. Arlington, Va: Information Resources Press.
- _____. (1967). *Privacy and freedom*. New York: Atheneum.
- Westwood, J. (1999). Life in the privacy trenches: Experiences of the British Columbia Civil Liberties Association. *Visions of privacy: Policy choices for the digital age*. Toronto: University of Toronto Press.
- Whitaker, R. (2000). *The End of privacy*. New York: The New Press.
- Will, I. (1983), *The Big Brother Society*. London: Harrup.
- Winseck, D. (2001). Doctoral seminar. Carleton University. 9 Oct. 2001.
- WorldNetDaily. (2003). Clothier pushes porn, group sex to youth.
http://worldnetdaily.com/news/article.asp?ARTICLE_ID=35604
- YTV. (2002). *YTV tween report, wave 8, 2002: Special kidfluence edition*.
<http://www.corusmedia.com/ytv/research/index.asp#TWEEN>

Web Sites

addictinggames.com
www.addictinggames.com

Alloy
www.alloy.com

Amazon.com
www.amazon.com

Art Attack
<http://www.hitentertainment.com/artattack/>

Barbie
www.barbie.com

Beer.com
www.beer.com/beerdotcom

Bolt
www.bolt.com

Candystand
www.candystand.com

Cosmogirl
www.consmogirl.com

Electronic Privacy Information Center
<http://www.epic.org>

Girls Inc.
www.girlsinc.org

Little Robots
www.littlerobots.com

Mannvernd, the Association of Icelanders for Ethics in Science and Medicine.
www.mannvernd.is/english/home.html.

MSN.com
www.msn.com

Neopets
www.neopets.com

newgrounds.com
www.newgrounds.com

Privacy & American Business
<http://www.pandab.org/whoswho.html>

Privacy Exchange
<http://www.privacyexchange.org/>

Public Interest Advocacy Centre
<http://www.piac.org>

Return Path
<http://www.returnpath.net/>

Seventeen Magazine
www.seventeen.com

Shockwave
www.shockwave.com

Sponge Bob Squarepants
http://www.nick.com/all_nick/tv_supersites/spongebob/main.jhtml

Teen Magazine
www.teenmag.com

TVOKids
www.tvokids.com

YM Magazine
www.ym.com

YTV.com
www.ytv.com

zip4tweens
www.zip4tweens.com