2011

Privacy Rights Mobilization Among Marginal Groups in Canada: Fulfilling the Mandate of PIPEDA

Lesley Jacobs
York University

Barbara Crow
York University

Kim Sawchuk

Privacy Rights Mobilization Among Marginal Groups in Canada:

Fulfilling the Mandate of PIPEDA

Research Report Prepared as Part of the Office of the Privacy Commissioner of Canada Contributions Program, 2010-2011

March 2011

York Centre for Public Policy & Law

York University

ycppl.osgoode.yorku.ca

Contributors

Lesley Jacobs
Barbara Crow
Kim Sawchuk

TABLE OF CONTENTS

CONTRIBUTORS

Lesley Jacobs is Professor of Law & Society and Political Science and Director of the York Centre for Pu blic Policy and Law at York University in Toronto, Canada. He completed his D.Phil. in politics at Oxford University. He has held a range of visiting appointment at other universities including the Harvard Law School (Liberal Arts Fellow, 1997-1998), Oxford Centre for Socio-Legal Studies (Wolfson Fellow, 1994), Law Commission of Canada (Virtual Scholar in Residence, 2006-2007), the University of California, Berkeley, (1994), University of Toronto (Centre of Criminology, 2004-2005), Institute for Human Rights, Emory University (Summer 2010), University of British Columbia (Political Science, 2001), and in 2010 he was a Distinguished Visiting Professor teaching in the Transnational Health Law Program at Waseda University in Tokyo, Japan . He serves on the Research Advisory Board of the Law Commission of Ontario, Series Co-Editor of the Asia Pacific Globalizaton and Legal Culture Book Series for UBC Press, Associate Editor of Law and Politics Book Review, Canada Research Team Leader on the SSHRC MCRI Asia Pacific Dispute Resolution Project on International Trade and Human Rights, and Co-Director of the Canadian Forum on Civil Justice SSHRC CURA The Costs of Justice Project. His books include *Rights and Deprivation* (Oxford University Press, 1993); Workfare*: Does it work? Is it fair?* (IRPP, 1995); *The Democratic Vision of Politics* (Simon & Schuster, 1997), Pursuing Equal Opportunities (Cambridge University Press, 2004) as well as a number of edited volumes including most recently *Balancing Competing Human Rights* (Ontario Human Rights Commission/Canadian Diversity Summer 2010) and *The Globalization of the Race Relations Policy Dialogue* (Canadian Race Relations Foundation/Directions, March 2011).

Barbara Crow is Associate Dean Research in the Faculty of Liberal Arts and Professional Studies at York University. Dr. Crow's current research interests relate to the social, cultural, political and economic implications of digital technologies. Her most recent project, with Professor Kim Sawchuk of Concordia University and funded by SSHRC, focuses on senior citizens and mobile technologies. She has also edited collections on mobile technologies, including: *The Wireless Spectrum: The Politics, Practices and Poetics of Mobile Communication* (UTP, 2010), co-edited with Michael Longford and Dr. Sawchuk; a special issue in 2008 of the *Canadian Journal of Communication*entitled "Wireless Technologies, Mobile Practices," co-edited with Dr. Sawchuk and Dr. Smith; and a special issue in 2008 of *Atlantis* entitled "Digital Feminisms," co-edited with Dr. Petty. In addition, Dr. Crow has worked on a number of large-scale interdisciplinary grants with engineers, designers, artists and communication scholars to produce technical and cultural content for mobile experiences, the Mobile Digital Commons Network (MDCN), 2004-2007 and the Canadian Wireless Infrastructure Research Project, (CWIRP), 2006-2008. Dr. Crow is also one of the co-founders of the Mobile Media Lab, co-located at York and Concordia.

Kim Sawchuk is a Professor in the Department of Communication Studies, Concordia University. She is the Editor of the *Canadian Journal of Communication* and co-editor of *wi: journal of mobile media*. She is the holder of an SSHRC standard research grant, with Dr. Barbara Crow, titled *Redressing silences, confronting mobility: Seniors, cell phones and aging* a project that foregrounds the cell phone practices of those who are sixty-five years and older. Co-authored publications from this project, with Dr. Crow, include a recent article in the *Telecommunications Journal of Australia*. The co-edited anthology T*he Wireless Spectrum*, with Dr. Crow and Michael Longford, was published by U of T Press in 2010. She is involved with the Under the City research team, a group exploring the use of mobile devices in the context of environmental issues. She has directed the Joint PhD in Communications at Concordia and the Masters Program in Media Studies. She is now the co-director of the Mobile Media Lab-Montreal and the co-founder of studioXX, a Montreal-based centre for women and digital technologies. Dr. Sawchuk's writings on feminism and the politics of the body include forthcoming articles in *Body and Society* and the *Visual Communications Journal*.

Privacy Rights Mobilization Among Marginal Groups in Canada: Fulfilling the Mandate of PIPEDA[1]

INTRODUCTION

"*Human rights can and should be declared universal, but the risk of having one's rights violated is not universal.*"[2]

This research project is designed to further our understanding of how individuals from certain marginal groups in Canada understand their right to privacy, the legislative protections that the Office of the Privacy Commissioner of Canada (OPC) is mandated to fulfill, and how these understandings affect privacy rights mobilization. The context for this research is provided by the increasing regulatory engagement of the Office of the Privacy Commissioner with invasions of privacy in the private sector involving new digital technology, new information technology, and the evolving digital economy in Canada.[3]

Although federal legislation ascribes the right to privacy to all Canadians, there is little reason to think that all Canadians are equally vulnerable to privacy rights infringements. This is certainly widely acknowledged in the case of security measures developed since 09/11 within the public sector. *The Anti-Terrorist Act* (2002) for example created certain police powers that by design have had a disproportionate impact on the privacy rights of particular ethnic and racial

[1] I would like to acknowledge the valuable research assistance to the project by Babita Ramlal, Kaitlyn Matulewicz, and Alex McLellan.

[2] Paul Farmer, *Pathologies of Power: Health, Human Rights, and the New War on the Poor* (Berkeley CA: University of California Press, 2005).

[3] For a detailed review of the current regulatory regime in Canada addressing privacy rights and the evolving digital economy

, see Lesley Jacobs and Kaitlyn Matulewicz , "Protecting Privacy Rights in the Emerging Digital Economy: Canada's Regulatory Scheme, Its Adaptability, and Its Future" (Paper Prepared for the Joint Industry Canada/ SSHRC Presidential Initiative on Research on Canada's Emerging Digital Economy, November 2010: 1-78.

groups in Canadian society.[4] The claim that some Canadians are more vulnerable than others to privacy rights infringements holds even more truth in the context of the private sector. Civil society provides the setting where we are most confronted by the inequalities that exist around us.[5] It is important to press the policy question of what this means in terms of privacy rights mobilization for persons who are members of these vulnerable groups.

The results of this research project have been divided into four chapters. The first three chapter are all authored by Lesley Jacobs. The first chapter develops the broad theoretical framework that underpins it, that is to say, the concept of legal consciousness and rights mobilization, and relates it to the legislative mandate of the OPC. The second chapter reports research results pertaining to Canadian youth and privacy issues that arise in their engagement with social networking such as *Facebook*. The third chapter reports research results pertaining to recent immigrants and their experiences with privacy concerns in electronic financial transactions. The fourth chapter, authored by Professors Barbara Crow and Kim Sawchuk, focuses on Senior Citizens in Canada and their experiences with invasions of privacy involving cell phones and other forms of communication devices.

These research results offer insights into how the Office of the Privacy Commissioner engages privacy rights mobilization among ordinary Canadians. The particular context is provided by The Protection of Personal Information and Electronic Documents Act (PIPEDA), which the OPC has the responsibility to implement. PIPEDA was introduced in 2001 to regulate the collection, use and disclosure of personal information by private organizations during

---

[4]Lesley Jacobs, "Securer Freedom For Whom? Risk Profiling and the New Anti-Terrorism Act," *UBC Law Review* 36: 2 (2003): 375-84.

[5]For a defence of this claim, see Lesley Jacobs, *Pursuing Equal Opportunities* (New York: Cambridge University Press, 2004), ch. 1.

commercial activities.[6] The express purpose of PIPEDA 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." The legislation is framed around ten core principles including Challenging Compliance, which means that under PIPEDA an individual is entitled to challenge an organization's compliance to privacy rights requirements by launching a complaint with the person responsible for the organization's compliance and that these organizations implement complaint procedures that are easy to access and understand. Fulfilling the mandate of PIPEDA includes meeting the demands of the principle of Challenging Compliance. It is with this in mind that the research reported in the chapters to follow have relevance. When an individual believes that his or her privacy rights have been infringed, the paths for protection, redress, and remedy available to that individual require an individual to be able to press a complaint. How do members of vulnerable or marginal groups such as youth aged 18-24, recent immigrants, and Seniors understand this complaint process and how does this affect their privacy rights mobilization? What are the policy implications of this? How can this be addressed with educational outreach and other measures?

Dr. Lesley Jacobs
Director, York Centre for Public Policy & Law
York University, Toronto, Ontario
http://ycppl.osgoode.yorku.ca/directorycppl.html

[6] *Protection of Personal Information and Electronic Documents Act, 2000*, c. 5

CHAPTER ONE

Legal Consciousness and Privacy Rights Mobilization in Canada

Lesley Jacobs

Introduction

The existing regulatory system for privacy rights protection in Canada is complex and reflects the fact that Canada is a federal state where privacy is a concern for both the Government of Canada and the provinces. From a comparative policy development perspective, Canada was slow in establishing a privacy rights protection scheme. The development of this system spans a mere four decades – other countries such as the United States have engaged privacy rights for much longer. The Office of the Privacy Commissioner was initially created in 1977 under the Canadian Human Rights Act, Part IV, as part of the Canadian Human Rights Commission; its mission is to "protect and promote the privacy rights of individuals."[7] Although the responsibilities and organizational structure of the OPC have evolved since 1977, its basic responsibility with regard to the privacy rights of Canadians has remained constant.

The research that is reported below treats privacy rights as an issue of rights mobilization. Rights mobilization can be best understood by distinguishing it from rights ascription. In legal

[7]Office of the Privacy Commissioner of Canada, Mandate and Mission. 27 Nov. 2010. <http://www.priv.gc.ca/aboutUs/mm_e.cfm#contenttop>.

terms, 'rights ascription' is a matter of what rights persons are ascribed in constitutional documents such as the Canadian Charter of Rights and Freedoms, legislation, the common law, and other sources of legal rights. 'Rights mobilization' is a matter of persons standing on the rights that they have been legal ascribed, asserting those rights claims in disputes and seeking legal remedies when those rights have been infringed or violated.[8] The main idea is that although persons may be ascribed legal rights, this does not necessarily translate into rights mobilization. Sometimes persons may be ascribed rights in law that they never stand on or claim, even in circumstances when those ascribed rights are clearly in the eyes of the law being violated.

In Canada, the ascription of privacy rights to Canadians is relatively straight forward in the sense that a right to privacy is recognized in numerous pieces of legislation at both the federal and provincial levels. Legislation that is particularly relevant to the Office of the Privacy Commissioner of Canada and this particular project is outlined briefly later on in this chapter. The essence of that legislation is to ascribe the same rights to privacy to all Canadians universally.

Privacy rights mobilization in Canada is, however, much less straight forward. Unlike the ascription of privacy rights in federal legislation, privacy rights mobilization cannot be assumed to be similar for all Canadians. It is doubtful, in other words, that all Canadians assert their privacy rights claims in disputes and seek legal remedies when those rights have been

[8] It is an interesting question, but tangential to the present research project, whether the mobilization of a legal right is possible when that right has been denied legal recognition. There have been, I think, some interesting examples in Canada's legal history of this sort of rights mobilization, in effect, persons standing on legal rights that they believe have been ascribed to them even though the courts have denied this and that over time this sort of rights mobilization has brought about legal change. The paradigm illustration of this, in my view, are the pleadings of the plaintiff Irene Murdoch in *Murdoch v. Murdoch* *[1975] 1 S.C.R. 423*.

infringed or violated. Is there a pattern to who mobilizes on their privacy rights and when they do so? Why do some people not mobilize on their privacy rights?

Access to Justice and Rights Mobilization

Traditionally, efforts to ascertain a pattern in rights mobilization are linked to resource and funding issues that are at the core of access to justice debates in Canada. The underlying reasoning is as follows:

(1) Legal needs arise in many instances when persons have their rights violated and need the legal system to protect their interests;
(2) access to justice is principally a challenge because some people have unmet legal needs;
(3) legal needs can be met by providing funding and resources for legal services such as legal aid and other venues for legal advice;
(4) when persons have their legal needs met, they mobilize on their rights;
(5) improving access to justice in Canada will diminish unmet legal needs;
(6) which means that improving access to justice in Canada will translate into greater rights mobilization for all.

The important implication of this type of argument is that rights mobilization is in effect a funding problem for the justice system in Canada.

In practice, there is an elaborate patchwork of access to justice programs in Canada that result in the legal needs of many Canadians, especially those who are marginalized in Canadian

society, going unmet.[9] The policy prescription that follows from this is that if the goal is same level of rights mobilization for all Canadians, then what is needed is resources and funding for access to justice programs to a level that ensures that the legal needs of all Canadians are adequately met.

In the case of privacy rights mobilization specifically, the logic of this sort of traditional access to justice approach is that in order to increase privacy rights mobilization among marginal groups in Canada, what is needed is a much greater commitment to funding access points in the justice system that facilitate opportunities for people from these groups to stand on their rights.

The approach to privacy rights mobilization in this research project has a different emphasis, although it still allows for the importance of access to justice considerations. Elsewhere, in earlier work on rights mobilization, I have argued at length that legal consciousness is an insightful theoretical framework for better understanding voting rights mobilization in First Nations communities.[10] Here, in this research, I propose to extend that approach and research agenda by claiming that a fundamental key component to privacy rights mobilization is the *legal consciousness* of the persons who have had their privacy rights violated. This approach holds that significant insight into privacy rights mobilization among persons from marginal groups can be achieved by answering questions about what having those rights mean to those persons: How do individuals from these marginal groups view the legality of the privacy rights? What sort of cultural meanings are bound up in standing on one's privacy rights and

---

[9]For a recent snapshot of the access to justice situation in Canada, see Lesley Jacobs, "Securing Better Access to Justice: Country Report Canada" (Report prepared for the Vance Center for International Justice, New York, March 2011). <http://www.abcny.org/citybarjusticecenter/vancecenter-overview>.

[10]Lesley Jacobs, "Mapping the Legal Consciousness of First Nations Voters: Understanding Voting Rights Mobilization," (in English and French) (Ottawa, Elections Canada, May 2009) <http://www.elections.ca/med/eve/APRC/vot_rights_e.pdf>.

claiming those rights in a legal process? Does the meaning vary according to what sort of privacy is at stake? What sort of identity must be assumed in order for someone to mobilize on their privacy rights?

The Theoretical Framework of Legal Consciousness

I have drawn a distinction between two approaches to better understanding the obstacles and challenges of privacy rights mobilization among marginal peoples in Canada. One approach, which utilizes the theoretical framework of access to justice, treats these obstacles and challenges as ones of underfunding and the lack of resources in the Canadian justice system. Privacy rights mobilization among marginal peoples is, in other words, a problem of unfair distribution of the opportunities to access paths to claim rights. The other approach, which is the one explored in the chapters to follow in this research project, holds that when marginal peoples in Canada do not stand on their privacy rights when those rights are violated, this is a reflection of how they themselves understand and make sense of the legal construction of privacy rights. How people understand and make sense of the legality of rights constitutes their legal consciousness.

The idea of legal consciousness is, at its core, how ordinary people, as opposed to legal professionals such as judges and lawyers, understand and make sense of legal rights. Legal consciousness, in this sense of the term, refers to an individual's knowledge or awareness of the law and its potential for resolving disputes and affecting social change.[11] The significance of

[11] David Trubek (1984). "Where the Action Is: Critical Legal Studies and Empiricism," *Stanford Law Review* 34:1/2 (January 1984): 575; Sally Engle Merry *Getting Justice and Getting Even: Legal Consciousness Among Working-Class Americans*. (Chicago: University of Chicago Press, 1990). For the idea that there are competing conceptions of legal consciousness, see Patricia Ewick and Susan Silbey, Conformity, Contestation, and Resistance: An Account of Legal Consciousness," *New England Law Review* 26 (1992): 731-742.

legal consciousness, in other words, is that it provides people with interpretive frameworks to guide their interactions with law and inform their beliefs about law's promise or danger. Any answer to the question I posed above, What is the meaning of privacy rights mobilization for an individual is a claim about the legal consciousness of that person.

Legal consciousness is more than a simple reflection of attitudes or beliefs about legal rights. It is better thought of as a form of cultural practice where beliefs and attitudes about legal rights affect practices and what people do, which in turn shape beliefs and attitudes. "In this theoretical framing of legal consciousness as participation in the construction of legality," explain Ewick and Silbey, "consciousness is not an exclusively ideational, abstract, or decontextualized set of attitudes toward and about the law. Consciousness is not merely a state of mind. Legal consciousness is produced and revealed in what people do as well as what they say."[12] Legal consciousness is, however, never entirely the construction of a single individual or simply a subjective viewpoint.[13] It is, in the words of Ewick and Silbey, "always a collective construction that simultaneously expresses, uses, and creates publicly exchanged understandings."[14] To put the point in another way, legal consciousness is not a function of doctrinal law and hence changes in doctrinal law do not necessarily lead to parallel changes in

[12] Ewick and Silbey, The *Common Place of Law*: 46.

[13] Although almost all existing research on varieties of legal consciousness has focused on individuals, some have focused on organizations. See Erik Larson, "Institutionalizing Legal Consciousness: Regulation and the Embedding of Market Participants in the Securities Industry in Ghana and Fiji," *Law & Society Review* 38 (2004): 711-736; and Lesley A. Jacobs, "Differentiated Corporate Legal Consciousness in International Human Rights Disputes: Security and Transnational Oil Companies in Sudan," *APDR Research Notes* 1:3 (Oct 2008):37-49. <http://apdr.iar.ubc.ca/publications/ejournal/APDR_1.3/APDR_1.3_LJ.pdf >.

[14] Ewick and Silbey, *The Common Place of Law*: 46.

legal consciousness.[15] For example, changes in legislation regarding privacy do not necessarily lead to changes in legal consciousness about privacy rights among ordinary Canadians.

Legal consciousness research is designed to identify its shapes and patterns. This assumes that although the legal consciousness of an individual is constantly changing, there is something instructive about trying to identify the variety of forms it can take. These forms or varieties of legal consciousness are by necessity only ideal types or approximations. The underlying idea that how a person deals in a particular interaction with political and legal institutions and the law generally – a police stop, a letter from the bank's lawyer threatening to foreclose on a mortgage in default, a complaint about discrimination against a landlord – is largely a function of the broad position or viewpoint he or she has on law and legality. And moreover this viewpoint is a reflection of law's presence in and relevance to a person's everyday life. Elsewhere, I have introduced the idea of differentiated legal consciousness.[16] Instead of assuming a uniform legal consciousness when crises arise in a particular jurisdiction, my approach has been to treat legal consciousness as varied among groups of individuals differently situated in the crisis. The promise of this differentiated approach to legal consciousness is that it enables me to both draw contrasts between perspectives of differently situated groups within the same jurisdiction, which reinforces the fact that many marginal groups are not homogeneous, and note commonalities between similarly situated groups in other jurisdictions.

Another important strand in legal consciousness research is exploring the effects of legality on identity. The underlying idea is that often mobilizing legal rights demands taking on

---

[15] See for example my "Legal Consciousness and the Promise of Law & Society," *The Canadian Journal of Law and Society* 18:1 (2003): 61-66.

[16] Lesley A. Jacobs, "Rights and Quarantine during the SARS Global Health Crisis: Differentiated Legal Consciousness in Hong Kong, Shanghai, and Toronto," *Law and Society Review* 4:1/3 (Sept 2007):511-553.

a particular identity. Perhaps this is clearest in the case of disability rights law.[17] It is a familiar theme that the past three decades have been characterized by a dramatic expansion by legislatures and the courts in the field of rights for persons with disabilities. Yet, it has been discovered that the pattern of mobilization of these rights is a complex one. In particular, in order for individuals to stand on these rights, they need to identify as persons with disabilities – taking on this identity is something that some people struggle with and indeed resist, which affects their capacity to mobilize the rights enacted by disability rights law. As one recent study of disability rights mobilization noted, "Not only does identity determine how and when rights become active, but that indeed rights can also shape identity."[18]

Similarly, I am stressing here that an answer to the question, What is the legal meaning of the right to privacy for the individual?, is a claim about the legal consciousness of that person. How that question is answered can provide great insight into privacy rights mobilization, for rights mobilization is a function of what those rights mean to those individuals who hold them. Instead of seeing rights as instruments or tools, rights are viewed from the perspective of what they actually do and how they matter, or do not matter to their intended beneficiaries. Privacy rights in Canada are, as I emphasized at the outset, a legal right that are set within a complex web of legal sources including legislative, constitutional, and common law.; when individuals choose to exercise their privacy rights, this is in part a reflection of what the legality of those rights means to them. And for that reason, an important dimension of privacy rights mobilization is legal consciousness.

---

[17] David Engel and Frank Munger, "Rights, Remembrance, and Reconciliation of Difference," *Law and Society Review* 30:7 (1996): 7-54, and *Rights of Inclusion*, ch. 3.

[18] Engel and Munger, *Rights of Inclusion* 242.

Description of the Overall Research Project

The research in this project can be understood as a mapping of the legal consciousness of three marginal groups in Canada – Youth ages 18-24, recent immigrants, and Seniors – with regard to their privacy rights, focusing in particular on their experiences with social networking, electronic financial transactions, and digital telecommunications, respectively.

How did the project investigate the legal consciousness of persons in these groups? The methodology utilized was data collection based on interviews with individuals belonging to these three groups. The interviews revolved around a series of open-ended questions that were recorded and transcribed. The interviews lasted on average about 30 minutes. The subjects for the interviews all live in the Greater Toronto Area. The sample for each group was as follows: youth (56), recent immigrants (24), and Seniors (24). The interviews were conducted by either the faculty who wrote the individual chapters or by a team of graduate students at York University.[19]

The transcriptions for these interviews, which total approximately 750 pages of text, provide the basis for determining the legal consciousness of these three groups. In effect, these transcriptions offer us insights into what the right to privacy mean to the individuals interviewed as part of the project. It is these insights and the broader analysis that is offered in the three chapters to follow.

[19] The team of graduate students at York University who conducted and transcribed the interviews were Preet Virdi, Feiyu Sun, Beverley Quaison, Hannah Bahmanpour, Charine Mattis, and Alex McLellan.

Overview of the Federal System of Privacy Rights Protections[20]

The system of privacy protections put in place by the federal government in Canada revolves around two pieces of legislation – The Privacy Act and Protection of Personal Information and Electronic Documents Act -- and the regulatory agency, The Office of the Privacy Commissioner of Canada. The Privacy Commissioner of Canada is an Officer of Parliament appointed by the Governor in Council for a seven year term. The Commissioner, currently Jennifer Stoddart (who had her term renewed in November 2010), has an expansive mandate which includes: investigating complaints, conducting audits, research, reporting annually on the federal privacy laws, and promoting awareness of privacy issues through public education. However, in terms of enforcement power, the OPC is not an administrative tribunal and so the Commissioner does not have the legal authority to issue binding decisions. Rather, disputes are settled informally and matters that remain unresolved can be pursued at the level of a Federal Court. The work of the Commissioner is supported by an Assistant Privacy Commissioner and the Office of the Privacy Commissioner (OPC).

The most important responsibility of the OPC is for overseeing both the federal Privacy Act and PIPEDA, which are outlined below. In addition, where provinces have not enacted legislation declared substantially similar to PIPEDA, the OPC has jurisdiction to handle requests and complaints relating to provincially regulated private organizations. And, the reach of the OPC extends to the provincially regulated private sector when personal information transcends provincial or national borders. Structurally, the OPC is divided into seven branches: Investigations and Inquiries; Audit and Review; Research, Education and Outreach;

[20] This section draws in part on Lesley Jacobs and Kaitlyn Matulewicz , "Protecting Privacy Rights in the Emerging Digital Economy: Canada's Regulatory Scheme, Its Adaptability, and Its Future" (Paper Prepared for the Joint Industry Canada/ SSHRC Presidential Initiative on Research on Canada's Emerging Digital Economy, November 2010):13-17.

Communications; Legal Services, Policy and Parliamentary Affairs; Human Resources; and, Corporate Services. [21] In addition, the OPC created an External Advisory Committee in February 2004 which is made up of privacy experts, lawyers, professors and a former Supreme Court Justice. The Committee assists the OPC in identifying strategic plans and future directions of the office. Currently, the OPC has identified the following areas as four top priorities: information technology, national security, identity theft and genetic information.[22]

The Privacy Act,[23] which came into effect on July 1, 1983, applies to approximately 250 federal government departments and agencies. The Privacy Act was established to protect the personal information collected, used and disclosed by the federal government, and also legislates access to information that is of either a personal or general nature. Under the Privacy Act, personal information is not to be disclosed, without prior consent, except under few circumstances. For example, the Privacy Act allows personal information to be disclosed without consent when it is in the best interest of the public or the individual to do so. [24] Although the Privacy Act was introduced in 1983, the broad definition of personal information as "information about an identifiable individual that is recorded in any form"[25] demonstrates the potential of the Act to apply to technological advances in the public sector and new mediums used to store personal information. Requests to correct or change personal information that is held by a public

---

[21] Office of the Privacy Commissioner of Canada, Organizational Structure. 27 Nov. 2010. <http://www.priv.gc.ca/aboutUs/au_org_e.cfm#contenttop>.

[22] Interestingly, while the OPC has identified information technology as one of its key future directions and recognizes the benefits technology can bring to governments or private organizations, the OPC itself precludes the use of online applications for information requests or complaints; the website of the OPC warns: "Please do not make complaints or provide personal information by e-mail, as security cannot be ensured". See Office of the Privacy Commissioner of Canada, Access to Information and Privacy FAQs. 27 Nov. 2010. <http://www.priv.gc.ca/atip/faqs_e.cfm#contenttop>.

[23] *Privacy Act, R.S. 1985*, c. P-21.

[24] *Privacy Act, R.S. 1985*, c. P-21, s.8 outlines situations where personal information can be disclosed without consent.

[25] *Privacy Act, R.S. 1985*, c. P-21, s.3.

body, or complaints regarding a violation of the Privacy Act are sent to the Office of the Privacy Commissioner of Canada (OPC). In addition, as of April 1, 2007, the Office of the Privacy Commissioner of Canada itself is subject to the Privacy Act; complaints about the OPC are handled by Privacy Commissioner ad hoc, an independent complaint mechanism.

The Protection of Personal Information and Electronic Documents Act (PIPEDA) was introduced in 2001 to regulate the collection, use and disclosure of personal information by private organizations during commercial activities.[26] Unlike the federal Privacy Act, which does not mention the use of technology, the express purpose of PIPEDA 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."[27] Furthermore, the preamble of PIPEDA describes the law as "[a]n Act to support and promote electronic commerce." In determining what type of information fits the definition of "personal information" the OPC has included business e-mail addresses, photographs, an employee's identification number, and a Computer Internet Protocol (IP) addresses.[28] The legislation is framed around ten principles that are outlined in Schedule One of the Act: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and, challenging compliance.

PIPEDA initially applied to federally regulated banks, telecommunications companies, airlines and transportation companies. On January 1, 2004, the application of PIPEDA was

---

[26] *Protection of Personal Information and Electronic Documents Act, 2000*, c. 5

[27] *Protection of Personal Information and Electronic Documents Act, 2000,* c. 5, s.3.

[28] Office of the Privacy Commissioner of Canada, *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act.* (Ottawa: Office of the Privacy Commissioner of Canada, 2008):5 <http://www.priv.gc.ca/information/pub/lbe_080523_e.pdf>.

widened to incorporate commercial activities undertaken by provincially regulated private sector organizations when there is not substantially similar provincial legislation. Québec, British Columbia, Alberta, and Ontario (with respect to health information) have been recognized as the only provinces with substantially similar legislation. However PIPEDA continues to apply to even these jurisdictions in cases involving inter-provincial and international commercial transactions. Since the OPC is not an administrative tribunal and the Commissioner does not have the legal authority to issue binding decisions, disputes and complaints regarding a violation of PIPEDA are settled informally and matters that remain unresolved can be pursued in the Federal Court of Canada.

PIPEDA extended considerably the mission of the OPC to function as an ombudsman, protector and champion of the right to privacy in Canada. Traditionally, the Canadian courts have identified the interests covered by the right to privacy as three-fold: territorial/spatial, personal, and informational.[29] Under PIPEDA, the OPC has increasingly been shifting its focus from the federal public sector to the protection of Canadians' personal data and information from threats posed by private corporations and organizations, often working within regulatory frameworks established by the federal government. The context for PIPEDA is the fact that businesses and other private organizations are collecting more and more personal information. In effect, the enactment of PIPEDA is a reflection of the recognition that private sector activity has significant potential to infringe on the privacy rights of Canadians and the need to have an independent federal agency to protect against those infringements. What's more, as evidenced with cases handled by the OPC regarding cross border outsourcing, the reach of the OPC and PIPEDA transcends provincial and national borders.

[29] *R. v. Dyment*, [*1988*] 2 S.C.R. 417

CHAPTER TWO

Youth Legal Consciousness and Social Network Privacy Issues

Lesley A. Jacobs

Introduction

In the brief history of digital technology and communications, there are certain significant watersheds – mobile telephones, e-mail, internet surfing, *YouTube,* social networking, texting – that have been characterized by transformations not just in terms of new opportunities to integrate digital technology into daily life but also by their rapid adoption among huge segments of the population. In Canada, as was noted in the previous chapter, the regulatory reach of the Office of the Privacy Commissioner of Canada (OPC) was extended significantly under PIPEDA in 2001. This extension of the regulatory powers of the OPC coincided with the explosion of social networking, in particular, the spread of *Facebook*. At present, *Facebook* itself claims that it has more than 500 million active users while other sources have reported that *Facebook* now has approximately six hundred and thirty million members worldwide.[30] Fifty

[30] Michael Oliveira, "Facebook not just for friends anymore as businesses makes it marketing network," *The Canadian Press*. 23Mar. 2011. Canadian Business Online . <http://www.canadianbusiness.com/ markets/ headline_news/article.jsp?content=b6340152>.

per cent of these members log on every day and the total membership usage amounts to more than seven hundred700 billion minutes per month.[31] There were an estimated twelve million Canadian users in 2009.[32] The OPC was a global pioneer in 2009 in its assertion that *Facebook* falls within its regulatory mandate, largely as a result of the PIPEDA. Since then, the OPC has investigated and issued reports about privacy complaints directed at *Facebook* as well as developed policy tools and educational initiatives that reflect this mandate.

This chapter examines, through a legal consciousness lens, privacy rights mobilization among youth aged 18-24 in Canada with regard to social networking, with a particular emphasis on *Facebook*. Within the community of law makers and policy analysts focused on privacy rights protection in Canada, and indeed the mainstream media generally, the important innovations by the OPC and other privacy commissioners have received much of the attention. This chapter is designed to encourage the undertaking of more research on the perspectives on legality and privacy among one of the largest user groups of social networking in Canada, youth between the ages of 18-24.

The starting point for this research is the intuition that, despite all of the important work done by the OPC, very few youth in Canada has neither any sense of the regulatory reach of the OPC nor its role as an agency for receiving and addressing complaints and concerns about privacy rights violations arising on *Facebook* or other social networking sites. The original research reported in this chapter is designed to improve our understanding of how youth aged 18-24 in Canada understand the ambit of privacy rights as it pertains to social networking and the intersection with law and legal regulation as a realm for addressing their concerns with privacy.

[31] Facebook website. <http://www.facebook.com/press/info.php?statistics>.

[32] Elizabeth Denham, "Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic(CIPPIC) against Facebook Inc. Under the personal Information Protection and Electronic Documents Act." (Ottawa: Privacy Commissioner of Canada, 2009): 6.

The chapter is divided into four sections; the first two is intended to provide the context for the original research findings reported in the third section. The first section provides some preliminary background on the recent history of digital social networking. The second section provides a brief overview of privacy issues with *Facebook*. The third section reports some of the significant findings of the interviews with youth in the study and provides a legal consciousness analysis of those findings. The fourth section identifies some of the policy implications of those findings.

There are, in summary, two main findings in the analysis of the findings. The first is that although almost none of the youth aged 18-24 interviewed identified federal legislation, the OPC or any other privacy commission as having a role in the protection of privacy rights in Canada, virtually all of them understood privacy and the ambit of privacy rights as pertaining to the access and use of personal information. This emphasis on personal information is a hallmark of modern privacy legislation in Canada such as PIPEDA and can be contrasted to some of the earlier emphasis in the legal construction of privacy on, for example, the protection of choices such as those pertaining to who should make decisions about terminating a pregnancy. The important point is that there is little or no gap between the legal consciousness of youth about privacy and how privacy is understood in PIPEDA. The second main finding is that when youth aged 18-24 were asked to imagine their privacy rights being violated through a social network site like *Facebook*, they identified three principal paths for responding – self-regulation, complaining to the site provider, or complaining to a legal/governmental institution. A more precise description of these avenues as well as the doing nothing response is described below. Only a quarter of those interviewed embraced the legal/governmental institution path as a default option; a small number saw it as an option should the other paths not be effective. A majority of

respondents preferred the path of complaining to the site provider. A quarter preferred the paths of self-regulation, which was about the same number as those who preferred a governmental/legal path. What is especially noteworthy is that neither the service provider nor the self-regulation path is seen as involving legal regulation or government policy.

Background on Social Networking

Social networking has been defined as "...web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system". [33] The range of social networking services is extensive, enabling special interest or niche market communication centres; the facilitation of professional and market based goods and services; the initiation and continuation of romantic relationships; and more generally a platform for the exchange of personal information such as photographs, birthdates, interests, and relationships.

In practice, social network websites are characterized by three defining features.[34] The first feature is that the network is composed of a body of individual profiles that are created and controlled by the user. The second feature is some measure of categorical lists of other users controlled by each individual user that allows access to his or her profile. Finally, these networks allow for communication between users through various long and short messaging

[33] Diana Boyd and N.B. Ellison, "Social network sites: Definition, history, and scholarship." *Journal of Computer- Mediated Communication* 13:1 (2007): 211.

[34] Ibid.

mechanisms, as well as through either public or semi-public forums. Social networking as a term of art can be understood as making reference to this sort of communication.

Social network websites have existed since 1997 and for the most part have been developed with a commercial purpose. How different websites generate revenue for their developers is varied. Websites such as *E-Harmony* or *LavaLife*, for example, are based on a business model that charges fees in order to facilitate dating and romantic relationships for users. Others showcase companies and firms for fee with the promise of connecting them to customers. However, the most significant development in social networking has occurred through a business model that generates revenue through targeted advertising, that is to say, advertising that is calibrated to the profile of the particular user. Social networking websites that now use this business model include *Facebook, MySpace, Classmates, My Yearbook, Friendster, Cyworld, Profile Heaven, Bebo, LinkedIn, Webshots, Face Party, Friends Reunited* and *Flickr*. In other words, users do not pay a fee to register or use their services.

Facebook is, of course, the exemplar of this last kind of social networking website, characterized by a general interest user base, a global reach, and the largest number of members of any comparable service.[35] It allows users to place an assortment of personal information including photographs and videos of their choosing onto an individual profile page and then link their page to any number of other profiles designated by the user as friends. The personal profile page also gives users an open ended "about me" section that allows for personal statements about concerns or relationships, or what they may be feeling, thinking or doing at the moment. Friends

[35] Elizabeth Denham,"Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic(CIPPIC) against Facebook Inc. Under the personal Information Protection and Electronic Documents Act." (Ottawa: Privacy Commissioner of Canada, 2009): 5. Facebook was launched in 2004 primarily for use by U.S. college students, but rapidly opened membership to any user with an email address.

can comment on the status of others, creating an ongoing dialogue among friends. *Facebook* also provides its own built in instant messaging service similar to MSN Messenger or AOL Messenger. In other words, friends can communicate either publicly using *Facebook's* wall or privately using the Message feature. Users can also play online games with other users. One of the especially notable features of *Facebook* is the ability of users to easily search and find points of contact with other users, for example, by allowing users to identify others who attended by the same elementary school. This sort of search engine is perhaps the clearest illustration of the new sorts of opportunities that social networking offers.

In 2009, *Facebook* claimed over three hundred and fifty million members and was reported to have annual revenues between seven to eight hundred million dollars.[36] Its membership has nearly doubled since then. The largest group of *Facebook* user's remains teens; in 2009 it was estimated that over half of all American teenagers use *Facebook*.[37] In Canada, sixty-six per cent of internet users use *Facebook*. [38] Roughly Seventy-five per cent of young people visit *Facebook* sixteen times a week, on average.[39] There has also been an increasing expansion of commercial use of *Facebook*. It has been reported in the media that there are fifty million daily connections between social users and businesses.[40] For example, according to

---

[36] "Facebook '09 revenue neared $800million. The Economic Times. 18 *Jun.* 2010. Reuters. <http://economictimes.indiatimes.com/infotech/internet/Facebook-09-revenue-neared-800-mn-Sources/articleshow/6063819.cms>.

[37] "How Teens Use Media: A Nielsen report on the myths and realities of teen media trends." < http://blog. nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf>

[38] People from Cossette (December 8, 2009) Press Release. <http://www.cossette.com/data/impact-social-press-release.pdf>; Nick Krewen, "Social media more than just a fad: studies," Media in Canada. (December 16, 2009). <http://www.mediaincanada.com/articles/mic/20091216/socialmediastudies.html>.

[39] People from Cossette. Press Release. (8 Dec. 2009). <http://www.cossette.com/data/impact-social-press-release.pdf>; Krewen, Nick (16 Dec. 2009). Social media more than just a fad: studies, Media in Canada. <http://www.mediaincanada.com/articles/mic/20091216/socialmediastudies.html>.

[40] Michael Oliveira, "Facebook not just for friends anymore as businesses makes it marketing network," *The Canadian Press* 23 Mar. 2011. Canadian Business Online Website. <http://www.canadianbusiness.com/ markets/ headline_news/article.jsp?content=b6340152>.

Facebook's director of public affairs, Tim Horton's has accumulated over 1.4 million *Facebook* fans since it first became a member in 2009.[41] It has since been buying ads, referred to as 'engagement units', and while it is still weighing the benefits of using the social networking site as an advertising outlet, the exposure it has garnered is immense.[42] The *Wall Street Journal* has projected that if there is a public offering of shares in Facebook in 2015, the value of the company will be more than one hundred billion dollars.[43]

What explains the popularity and attractiveness of social networking? In general, it is a reflection of the technological platform: an adaptable organizational structure that is based on the profiles of people, as opposed to one organized around a specific interest.[44] Another reason is that a website like *Facebook* provides a range of activities conveniently located in a single virtual space that otherwise in the non-virtual world would be far more time consuming.[45] This space enables connecting with family or friends at great distances relatively cheaply or creating a virtual living record through the posting of intersecting photographs, videos, ideas, thoughts, interests and experiences that can be accessed by friends, family and community.[46] The incorporation of micro-blogging features like current status updates or the relatively easy ability to comment on other users posts and statuses makes it a terrific up-to-date source for information. Surveys have shown that teens in particular use social networks as a source of

---

[41] Michael Oliveira, "Facebook not just for friends anymore as businesses makes it marketing network," *The Canadian Press* 23 Mar. 2011. Canadian Business Online Website. <http://www.canadianbusiness.com/ markets/ headline_news/article.jsp?content=b6340152

[42] Michael Oliveira, "Facebook not just for friends anymore as businesses makes it marketing network," *The Canadian Press* 23 Mar. 2011. Canadian Business Online Website. <http://www.canadianbusiness.com/ markets/ headline_news/article.jsp?content=b6340152>.

[43] "Investors bet on price of Facebook IPO." *The Wall Street Journal.* 4 Mar. 2010. 26 Mar. 2011. <http://blogs.wsj.com/digits/2010/03/04/investors-bet-on-price-of-facebook-ipo/>.

[44] Diana Boyd and N.B Ellison, "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication* 13: 1 (2007): 219.

[45] Mary Madden, "Older Adults and Social Media," *Pew Internet & American Life Project.* <http://pewinternet.org/Reports/2010/Generations-2010/Trends/Social-network-sites.aspx>.

[46] Mary Madden, "Older Adults and Social Media," *Pew Internet & American Life Project.* <http://pewinternet.org/Reports/2010/Generations-2010/Trends/Social-network-sites.aspx>.

information and advice.[47] Older Users aged 56-64, who constitute one of largest growing groups of social network sites, often use them to find people from their past or to connect with others facing similar situations such as retirement, change of career, or illness.[48]

Privacy and Facebook

Social network websites by their very nature traffic in personal information. The profiles created by users organize this personal information in a way that is easily readable and can readily be linked to particular individuals. At its outset in 2004, *Facebook* employed stronger privacy features and user control than other social network websites and initially benefitted from its exclusivity in terms of membership being restricted to college, university and professional organizations, which gave its users a strong sense of trust about who had access to their profiles.[49] *Facebook* has continued to update its privacy features with a commitment to make them more user-friendly. Currently, privacy options and settings are available that, in theory, give the user control over who can see their personal information and how much of it they can see. Users are provided with clear, detailed information regarding *Facebook* privacy practices and a simple process for adjusting privacy settings.

There are three main strands of concern about breaches of privacy involving *Facebook.* The first and most obvious concern is that personal information voluntarily published on *Facebook* by a user could end up being viewed by someone for whom it was not intended. For

[47] "How Teens Use Media: A Nielsen report on the myths and realities of teen media trends." <http://blog. nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf>.

[48] Kathryn Zickuhr, "Major Trends in Online Activities," *Pew Internet & American Life Project*. < http://pewinternet.org/Reports/2010/Generations-2010/Trends/Social-network-sites.aspx>.

[49] Alessandro Acquisti and Ralph Gross, "Imagined Communities: Awareness, information sharing, and privacy on the Facebook." *Proceedings of 6th Workshop on Privacy Enhancing Technologies* (Cambridge, UK: Robinson College, 2006): 36 at 2.

instance, if the privacy settings, which are controlled by the user, are weak the user's personal information and photographs may be visible to everyone. In fact, the privacy settings *Facebook* recommends are so weak that they would allow for the sharing of a users photos, posts, biography, favourite quotes, and family and relationship status with everyone on *Facebook*. The consequences of this level of visibility are hard to anticipate. It could, for example, damage a user's image with an employer. Ann Cavoukian, Privacy Commissioner of Ontario, warns: "Your activities, comments and views, even though you may have just been joking around with your friends, all become part of an online resume that, inadvertently or not, becomes available to everyone."[50]

The second concern revolves around disclosure of data generated by the decisions and choices users make while on *Facebook*. In 2007 *Facebook* launched *Beacon*, a marketing program designed to provide information on users buying habits and purchases in order to keep friends informed on each other's interests, but also to boost the sales of partnered commercial websites. In response to numerous privacy complaints and law suits, the program was shutdown in 2009.[51] According to one *Facebook* spokesperson, "We learned a great deal from the Beacon experience. For one, it was underscored how critical it is to provide extensive user control over how information is shared. We also learned how to effectively communicate changes that we make to the user experience."[52] In 2009, *Connect*, a new program by *Facebook*, was launched to

---

[50] Ann Cavoukian, "Reference Check: Is your Boss Watching? Privacy and you Facebook Profile. 24 Oct. 2007; Revised June 2010: 2. <http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=672>.

[51] Barbara Ortutay, **"Facebook to end Beacon tracking tool in settlement."** *USA Today* 24 Oct. 2007; Revised June 2010. *Associated Press.* 21 Sep. 2009. < http://www.usatoday.com/tech/hotsites/2009-09-21-facebook-beacon_N.htm>.

[52] Barbara Ortutay, **"Facebook to end Beacon tracking tool in settlement,"** *USA Today* 21Sep. 2009. < http://www.usatoday.com/tech/hotsites/2009-09-21-facebook-beacon_N.htm>.

replace the dismantled *Beacon* that allowed users to log-in to partnered websites using their *Facebook* log-in information and share their personal information. Significantly, *Connect,* unlike *Beacon*, was designed to place control over sharing with the users and not the advertisers.[53]

The third major concern involves "Applications," such as games operating within *Facebook*, which allow third-party access to personal information. The personal information of *Facebook* application users is purchased from *Facebook* by corporations, advertisers and marketing companies that thereafter target *Facebook* users with specific products based on their personal information. When enabling applications, *Facebook* users are asked to give permission for third-parties to access personal information in the context of a lengthy "terms of services" agreement that very few users are believed to have read. And of course if the user does not agree to the terms of service, then he or she will not be able to use the application.

In May 2008, a complaint filed against *Facebook* with the OPC by the Canadian Internet Policy and Public Interest Clinic under the *Personal Information and Protection of Electronic Documents Act* (PIPEDA) [54] resulted in Canada becoming the first country to lead a formal privacy investigation into *Facebook*.[55] In July 2009, the OPC released the findings of its investigation. Four complaints against *Facebook* were well-founded and resolved: collection of date of birth, default privacy settings, advertising, and monitoring for anomalous activity. Four other complaints were well-founded but still unresolved: third-party applications, account

---

[53] Barbara Ortutay, **"Facebook to end Beacon tracking tool in settlement,"** ***USA Today*** 21 Sep. 2009. < http://www.usatoday.com/tech/hotsites/2009-09-21-facebook-beacon_N.htm>.

[54] *PIPEDA Case Summary # 2009-008. CIPPIC v. Facebook Inc*. <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>.

[55] Susan Delacourt, (July 17 2009). "Facebook gets poked by Canada over Privacy." *The Star* 17 Jul. 2009. <http://www.thestar.com/News/Canada/article/667700>.

deactivation and deletion, accounts of deceased users, and the uses of personal information of non-users. In September 2010, the OPC announced that the outstanding issues had been resolved and the investigation was complete. [56] However, in late October of 2010, the Federal Government's Privacy Commissioner Jennifer Stoddart was reported to again be looking into *Facebook* over allegations that certain popular applications were still transmitting the personal information of users to third parties without consent.[57]

The Research Findings and Analysis

Over the period of eight months from July 2010 to February 2011, fifty-six youth aged 18-24 were interviewed in order to identify trends and patterns in their legal consciousness regarding privacy rights and social networking. All of the youth were interviewed individually. About a quarter of them also agreed to participate in a group interview. The youth interviewed came from very diverse ethnic, racial, and socio-economic backgrounds. There were roughly equal numbers of men and women. All live in the Greater Toronto Area and all are *Facebook* users. Each interview lasted between 25 to 60 minutes. The interview was organized around a sequence of open-ended questions that allowed the individual considerable latitude in his or her response.

[56] Office of the Privacy Commissioner of Canada, "Privacy Commissioner completes Facebook review." News Release. <http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.cfm>.

[57] Matt Hartley, "Privacy watchdog mulls fresh Facebook probe," *The Financial Post* 18 October. *The National Post.* <http://www.nationalpost.com/related/topics/Privacy+watchdog+mulls+fresh+Facebook+probe/3689323/story.html>.

The Legal Meanings of the Right to Privacy

The findings can be organized around two legal consciousness themes. The first theme pertains to how the youth understand what privacy amounts to and what having a right to privacy means. None of the youth appeared to have any knowledge of doctrinal law regarding these issues.

But every single one of them nonetheless offered an account of what privacy amounts to. Although these accounts are quite varied in their sophistication and precision, they are striking in so far as their convergence around the idea that privacy concerns personal information. The following is a brief sampling of these accounts in response to the question, 'What in your opinion is privacy?'

> "Privacy to me would be information that no else should know…I guess your SIN number, things like that, that no one else has a hold of." (#3)

> "Your personal space, personal identity, anything that pertains to you." (#9)

> "Something private, for instance your family life, you don't want it out there. You want everything to be private and don't want a third person knowing your business." (#12)

> "Privacy means having my personal information being protected." (#13)

> "I think privacy is for an individual or a group of people who want to keep their personal affairs and lives to themselves." (#15)

> "Information or fact about a person that is not publicized." (#17)

> "It's the things or information that someone would not want to give out." (#26)

> "Privacy would be characteristics of myself that I don't want other people to know about or disclosing information that I don't want other people to see or even um, hearing about." (#31)

> "Personal information that basically only you know, type of thing." (#32)

> "It's things that you don't want other people to see." (#52)

These accounts suggest that youth privacy is predominantly understood in terms of its relevance to personal information and identity.

The predominant understanding among the youth about what the right to privacy means reinforces this conclusion. Although some of those interviewed could not differentiate between what is privacy and what it means to have a right to privacy, most of those interviewed saw the right to privacy as a way to protect the sort of personal information that they associate with privacy. In particular, most understood a right to privacy as protecting the choice or control an individual has over who can see or has access to their personal information.

"Certain things that you are the sole owner of it." (#9)

"Right to privacy means that individuals should have the choice to what information about themselves they wish to share with the state or the public." (#10)

"a given or ethical privilege we have to control things that we consider to be private." (#11)

"I have the right to keep things, things that belong to me, its's my information…I would not want anybody to have access to it without my permission." (#13)

"The right to protect my information from unauthorized disclosure." (#18)

"The right to conceal what they wish." (#19)

"The power of making the decision of whether or not you want someone to know something about you." (#23)

"Who has access to private information and under what context that is given." (#27)

"Privacy rights are rights to keep personal information to oneself and to reveal it by own choice…I mean, only you can do it. Other cannot do it." (#37)

"People have the right to keep their own information private without harming others." (#39)

"Privacy rights are designed to protect the personal well being stuff that one would like to be kept from the general public…anything that is personal that should not be shared with anyone unless deemed ok by the person this belongs to." (#40)

"Privacy rights are the rights of concealing personal information. It is designed to protect the independence of each individual." (#45)

"When you have the right to privacy it means you get to pick when you want to be seen, and when you want to be exposed to the rest of the world." (#49)

"Privacy rights, like most other rights, allow you to make a decision on something is fundamentally your decision." (#51)

For most of those interviewed, a privacy rights violation arises when personal information is accessed without permission, full stop. A small number emphasized, however, that privacy rights are intended to protect us from the misuse of our personal information, and not simply access by third parties.

These revelations about legal consciousness are significant because of how well they mirror and track the understandings of privacy that are prevalent in recent legislation and the

popular media. In Canadian legislation such as PIPEDA as well as American legislation such as the newly proposed Kerry-McCain ‘‘*Commercial Privacy Bill of Rights Act of 2011*’’ restrict the reach of the right to privacy to personal information and who controls access to it. Canadian youth appear to have bought into this meaning of the right to privacy.

It is my suspicion that if I had asked a similar set of questions to Canadian youth two or three decades ago, the findings would have been different, a reflection of very different legal debates. As is well known, the United States Supreme Court initially constructed a constitutional right to privacy in the context of protecting the reproductive decisions of women. It did this initially in *Griswold v. Connecticut in 1965,* holding that the constitutional right to privacy created a protected sphere for married women to choose whether or not to buy contraceptives that could not be regulated by the criminal law.[58] Even better known is the opinion in *Roe v. Wade* in 1973 that the right to privacy protects women from criminal prosecution if they choose to have an abortion.[59] I suspect that the legal consciousness of youth in the 1970s or 1980s would have been more inclined to understand the right to privacy in terms of a sphere of personal decision making about sexuality and their bodies that was beyond the reach of the criminal law. My point is not that these earlier legal opinions accurately reflect the true ambit of the right to privacy, but rather to emphasize that the legal consciousness of contemporary Canadian youth aged 18-24 with its understanding of privacy in terms of control over personal information seem to have moved on, reflecting the current agenda of legal regulators concerned with information technology and a digital economy.

[58] *Griswold v. Connecticut,* 381 U.S. 479 (1965)
[59] *Roe v. Wade*, 410 U.S. 113 (1973)

Privacy Rights Mobilization and Facebook

Despite the finding that Canadian youth 18-24 have an understanding of what the right to privacy means that is very similar to that found in legislation like PIPEDA, it is a striking finding in the interviews that almost none of the youth are aware of the Office of the Privacy Commissioner of Canada or indeed that any such regulatory body of its kind exists in Canada. Many of the youth reported that they experienced some sort of privacy rights breach in the course of social networking. This breach amounted in most cases to a situation where the personal information on their profile or someone they knew had been accessed or shared with somebody without the permission of the user. For these youth as well as the others who were asked to imagine a situation where their privacy rights had been violated, less than a quarter of them thought they had ever experienced a privacy violation or indeed had pursued legal routes to complain. The law and government agencies like the OPC are at the margins of privacy rights mobilization for them.

In my analysis of the interviews, it is possible to identify at least four different responses to situations where privacy rights violations arise on *Facebook*. Some of the respondents envisioned taking more than one path, taking an initial path, and then a different one if that first path did not work out. The interviewer did not identify any possible paths; it was the youth who came up with possible responses. The findings suggest clearly that they are able to imagine only a limited set of options or paths.

One type of response was to acknowledge that their rights had been violated but to decide not to do anything about it. This sort of inaction as a response to a rights violation is often described as "lumping it". Sometimes lumping it is a reflection of the view that the privacy breach was not a significant one, at other times it is a reflection of not knowing what else to do, and at still other times it is a reflection of a worry that complaining will have negative repercussions. Only about fifteen per cent of the youth said they would lump it, even though my suspicion is that the likely number is much higher. The following are some examples of this type of response:

> "Most of the time I don't do anything about it because I do not know who gave out my personal information." (#14)

> "Yes, but I didn't do anything." (#20)

> "This depends on the situation. If it's a small stuff, I will be just upset for a while." (#25)

> "I would delete my account. I would erase everything. I would forget about it." (#30)

> "What can we do about this? She delete that guy. But that's all. *Facebook* cannot stop such kind of things." (#43)

> "I don't think we have any privacy rights while on social networks." (#46)

The second type of response is a form of what I term "self-regulation." By this, I mean that the youth takes actions himself or herself to avoid a similar sort of privacy rights violation in the future. This may mean in the case of *Facebook* making the privacy settings stronger or removing particular information like a date of birth or phone number or untagging a photo on another user's picture wall. I found that self-regulation is among those youth that were interviewed for the project, about quarter appealed to some form of self-regulation.

> "Take better care in deciding what information I share online or upload as well as frequently checking on the privacy settings placed on my account." (#11)

> "I believe that the individual should address their own concerns. If you are worried about privacy rights etc, do not use any social networking sites." (#15)

> "The site developers…although I don't have too many concerns about my privacy rights. I always think about stuff I upload and make sure I can delete stuff I upload, and things I really want to keep private." (#19)

> "You choose accordingly. You have to survey yourself in what you are posting." (#27)

> "De-activate. Even if you de-activate and you go back on, your information is still there. It doesn't get deleted. It didn't click to me. If I knew about it, I wouldn't have signed up." (#32)

"I reset my privacy account with more strict limitation." (#37)

"Sometime I can feel it when I found my own information released. So I tried to join less groups on *Facebook* and add less friends who you do not really know well." (#45)

The third type of response – the most frequent – is to complain as an individual to *Facebook* as the social networking site provider. Unlike the self-regulation option, this type of response relies on the privacy regulations of the service provider. The youth see themselves as consumers of the websites services and the situation of a privacy rights violation as a matter of customer dissatisfaction. The path is imagined to be a sort of online consumer complaint process. This type of response was identified by more than half of the youth in the study as their first response to a privacy rights violation while social networking. The following are a sampling of this type of response. Notice that many present this response as the first in a sequence.

"I am sure they have like a customer service privacy support centre, they have on the website, so if I have any concerns about privacy I should kinda send them a email." (#2)

"I think the Facebook Corporation…should be addressing as owners of the company…they are responsible for it. But I think I am part responsible for it as well…it's such a thin line because I think it's the responsibility of not just the people who own the company but also the people who are putting on information online. Because if you really want privacy then you won't be put anything online." (#3)

"The creator of *Facebook* and then if it is not enough, I think the fact that it is a big social network they should have a department that regulates it. So if it is not *Facebook* then the government." (#13)

"The administrators of those social networking." (#21)

"The guy who violated my privacy rights and the website people who are in charge." (#22)

"The host website. I think I would find out the people in charge and call them if it had happened to me." (#24)

"The administrators of *Facebook*, I guess, or like, the MSN people, the Hotmail people." (#28)

"I'd contact *Facebook* and be like, this is what happened." (#29)

"All I could do is was I got the control back on my email and I
emailed MSN Copyright – no MSN Privacy – and I made a complaint about it." (#31)

"If I had any issues in terms of privacy in terms of social networking, I would actually try to directly contact the person or CEO or creator I guess if that's possible, or the head

office and I guess their human resources or public relations and try to talk to them through that." (#33)

"The company/owner/designer of the online social network. I mean, if it's only a small issue, I can forget it and only talk with my close friends about it. But if it's a big violation, I will surely call the company." (#37)

"The network admin of the social network website. The company." (#40)

"The service provider who is benefiting from it should also regulate how it functions." (#41)

"I guess to a certain extent *Facebook* is accountable for the stuff it does with your information, but again the question is what they can be accountable for." (#48)

The fourth type of response is the pursuit of a privacy rights complaint about social networking through a government agency or in a legal venue. About a quarter of the youth presented this as the main option. Only a small number of the youth expressed an awareness of the existence of federal or provincial privacy commissions. Some were skeptical of government involvement at all.

"Government…government not going to do anything for you." (#2)

"I don't think government should. I think whoever created *Facebook* should address it...I don't think *Facebook* is such a big issue for the government to get involved." (#4)

"The government should. This is because the government is the one regulating these activities." (#5)

"In a broader sense, the Privacy Commission within Canada. But then when it comes to things such as *Facebook*, because it is of a global nature, I believe there should be a form of global body to regulate these realms." (#7)

"In Canada, I think the Privacy Commission. They should be the one initiating law to protect people." (#8)

"For something like *Facebook* I'm sure the government has regulations that binds them and, if not, the owner of the social network has something in place that people to voice their concerns or can complain." (#9)

"I would obviously file a complaint with *Facebook.* And depending on how serious it was or who it got to, I would go to law enforcement..I would start the bottom, local law enforcement." (#50)

The finding that so few youth imagine turning to the government when mobilizing on their rights is surprising and indeed interesting, given the fact that, as I emphasized above, almost

all of the youth understood the right to privacy in terms similar to that found in legislation and regulatory agency mandates.

Policy Insights

What are some of the policy insights for the Office of the Privacy Commissioner of Canada that follow from these findings? There are two that seem to me especially noteworthy.

One is that the OPC should continue to take seriously the self-regulation response to privacy rights breaches among youth. The OPC already has put considerable efforts into educational outreach to youth about protecting themselves and responding to privacy breaches. Concrete examples are its educational videos and the "Think Before you Click" program.[60] Another example is the OPC youth privacy website.[61] The insight is that realistically many Canadian youth are going to respond to privacy breaches with self-regulation; measures like this and others should take this response seriously.

The other insight concerns the finding that a majority of youth see the social network website provider as the principal avenue for seeking redress for privacy rights violations. Recall from the previous chapter that PIPEDA is organized around ten fundamental principles and that one of them is Challenging Compliance. Under PIPEDA an individual is entitled to challenge the organization's compliance to the privacy principles by launching a complaint with the person responsible for the organization's compliance and that these organizations implement complaint

[60] Office of the Privacy Commissioner of Canada, "Privacy and Social Networks, What does a friend of a friend need to know about you?"< http://blog.privcom.gc.ca/index.php/privacy-on-social-networks/; and http://www.youtube.com/Privacycomm.>

[61] Office of the Privacy Commissioner of Canada. *My Privacy. My Choice. My Life.* <http://www.youthprivacy.ca/en/>.

procedures that are easy to access and understand.[62] This suggests to me that the OPC should begin to work closely with the social network companies and organizations in Canada that have a long history of developing civil society-based consumer protection models such as the Consumers' Association of Canada. In other words, in addition to investigating and pressuring *Facebook* and other social networking companies, the OPC should take more seriously in the context of social networking how consumer protection models can be utilized to better facilitate privacy rights mobilization.

[62] Protection of Personal Information and Electronic Documents Act, 2000, c. 5, Principle 4.10.2.

CHAPTER THREE

Legal Consciousness, Recent Immigrants, and E-Finance Privacy Issues

Lesley A. Jacobs

Introduction

Like many other daily routines, developments in information and digital technology have transformed how many banking and financial transactions in Canada are performed. The evolution of electronic financial transactions (e-finance) has impacted not just how business is conducted but also how ordinary Canadians receive their wages or pensions, do their banking, buy and sell things, pay bills, apply for loans, renew mortgages, transfer money to others, and make cash withdrawals. Although banking and financial transactions have always been a field that has received greater scrutiny for privacy breaches, the development of wide spread engagement by ordinary Canadians with e-finance has reinvigorated this concern about privacy. In Canada, as was noted in Chapter One, new federal privacy legislation (PIPEDA) was enacted in 2001 with a specific emphasis on concerns about the rapid developments in e-finance. This

legislation extended the regulatory reach of the Office of the Privacy Commissioner of Canada into the privacy sector

This chapter examines through a legal consciousness lens privacy rights mobilization with regard to e-finance among one segment of the Canadian population – recent immigrants. Within the community of law makers and policy analysts focused on privacy rights protection in Canada, and indeed the mainstream media generally, the important innovations by the OPC and other privacy commissioners have received much of the attention. This chapter is designed to encourage the undertaking of more research on the perspectives on legality and privacy among one marginal segment of the general population.

The starting point for the research reported in this chapter is curiosity about whether recent immigrants in Canada have unique understandings of the legal meanings that attach to privacy rights and how this might be reflected in their views on privacy rights mobilization involving e-finance. Recent immigrants are defined in the study as those who gained landed immigrant status in the past five years. The working assumption is that these recent immigrants, like most other ordinary Canadians, engage with e-finance and that this engagement has the potential for privacy issues to arise. The original research reported in this chapter is designed to improve our understanding of how recent immigrants in Canada view the ambit of privacy rights as it pertains to e-finance and the intersection with law and legal regulation as a realm for addressing their concerns with privacy rights violations.

The chapter is divided into four sections, the first two are intended to provide the context for the original research findings reported in the third section. The first section provides some preliminary background on recent developments in e-finance in Canada. The second section

provides a brief overview of privacy issues that arise in e-finance and the regulatory response by the federal government. The third section reports some of the significant findings of the interviews with recent immigrants in the study and provides a legal consciousness analysis of those findings. The fourth section identifies some of the policy implications of those findings.

There are, in summary, two main findings in the analysis of the findings. The first is that although almost none of those interviewed identified were acquainted with federal legislation, the OPC or any other privacy commission as having a role in the protection of privacy rights in Canada, virtually all of them understood privacy and the ambit of privacy rights as pertaining to the access and use of personal information. In this respect, recent immigrants are remarkably similar to the youth aged 18-24 who were interviewed for Chapter Two of this study. The emphasis on personal information is, as I emphasized in the previous chapter, a hallmark of modern privacy legislation in Canada such as PIPEDA and can be contrasted to some of the earlier emphasis in the legal construction of the right to privacy on, for example, the protection of choices such as those pertaining to who should make decisions about terminating a pregnancy. The important point is that there is little or no gap between the legal consciousness of recent immigrants about privacy and how privacy is understood in PIPEDA. The second main finding is that when recent immigrants entertained privacy rights mobilization, many of them expressed frustration about not knowing what their options are and when they did identify paths for complaining about privacy rights violations should they arise in e-finance, they identified two paths, complaining to the financial service provider or to the police. Unlike youth aged 18-24 involved with social networking, as reported in the previous chapter, recent immigrants did not blame themselves for privacy rights violations that arise in e-finance and opt for responses that constitute what was described in Chapter Two as self-regulation.

Preliminary Background on E-Finance

In comparison to many of the watershed developments in information technology and digital communication such as social networking or texting where five years is a lifetime, e-finance has developed in Canada over a much longer period of time. In many respects, financial institutions in Canada have been pioneering information technology innovations since the wide spread introduction of ATMs in the late 1970s. For our purposes, however, the emphasis in this chapter is on e-finance in so far as financial transactions have integrated internet technology.

Although bank websites are the most common site for e-finance in Canada, it is important to recognize the diverse character of the financial service sector and its capacity to facilitate e-finance. This is, for instance, especially evident in the so-called cheque-cashing industry in Canada. This sector has experienced exponential growth over the past decade and is utilized largely by vulnerable and marginal persons including recent immigrants. Significantly, this industry is not regulated by the federal government at all and is only loosely regulated in most provinces.[63] Non-banking financial services companies engaged in e-finance are often called Money Service Businesses (MSB). A MSB can be defined as "an individual or an entity that is engaged in the business of any of the following activities: foreign exchange dealing; remitting or transmitting funds by any means or through any individual, entity, or electronic funds transfer network; and/or issuing or redeeming money orders, traveler's cheques or other similar

[63] See the report by the Law Commission of Ontario, "Fees for Cashing Government Cheques Final Paper"(November 2008), which is available at http://www.lco-cdo.org/en/cheque-cashing-fees-final-paper (last accessed: 27 March 2011).

negotiable instruments."[64] There are nearly 1000 registered MSBs in Canada but it is likely that many others are not registered. Among registered MSBs, 73% reported providing remitting or transmitting funds services and 80% provided foreign exchange services in 2008-2009.[65] E-finance also occurs on numerous non-bank websites with a Canadian domain address or a domain address based elsewhere.

The use of online banking is widespread in Canada. In 2009, 63% of Canadians reported using online banking. [66] Almost half reported using the Internet as their primary means of banking.[67] The online banking services utilized by the vast majority of online users include checking their account balances, paying bills, and transferring funds.[68] The Canadian Bankers Association's Bank Crime Prevention and Investigation Office (BCPIO) is a designated investigative body that seeks to protect banks and their customers from credit card and debt fraud, money laundering, and internet crimes such as hacking and phishing.[69]

E-finance has made international financial transactions easier and quicker. eBay for example is estimated to host more than 1 million transactions a day worldwide.[70] These electronic financial transactions typically involve the use of a credit card or some sort of online third-party payment service like PayPal. PayPal, which is owned by eBay, reportedly is used

---

[64] See Financial Transaction and Reports Analysis Centre of Canada "Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MCBs)" (July 2010), p. 3, available online at http://www.fintrac-canafe.gc.ca/publications/typologies/2010-07-eng.pdf

[65] ibid.

[66] Canadian Bankers Association, How Canadians Bank, available online: http://www.cba.ca/en/media-room/50-backgrounders-on-banking-issues/125-technology-and-banking (last accessed: 26 March 2011)

[67] ibid.

[68] ibid.

[69] Phishing refers to the use of "...e-mails and fraudulent websites designed to fool recipients into divulging personal information such as credit card numbers, account usernames and passwords, social insurance numbers, etc. By "impersonating" the trusted brands of well-known banks, online retailers and credit card companies, phishers try to convince recipients to respond to them and provide them with the personal information necessary to do financial transactions fraudulently or for identity theft". See Government of Canada, Canadian e-Policy Resource Centre, online: http://www.ic.gc.ca/eic/site/ceprc-ccrcp.nsf/eng/00025.html

[70] http://ebaystrategies.blogs.com/ebay_strategies/2009/12/fun-ebay-math-what-does-14-million-cyber-monday-transactions-mean.html (last accessed: 28 March 2011)

more than 2 million times a day. Euronet Worldwide, one of the many large companies that specializes in the facilitation of international electronic financial transactions, reported that in 2009 it had processed approximately $50 billion through automated tellers, prepaid and money transfer payments for over 115 financial institutions, 320,000 retailer, and millions of customers in 46 different countries.[71]

Many recent immigrants to Canada transfer money internationally, mainly to family members in their country of origin. The World Bank estimated that in 2008 $338 billion was transferred by immigrants worldwide to their countries of origin.[72] These international transfers occur through both formal and informal means. Banks are the most common formal means to send money, followed by money transfer operators and exchange bureaus.[73] Banks, money transfer operators, post-offices and exchange bureaus are the most common formal ways to receive money internationally.[74] There is a lack of sufficient regulation and data collection on informal means of international money transfers.

International e-finance has received increased legal scrutiny, especially since 9-11, because of concerns about money laundering and terrorist financing. The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is an independent intelligence agency created in 2000 with a mandate, "to facilitate the detection, prevention and deterrence of money laundering, terrorist activity financing and other threats to the security of Canada".[75] FINTRAC was established through the *Proceeds of Crime (money Laundering) and Terrorist Financing Act*

---

[71] Euronet Worldwide 'about us', available at www.euronetworldwide.com/our_company/businesses.cfm (last accessed: 26 March 2011)

[72] Jacqueline Irving, Sanket Mohapatra & Dilip Ratha, *Migrant remittance Flows: Findings from a Global Survey of Central Banks*, (Washington, D.C.: Office of the Publisher, The World Bank, 2010), p. 1.

[73] Irving et. al., p. 11.

[74] Irving et. al., p. 11.

[75] FINTRAC 'Who We Are', available at www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp (last accessed: 28 March 2011)

(PCMLTFA) and its related regulations.[76] FINTRAC disclosed 556 cases in the 2008-2009 year; 474 of these involved money laundering, 52 terrorist financing and threats to national security.[77]

Privacy and E-Finance

E-finance presents diverse opportunities for privacy rights violations ranging from mere sharing of personal financial data to credit card fraud to identity theft. Most e-financial transactions in Canada are subject to regulation under PIPEDA. When PIPEDA was first introduced on January 1, 2001, it applied immediately to banks and in 2004 was broadened to incorporate all commercial activities undertaken by private sector organizations throughout Canada unless a province enacted legislation that was considered substantially similar to it. In other words, the privacy rights protections that were created through PIPEDA exist in part to regulate the diverse opportunities for rights violations presented by e-finance.

From the government's perspective, as I noted above, e-finance is risky not only for its potential threats to privacy but also because it can be used to commit crimes ranging from fraud and theft to money laundering and funding terrorist activities. The institutions that the government has created to investigate and prevent these sorts of crimes are themselves potential threats to the privacy of individuals who utilize e-finance. The Office of the Privacy Commissioner of Canada has jurisdiction to investigate complaints against FINTRAC under the Privacy Act. FINTRAC itself holds that the protection of privacy is one of the most important

[76] FINTRAC 'Who We Are', available at www.fintrac.gc.ca/fintrac-canafe/1-eng.asp (last accessed: 28 March 2011.

[77] See Financial Transaction and Reports Analysis Centre of Canada, p. 19.

aspect of its operations and that it's enabling legislation, contains specific provisions that reflect the principles outlined in the Privacy Act, and the Canadian Charter of Human rights and Freedoms.[78] FINTRAC has several policies and procedures in place that protect individual privacy when dealing with information under its control including the 'need-to-know principle', specific guidelines for dealing with sensitive and classified information, and strong mechanisms for dealing with analysis and disclosure of information.[79] In the same way that FINTRAC is subject to the Privacy Act and Access to Information Act, similarly The Canadian Bankers Association's Bank Crime Prevention and Investigation Office is subject to PIPEDA.

The Research Findings and Analysis

Over the period of four months from November 2010 to February 2011, 24 recent immigrants to Canada were interviewed in order to identify trends and patterns in their legal consciousness regarding privacy rights and e-finance. All of the recent immigrants were interviewed individually. Each interview lasted between 25 to 60 minutes. The recent immigrants all had come to Canada in the past five years and were from diverse ethnic and racial, backgrounds. Their countries of origins were in Eastern Europe, the Middle East, Africa, and Asia. There were roughly equal numbers of men and women. All live in the Greater Toronto Area and all had experience with e-finance. 90% of them had sent money to their country of origin from Canada using electronic financial services such as bank wire transfers, Western

[78] FINTRAC "Privacy Protections", available at www.fintrac.gc.ca/fintrac-canafe/atip-aiprp/pp-prp-eng.asp (last accessed: 26 March 2011)

[79] FINTRAC "Privacy Protections", available at www.fintrac.gc.ca/fintrac-canafe/atip-aiprp/pp-prp-eng.asp (last accessed: 26 March 2011)

Union, or MoneyTrac. The interview was organized around a sequence of open-ended questions that allowed the individual considerable latitude in his or her response.

The Legal Meanings of the Right to Privacy

The findings can be organized around two legal consciousness themes. The first theme pertains to how the recent immigrants understand what privacy amounts to and what having a right to privacy means. Few appeared to have any detailed knowledge of doctrinal law regarding these issues.

Like with the youth aged 18-24 reported in the previous chapter, although the accounts of the rights of privacy provided by the recent immigrants are quite varied in their sophistication and precision, they are striking in so far as their convergence around the idea that privacy concerns personal information. The following is a brief sampling of these accounts in response to the questions, 'What in your opinion is privacy?' and 'What are privacy rights designed to protect?':

> "If for example maybe I go for an interview, someone asks me 'are you married?' or "how many children I have', those are my privacy. I don't expect such questions to be asked in interview." (#1)

> "My identity, my rights." (#2)

"Privacy rights in my opinion is the right to that you have to keep something secret, or the information that you want to keep secret." (#3)

"You have the right to keep information, your private information to yourself, not to disclose it to anyone." (#4)

"To protect personal information." (#7)

"Something that I can keep it to myself." (#8)

"It's a secret and it just stays with you and your family." (#11)

"Privacy is personal information." (#12)

"Privacy in general is just your personal information not to be shared with anyone else without your consent." (#13)

"Privacy means like...anything you have that other people don't know or should not know." (#22)

These accounts suggest, as was the case of youth, how prevalent it is to understand privacy in terms of its relevance to personal information and identity, which is consistent with the current agenda of legal regulators concerned with information technology and a digital economy.

Privacy Rights Mobilization and E-Finance

Despite the finding that the recent immigrants interviewed have an understanding of what the right to privacy means that is very similar to that found in legislation like the Privacy Act and PIPEDA, many of them expressed concern that they did not know what to do if they experienced a privacy rights violation while using electronic financial services and that this was a major point of frustration for them, as is evident in the following sample of comments:

"I don't think immigrants know everything; how to use their rights." (#2)

"I didn't know anywhere else to go I went to UNHRC and I made a complaint." (#3)

> "If it would be more obvious who I should contact in this case, then I would do that. So obviously I didn't have this information in hand, you know, handy, to react straight away." (#4)

> "There is nowhere to complain I think. I don't have names, I don't have numbers. I won't call to police yeah, they would look at me or hear me and say, 'What are you talking about?'" (#6)

> "Everyone is entitled to complain, but I just think that in order to access the proper channels, it's harder." (#15)

> "I wouldn't know where you would go to complain. I don't know if there is an agency ...so it's a hard question because where do you go?" (#17)

This finding contrasts significantly with the youth interviewed in the context of social networking who had no difficulty identifying possible paths to complain about privacy rights violations.

Distinct from those who worried about where or how to pursue a complaint about a privacy rights violation in e-finance were those who acknowledged that their privacy rights might have been violated but decided not to do anything about it. In the previous chapter, I characterized this sort of inaction as a response to a rights violation as "lumping it". Lumping it reflected in the interviews a range of views including that the personal information that was

accessed was not significant, that pursuing a complaint is only worthwhile if money was lost, or that whatever organization you might complain to – the bank, the police, the government – would not take the side of the person complaining any way, which makes complaining futile. The following are some examples of this type of response:

> "I might be upset at that time but I think about it and maybe let it go later. Except if they are withholding the money." (#5)

> "I am not the type of person to complain, you know. But they keeping you on file and they keeping all your transactions whenever you do that. You know, they can see how much, what time and when you send this amount of money and the person to who you send it...You like it's not a big of a deal but its like privacy too." (#6)

> "I just walked away, and didn't think too much of it. It bothered me initially but then I thought what's that person really going to do with that information." (#13)

> "If you go and do something with the police or something like that, they're always going to protect each other, depending on where you go. If you go to the government, depending on what it is, they're going to try and protect each other again." (#14)

It is interesting to notice that unlike in the context of social networking, individuals involved in e-finance do not blame themselves or assume partial responsibility for privacy breaches. This explains, I suspect, why although many of those recent immigrants interviewed are willing to lump rights violations, they do not see what I labelled self-regulation in the previous chapter as a serious option.

Those others who did identify paths to respond to a privacy rights violation in e-finance limited their options to complaining to the service provider in the form of a type of customer complaint process or to the police. The latter is a reflection that for most of them they imagine the privacy breach leading to theft or fraud, which is evident in the statements below:

> "Somebody was able to access my bank account and withdrawal money after using my bank card to buy something from the grocery shop. I went to the police, reported it, and then I went to a lawyer to swear an affidavit so that the bank would pay for it." (#7)

> "Every business and institution should have their own privacy laws." (#16)

> "I guess I would go to the branch manager or the police." (#22)

The important implication is that the resolution of the privacy rights violation would be the repayment of their lost funds.

Policy Insights

What are some of the policy insights for the Office of the Privacy Commissioner of Canada that follow from these findings?

One is that the OPC should consider developing an educational outreach that addresses the very specific concerns expressed in these interviews by recent immigrants about not knowing what to do if their privacy rights have been violated in the course of e-finance. Obviously, this could be done in cooperation with Canada's banks, many of them already having developed marketing strategies deliberately designed to establish customer loyalty among recent immigrant communities.

The second related insight, like in the case of social networking, is the importance of furthering the principle of Challenging Compliance under PIPEDA. That principle emphasizes that an individual is entitled to challenge the organization's compliance to the privacy principles by launching a complaint with the person responsible for the organization's compliance and that these organizations implement complaint procedures that are easy to access and understand.[80] Most financial institutions in Canada, and in particular the big banks, have well established customer complaint processes including ombudspersons. What is important is that these customer service models come to be viewed by recent immigrants as the appropriate first stop for expressing their concerns about privacy rights violations.

[80] Protection of Personal Information and Electronic Documents Act, 2000, c. 5, Principle 4.10.2.

CHAPTER FOUR

Privacy, Communications and Seniors

Kim Sawchuk and Barbara Crow

Introduction

There has been a radical transformation in how, where, when and why we communicate. Who would have imagined that we would be carrying lightweight phones to access our family and friends in less than a heartbeat? One generation of Canadians who have witnessed a radical transformation in wireless telecommunications, from the radio to the hands-free cellular (mobile) phone, have been those referred to as 'seniors'.[81] Despite this generation's experience with a variety of new media in their lives, this cohort often is absented and silenced from considerations of design, policy, costs or privacy concerns. In this report, we examine how two communities of Ontario seniors articulate the interconnections between telecommunications and privacy, what we call a privacy repertoire. This repertoire, which is distilled from their direct life experiences, their observations of the world around them, and their engagements with the media, has implications for policy-makers and legal scholars who seek to engage with the public, and

[81] For the purposes of this study, we define seniors as those who are 65 years of age and older.

provide meaningful services to them. What legal experts say about privacy and the law will be interpreted from within this set of understandings.

To summarize, the twenty-four people in this research project are of the opinion that their privacy is being eroded and that people have less privacy now than they did in the past. Technology, in general, is positioned as being culpable for this erosion. More specifically computers, the internet and social media - *Google, Twitter* and *Facebook* - are blamed. This repertoire is largely derived from their observations of the world around them, including their observations of children and grandchildren. However, in offering this assessment it is important to note that the cohort we interviewed neither use social media nor own computers. Yet, they do have direct experience with technology in other areas of their lives, which they identified, and linked to our questions about privacy. They understand that an information society "numbers you" and that information is collected through a variety of means including: magnetic stripe cards; pin numbers and chips; debit cards, credit cards; and most critically for our group in the Jane-Finch corridor, through their health cards and drivers licenses.

They also offered insights into how they take measures to protect their privacy. However, their responses indicate a mistrust of public or social means to curtail incursions into their privacy. Privacy was often expressed as a violation of their personal space (or their time) either by unwanted sales people, people wanting to conduct surveys or from government agencies. They spoke of putting their names on no-call lists, hanging up the phone if they were surveyed, monitoring to whom they gave their phone numbers and credit cards, and attempting to take care of their personal information by limiting its circulation. They expressed wonder that their home phones were still accessible to unwanted forms of solicitation despite these measures. Yet when asked about their privacy rights, or legal recourse, a sense of fatalism was expressed by our

participants. Legislation or government regulation is not seen as an adequate measure to "protect privacy." The fear is that legislation will incur a cost to them; give the government more power or be impossible to enforce.

To a certain extent, this attitude is derived from their context. The groups we spoke to are not simply marginal, socio-economically speaking: they are marginalized and live in conditions where they rely on government services, such as social housing and health care, which means that their personal housing spaces, and their lives, are under the scrutiny of social service agents. This context informed their discussions of privacy in general and digital privacy, in particular. As mentioned, most of our participants did not own computers, and only half owned their own cell phone. As a result, our discussions of privacy often returned to issues of the protection of personal space, their right to keep information from others, to keep secrets, to maintain confidentiality and trust, and to be alone and undisturbed. When privacy was discussed with respect to digital information, it often concerned the right to protect both one's home space from intrusion, or one's time from unwanted salespeople or surveys.

Finally, there was unanimous agreement that they do not know their privacy rights and despite their fatalism regarding government regulation, they do think they need to know about their privacy rights. Here, there is an opportunity for further work for social policy-makers and legislators. Any discussion of privacy within these communities will need to engage their pre-existing conceptions of privacy as personal responsibility, and deal with their mistrust of government agencies to protect them or to advocate on their behalf. It will also need to take into account their limited and infrequent use of digital tools (like the computer) and realize that privacy issues are contextualized by their understanding of technology and data-gathering.

Finally, advocacy work on privacy rights may be best promoted in the public milieus that matter to these people: their local community centres.

In summary, while our results are not definitive – since this is a pilot study involving two distinct and very specific communities of Torontonians – we think that this research has value, if only to bridge the chasm between academic privacy advocates and the populations they seek to serve. It points to the need for policy-makers and legal scholars to take into account the influence of 'popular' repertories and understandings of privacy when advocating information campaigns that may target specific populations of seniors, or indeed other social groups. It also provides an initial set of findings that can act as a set of potential research guidelines for future studies on the highly contextual repertoires of privacy circulating in the digital age.

What follows is a more detailed analysis and assessment of these issues.

Privacy and Aging

The Canadian population is aging: seniors now number 4.2 million.[82] By 2031, it is estimated that approximately one out of every four Canadians will be 65 years or older and that by 2056, one out of every ten Canadians will be over 80 years of age.[83] Life expectancy has risen in the past decades and is currently at its highest in Canada at 80.7 years, up from 78.4 years a decade ago. Women's life expectancy has increased by 1.8 years while men's life

[82] Statistics Canada, "Deaths, 2007." *The Daily* (February 23, 2007a): 2–3.

[83] Canadian Institute of Health Research, The future is aging: The CIHR Institute of aging strategic plan 2007-2012. Vancouver: Institute of Aging, 2006. 16 August 2010: 9. <http://www.criugm.qc.ca/fichier/pdf/plan_strategique_IRSC_anglais.pdf>.

expectancy has risen by 2.9 years.[84] At the same time as we age as population, we continue to work: our participation in the paid work force 'after retirement' continues to increase. Between 1996 and 2006, the employment rate for seniors rose from 12 per cent to 15 per cent for men and from 4 per cent to 6 per cent for women, following declines during the 1980s and 1990s. Senior men and women in the highest and lowest levels of the family income distribution were more likely to be employed than those in the middle income range.[85]

In terms of wireless mobile communications, the explosion of devices, world-wide has been dramatic. Currently, most of Europe, Japan and Hong Kong have a mobile telephone adoption rate that exceeds 100 per cent.[86] The number of cellular telephone subscribers in Canada has increased from 3.5 million in 1997 to 22.8 million in 2009.[87] However, Canadians have had lower and slower rates of cellular telephone adoption compared to other countries, due in part to the relative inexpensiveness of landline telephones and the provision of comprehensive public telephone services. This economic and regulatory context partially explains why seniors have been reticent to own or use mobile telephones: in Canada we have been able to rely on inexpensive and reliable landline services for communicating with family and friends.

As industry studies have shown, the turn to cellular communications has not been uniform across the different geographic regions of the country, nor is it spread evenly throughout

---

[84] Statistics Canada 2007a: 2.

[85] Sharanjit Uppal, "Labour market activity among seniors." *Statistics Canada: Perspectives on Labour and Incomes* 7 (2010): 5–18.

[86] International Telecommunications Union. "The world in 2010: ICT facts and figures."23 February 2011. <http://www.itu.int/ITU-D/ict/statistics/>.

[87] Canadian Wireless Telecommunications Association, *2008 Wireless Attitudes Study.* (Ottawa: Harris-Decima, 2008).

the Canadian population.[88] Indeed, one of the lowest rates of adoption is amongst those we call seniors. A 2008 report by the wireless industry indicated, while "cell phone penetration by age was at 73 per cent for those between ages 18 to 34, and at 66 per cent for those from 35-54, only 40 per cent of people aged 55+ owned a cell phone." [89]

Clearly, this shift in demographics will have seniors constituting a larger portion of the Canadian population. While the rates of adoption of mobile communications are lower than the rest of the population what remains to be seen is how this will change in the future, when the current cohort of cellular telephone users ages. However, with the proliferation of mobile, wireless communications and the increased delivery of government services in digital formats, the increasing numbers of seniors in the Canadian population, their continued reliance on landline telecommunications, and their lower uptake of mobile communications, it is imperative that we take into consideration the insights and needs of seniors living in the present context.

To date, most of the research on mobile telephone use has focused exclusively on youth. The adaptive[90] and resistant[91] practices of youth are seen as heralding new ways of communicating and redefining communication through their desire for perpetual and continual contact. The minimal research existing on the 'older' mobile telephone user tends to focus on these technologies in relation to health care delivery.[92] Those who are not shaped by these promises are all too often ignored when it comes to considering use and design, or matters of privacy.

---

[88] CWTA 2008.

[89] CWTA 2008.

[90] Y. S. Lee, "Older adults' user experiences with mobile phones: User cluster identification." *Proceedings of the 21st International Symposium: Human Factors in Telecommunications, User Experiences of ICTs.* Kuala Lumpur, Malaysia, 2008.

[91] R. Ling, "Should we be concerned that the elderly don't text?" *The Information Society* 24 (2008): 334-341.

[92] Eric Dishman, "Inventing wellness systems for aging in place." *IEEE Computer Society* 37:5 (2004): 34-41.

A number of scholars have described the availability of digital images, texts and sounds that are readily available online, as a digital trail or an 'identity' trail.[93] This research has raised concerns about who owns digital images, texts and sounds, how users remove their digital representations from various sites and contexts, and what protection and/or avenues users have when these digital representations move from one context to another without their permission and/or knowledge. The focus of this work has been on authentication, anonymity and net surveillance. These are critically important interventions, as they consider how digital information technologies are transforming what we know, who knows it, and who owns it.

Given this articulation and the imperative to understand how context shapes one's experience and social values pertaining to privacy, this small pilot study helps to understand and advocate for lower-income seniors in a digital context by including their voices, and knowledge in the debate. As a part of our research on 'seniors and cell phones,' we were commissioned to explore how seniors understood privacy in relation to mobile, wireless communications as well as in terms of social networking, including their uses of social media sites such as *Facebook* and *Twitter.* The vast majority of our respondents do not use these sites themselves, so they had little to say about the internet or social media based on direct experience. They did, however, have many observations on privacy as it related to the popular media, their observations of their friends and family, as well as their own experiences of surveillance and the breaching of their "privacy boundaries". The seniors in our study describe their everyday encounters with digital technologies and articulate their concerns with the question of 'privacy' in the age of digital data-gathering as an 'erosion' linked to the proliferation of computerization: for those in the Jane Finch corridor, the discussion largely centred on data-gathering through health cards, while for

[93] Ian Kerr, Valerie Steeves and Carole Lucock, eds. *Lessons from the Identity Trail: Privacy and Identity in a Networked Society*. (New York: Oxford University Press, 2009).

those in the downtown core, the major specific concern was with data-gathering related to housing. Both groups, however, were very concerned about the incursion of unwanted telemarketing, via the landline phone, into their homes pointing to the continued reliance on this device for communications. Our research suggests that seniors can be served better as a constituent group if we understand where they get their information, what kind of digital technologies they own, and their overall literacy (and engagement) with these devices.

In this pilot study, a number of themes emerged to form a part of a constellation of observations, explanations and analyses that we call a privacy repertoire, a type of interpretive repertoire (see Appendix A). By interpretive repertoire, we follow Potter and Wetherell's suggestions that such repertoires are "recurrently used systems of terms used for characterizing and evaluating actions, events and other phenomenon."[94] As Joke Hermes explains, interpretive repertoires are "a storehouse of possible understandings, legitimations, and evaluations that can be brought to bear on any number of subjects."[95]

In developing this privacy repertoire, our analysis relies on the verbal testimony of four focus groups conducted with twenty-four seniors in downtown and uptown Toronto, Ontario in November, 2010. The participants' ages ranged from fifty-eight to seventy-five with an average age of sixty-nine. Most of the participants in our York Gate group had immigrated to Canada in the last thirty years from the West Indies; the group from the downtown core was largely comprised of second and third generation Canadians of European descent. Participants included seven men and seventeen. Most of them participants had some high school education: three had

[94] Jonathan Potter and Margaret Wetherell, *Discourse and Social Psychology: Beyond Attitudes and Behaviour*. (London: Sage, 1987): 149.

[95] Joke Hermes, *Reading Women's Magazines: An Analysis of Everyday Media Use.* (Cambridge, Massachusetts: Polity Press, 1995): 203.

some college or university education. The overwhelming majority of participants in both groups had incomes under $20,000 per year. Recruitment of participants was undertaken through two sources. The downtown group was accessed through personal connections. As a result of a personal friendship, participants were recruited from a seniors' community centre. The majority of the research participants in the downtown location spend a minimum of three days per week at this Centre. For many of them, the community centre was their lifeline and place to seek out others their own age and to access community.

The second group was recruited from another study conducted by the authors earlier in the year. As a result of the previous study, the seniors were eager to participate in another round of questions about mobile technologies. We accessed this group through York University's TD-Community Centre. The Centre links university researchers with local community members to build research capacity and relationships between the university and the community. Through the Centre, we recruited participants from a local seniors' centre. This group did not spend as much time at the seniors' centre as the downtown group; however, they articulated the significance of the Centre as a place to spend time with other individuals their own age.

It has been our experience that working with seniors in small groups works better. We have also found it useful to separate mobile telephone users and non-users when discussing these matters. The smaller groups allow for more intimacy, time to process questions, and the ability to facilitate dialogue amongst all the members of the group. Dividing the groups into users and non-users gives non-users a space at the discussion table that would otherwise be dominated by users.

For this research project, we conducted four focus groups with six participants in each (one group of users and the other group of non-users) and the sessions were no more than two hours. The two authors conducted the focus groups and the groups were audio-recorded and transcribed with the participants' permission. Questions were set out by the primary researcher, Professor Lesley Jacobs, in his application to the Office of the Privacy Commissioner of Canada (OPC). While we tried to follow the questions set out, the prior discussion we had facilitated with these groups of users – which had been in an informal manner – as well as the absence of their direct experience with computers and social networking meant that we had to tailor the questions to this particular group of seniors. In addition, the number of questions could warrant separate, independent study in the future, as most discussion groups begin to lose energy and focus after an hour and a half.

We subsequently transcribed and analyzed the transcripts based on their responses to our questions. We developed a 'code frame' forming the basis of the classificatory interpretive schema that comprises our suggested privacy repertoire. While hardly definitive, the privacy repertoire is one of the outcomes that may act as a useful initial benchmark to understand how specific these responses are and to conduct more precise statistical analysis on these responses in future research with other segments of the public.

The Privacy Repertoire: Contextualizing Privacy

To comprehend this privacy repertoire, we want to acknowledge the importance of our own understanding of the concept of privacy. We are influenced by Canadian criminologist,

Valerie Steeves, who has written extensively on privacy-related matters in digital contexts.[96] Steeves articulates four principles of privacy, which she attempts to define in more social and cultural terms, rather than just individualistically: it is an essential part of the democratic process; it is a social value; it is about data protection; and it is a human right.[97] Yet while our analysis, and academic understanding of privacy was drawn from these sources, it must be noted that the language of privacy used by our participants was expressed in personal terms as the right to solitude, anonymity, confidentiality and the need for trust between people.

To make sense of this disjuncture between the more normative, academic critiques of privacy and the responses of our participants, we turn to the insights of Helen Nissenbaum, who defines privacy within the parameters of "contextual integrity."[98]

Her central claim is that:

> …contextual integrity captures the meaning of privacy in relation to personal information; predicts people's reactions to new technologies because it captures what we care about when we question, protest, and resist them; and finally, offers a way to carefully evaluate these disruptive technologies….social activity occurs in contexts and is governed by context-relative norms.[99]

---

[96] Valerie Steeves, "It's not child's play: The online invasion of children's privacy." *University of Ottawa Law and Technology Journal* 3:1 (2006): 169-188.

Valerie Steeves, "Privacy and new media." *Mediascapes: New Patterns in Canadian Communication*. 2nd ed. Leslie Regan Shade and Paul Attallah, eds., (Toronto: Nelson, 2006a): 250-265.

Valeries Steeves, "Data protection and the promotion of health research." *Healthcare Policy Journal* 2:3 (2007): 26-38.

[97] Steeves 2006; Leslie Shade, "Reconsidering the right to privacy in Canada." *Bulletin of Science, Technology & Society* 28:20 (2008): 80-91.

[98] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. (Stanford, CA: Stanford University Press, 2010).

[99] Nissenbaum 14.

Nissenbaum's attention to contextual integrity is very useful for making sense of the responses given by our seniors to the questions we asked about privacy. Given these principles and commitment to a contextual integrity, we must be mindful that the majority of the participants in this study did not own either their own personal computers or their own mobile telephones.

Indeed, there is a broader environment of digital ownership and access at work here. Our questions on privacy followed our own discussion on cellular telephone use. In our larger research project, all of our seniors have expressed concerns and reservations about the high costs of telephones as well as the complicated bundling packages.[100] (Sawchuk and Crow, 2010). This is further compounded by seniors' observations about the design of mobile telephones - their size and screen. As a result of the high costs, confusing bundling packages and poor design, these factors result in either non-use or force a limited use on the part of many of the seniors.

While our larger study has included a variety of seniors in a range of socio-economic positions, the majority of the participants in this pilot study lived near or below the poverty line, and many relied on different forms of social assistance to survive. The cost of the technology is not the only issue: access to the digital network, whether a phone or a computer, means that using these technologies are a luxury for them. For those who did own mobile telephones, the majority received them as hand-me-downs from family. Those with hand-me-down phones spoke almost exclusively in terms of how they were to be used for 'safety' and 'emergency' uses only:

[100] Kim Sawchuk and Barbara Crow, "Talking 'Costs': Seniors, Cell Phones and the Personal and Political Economies of Telecommunications in Canada." *Telecommunications Journal of Australia* 60:4 (2010): 55.1-55.11.

> Oh, my son was concerned that I did not have a cell phone. He's concerned about my safety and he thinks I live in an area that isn't quite so good or something … So when he got his new own, he said well, at least take this one and then if you have, if somebody does attack you, you can phone the police. (p19) [101]

While many of them had either no or little use of mobile telephones, they were generous with their observations and very much wanted to participate in deliberations about how all communications technologies, from the land-line to the mobile, are connected to computerized systems, and data-gathering imperatives that are changing their everyday experience of privacy. Like many other seniors groups we have interviewed, there is a sense that whether or not they own a device they are implicated in a larger assemblage of systemic social and technological change that is relevant to them, if only because entry into public space means they find themselves listening to private conversations.

Despite their distance from these technologies and tools, or perhaps because of it, they did have much to say about technology and the erosion of privacy based on their understanding of technology not just as a machine, but as an entire range of information-gathering systems. In this respect, all of our respondents had a contact and connection to the world of information and communication technologies (ICTs) and privacy, but not in the ways we anticipated. Many understood privacy in personal terms, but often this initial discussion of their personal sense of privacy could lead to set of questions about the social dimensions of the term that Steeves considers critical for us to reflect upon.

[101] We have chosen to identify the senior participants through a random assortment of numbers. Hence, (p19) refers to participant nineteen.

1) *Privacy as a Form of Solitude: The Right to Solitude in the Context of Socio-Economic Status*

Many of the seniors discussed the high costs of the mobile telephones, the complicated pricing, and their continued reliance on their landline telephone. For this reason, the most repeated refrain - aside from the high costs of mobile communications - in response to the question of how their privacy was violated, turned to the telephone solicitations they received from telecommunication companies. It is within this milieu that the seniors discussed privacy as a violation of their 'solitude': unwanted telephone solicitations are understood as invasions of their right to be left alone and to not be interrupted by anonymous others seeking attention.

This articulation of privacy also spilled over into a query connected to a concern with digital technologies. Many seniors wanted to know how companies got their numbers - "How did they get my number?" A number of seniors did not understand how these companies could make these solicitations even when they had an unlisted number. Their concerns were expressed in the following manner:

> I keep wondering how these people are getting your name and your address" (p 4)
>
> "…now, your number's supposed to be unlisted. How the hell do they get hold of your number? (p17)

They wondered what they could do to stop such unsolicited calls and expressed their discomfort with feeling pressured to buy things they did not want:

> I like my privacy and sometimes, I get a call and the call says we're doing research or we're doing this or we're doing that. First, they ask Mrs. XXXX. And then after they give their spiel, I say where did you get my name and phone number? Well, um and they can't answer. (p19)

When we asked if they knew about privacy legislation to address these matters, none of the participants indicated that they were aware of such legislation: "…because there are lots of people who don't know what their privacy right[s] [are], and I don't know much about mine either" (p3). Instead their strategies for resisting or addressing this invasion consisted of "try[ing] to ignore it and hope it will go away" (p10) or "I just hang up" (p17).

While seniors represented incoming calls as disruption of their solitude, and a question of "rights", they also represented this solitude in terms of their engagement with public services. As many of them lived in public housing, they had much to say about how the meshing of different government services were making it difficult for them to keep information about themselves confidential.

> And in government, in Community Housing, you have so few rights. The landlord has all the rights and they do trample your privacy… I think new technologies are a danger to privacy and I think we should have more information about our privacy rights and what um, is being collected. (p23)

It is important to acknowledge that the confluence of personal information and confidentiality takes on particular relevance for this group when their housing is so contingent upon regularly updated information about their personal finances and their health care.

In an elaboration of this disruption to their solitude, they were also concerned about what they are being asked to do:

> Like, like all the time, they phone you for a survey. And then they say you qualify for a survey and you can go to this place, this place….You know, don't bother phoning me, because I've told them before, they disturb me, don't, these people, don't phone me…(p17)

> Well, the Bell Telephone phones me all the time. I have Rogers. I say why should I change it? Now, everything is set up. (p14)

It was their position if they wanted to change such matters pertaining to a product or service, they would seek out such information themselves. Implicit in many of the seniors' repertoires about these unsolicited phone calls were concerns about why they were they being asked to change their services. Most critically, they wondered why they were getting these phone calls if they had taken measures to protect themselves against them either through registering with the national no-call list or by paying for a private, unlisted number.

This discussion of unwanted telephone calls, and ways they had protected themselves to not receive them, raised other matters pertaining to privacy:

> Most of the time when people call you, it's recorded and I don't think that's right because you want your privacy and if it's anything medical or personal about your

> income or whatever, it should be done face to face with the person in private, not on the telephone to be recorded. (p21)

Telephone solicitations were understood as companies and government entering into their private space and having the possibility to gather information and data whose future use was uncertain. While they viewed these disruptions as violating their private space, these personal narratives were often the foundation for a further discussion on larger societal issues discussed in the literature, such as "data-veillance". It was also discussed in terms of "intimacy" and social norms regarding sexuality and explicitness.

> I think they should be more careful of things that they put on the computer because sometimes it's not everybody want to see it or like to see it or enjoy it. Like, they have R rated movies on televisions but they put it on late at night when kids can't get to watch them and stuff. Even that, I don't like because I don't watch them. (p3)

Here privacy was equated with the sphere of personal intimacy which often leads to a discussion of generational shifts in values and norms connected to sexuality.

In summary, in response to the question of "do we have more or less privacy" and if they had an experience of a privacy violation, the first response was through personal example, making privacy a personal affair, and not a public issue: privacy was first represented as a disruption to their right to solitude, anonymity, the control of their personal information, and in terms of confidentiality. The participants had a desire to maintain some personal information as confidential: "…I'd say that if you have something private and I speak it with someone I want it to remain between myself and you" (p3) and "…if you have, say anything very, very private,

that's going to go with me because I'm not going to tell you about it … That's my privacy."(p2) However, through the process of group discussion, a collective conversation about personal privacy often lead the participants into the territory of privacy as a public, social, or cultural issue connected to shifts in technology and the ability of those in power to engage in data-gathering.

2) Erosion of Privacy: Technology at Fault

The invasion of their privacy in their home via phone solicitation was often represented as a disruption to their solitude, but they also related it to what they expressed as a general erosion of privacy. When we probed what was causing this erosion, one of the first causal facts that they identified was technology. Technology was often equated with computers and their widespread presence was often blamed for the erosion of privacy. They saw individuals as being responsible for what they put into a computer and yet there was a general understanding that we are all now in a system where our identities are registered in some way, with those who have access and control over computerized systems:

> …because they punch you up in that computer and they start to search, do the search and find out everything about you, well, there is not, I'm not a criminal, never be, and I don't think I will be at this age, but there are things that I would like to keep private in my life. (p3)

While computers were sometimes seen as the technology most specifically to blame for the erosion of privacy, in other points of the discussion, the internet and its reach was figured as the problem as was the transformation of information about identity into the language of numbers:[102]

> I would say privacy means that you can, just don't want anybody to know, and how are they getting into your personal files and things like that … You don't know where, didn't give this person your number but they've got your number. (p5)

When we pressed them about computer's reach and asked specifically about social networking technologies they often mentioned *Facebook.* Their concerns about *Facebook* pertained to where the information was going and in some ways reflected the relation of an understanding of privacy to intimacy: "*Facebook* doesn't allow you to distinguish between close friends and your acquaintances" (p9). As another participant mentioned,

> So if I hear something on *Facebook*, like this individual come and tell me about this person, I hear from you, I hear from you, everybody, but I'm not. I said you know something? My *Facebook* is I see you and I have something to tell you; I'll tell you and poke you in your eye. (p5)

In their discussion of both privacy and the media, many of our participants expressed a concern about the use of social media by youth. They expressly felt that 'young' people were revealing too much and that they were getting "too much, too fast" (p15), a repertoire connected to their understandings of privacy as intimacy.

[102] A couple of participants mentioned Google, although there was some ambivalence: they like access to the information they get from search engines, but they were not sure where all the information was going.

Much of their information on social networking was not based on their own experiences with the technology, but with their observations of grandchildren, or from the media. Their observations about the erosion of privacy on the internet came from stories they read in the newspapers, what they had watched on television, or stories told by friends, but not necessarily from any personal violation of privacy they experienced on the internet.

3) Privacy and Digital Disclosure: Chips, Stripes and Cards

A concern about disclosure was manifest in how the seniors talked about 'cards' and 'black strips.' These cards, particularly the black stripe on the health card and driver's license, functioned as a way to monitor them and prevented them from 'exchanging' government services. Many of them pulled out their cards in the interview and pointed to them. In other words, these 'black stripes' were providing a way for institutions to converge information about them – financial, tax and health information: "The government can get a printout of you from the time you were born 'til the time you die and have all kinds of stuff on there that you don't even…"(p13).

This concern about the convergence of information was translated into a distrust or wariness of government. They did not view this convergence as a way to offer them better services and/or care. Their encounters with the convergence of information have been about taking things away from them rather than enhancing the provision of services. Moreover, their way to intervene in this convergence of information has been about how to control what

information they provide and who has it. As a result of their public housing arrangements mentioned earlier, they found it particularly difficult to control what the government knew about their finances and health. Others discussed how this might impact them if they were searching for jobs, and what data might be available for scrutiny. A number of them were concerned about how this convergence may affect their access to subsidized public funds on which they have come to rely. Hence, the seniors experienced the convergence of information and its availability to different public sector contexts as both a disruption of their solitude and an erosion of their privacy.

They also expressed concerns about how new technologies like the internet were making information more widely available and how individuals no longer had privacy in these contexts which raised another repertoire issue of the intertwining of privacy and confidentiality. They voiced their concerns with their regular encounters with government services such as housing and health care in terms of having to provide what they thought was private and confidential information: "Privacy to [me] means confidential" (p3). They wanted to have control over disclosing information and what would happen to it.

When asked about what they knew about privacy rights, in general, many liked the idea of privacy rights, but they did not know what this might entail. They said things like "we don't know our rights" (p2). When we asked where they learn about privacy, it was generally constructed in terms of the places that they have access to information. They get their information about privacy from the television news, from celebrity culture, from direct experience, from watching others or from hearing other people's stories. Legal remedies were not even offered or even favoured in terms of addressing their concerns about privacy and many understood privacy as a personal matter. These were viewed and understood as extensions of the

convergence of information about them collected by other institutions. They commented that legislation worked only for those with money, that it would increase costs, that it would give the government more power and that in the digital context, it would be difficult to enforce.

When pressed further about privacy legislation and protection, they often commented that some individuals get 'special treatment' pertaining to privacy matters. Privacy was not a legal or protected right for them; it was understood to be a privilege for the rich. Special treatment was accorded to those with money:

> Yeah, you can buy your way through. (p2)
>
> That's right. (p3)
>
> You get the best treatment. (p1)

Hence, legislative or policy remedies were not viewed as a mechanism or avenue to resolve their concerns about disruption to their solitude. They understood such remedies as only working for those who had money.

Policy Insights

A lot more work needs to be done in order to understand the needs of seniors with respect to contemporary communications and privacy. Clearly, the participants in our study, living near or below the poverty line with a deep commitment to and a significant sustenance derived from their communities, have a range of understandings of privacy, which we have defined as a

privacy repertoire. There is a general sense that there is an erosion of personal privacy, which they experience in relationship to their dependency on government-subsidized services.

As such, their understanding of privacy is linked to a right to solitude and anonymity from the prying eyes of agencies who have the right to examine their financial records, who record their incomes and health data, and to corporations who solicit them for information or interrupt their solitude to peddle unwanted (or unaffordable) services. As many of the research participants live in public housing, they were most concerned about how information from various sources would be used against them - a kind of perpetual surveillance from converging information sources. They are concerned about who has access to information about them, and how it will be used.

In general terms, there was a sense amongst these seniors that privacy issues are related to new technologies, like the 'computer' and the 'internet' but most importantly through access to information in devices not typically thought of as technologies, but which contain information and allow for its easy circulation: the magnetic strip card with an embedded chip. This is their understanding of digital technology. Many of them did not own mobile telephones and also had limited access to other forms of digital technologies like the internet. When they did access the internet it was either through the community centres they frequented or when they visited family members with the technology.

This access is a matter of major concern as more and more public services are accessible on-line and as the numbers of seniors increase in the province. In developing information for this population on privacy, there must be some understanding of what kind of technologies

seniors own, how they use them, and where they use them. Policy makers should take into consideration the continued reliance of seniors on landline telecommunications.

Our research indicates that seniors living near or below the poverty line have less access to digital technologies. Hence, strategies to empower this group must take into consideration where they do learn and get their information from such as the radio, newspapers and television and to provide them with public and affordable access to digital technologies such as the internet. While it is outside the scope of the issue of privacy, there must be ways to provide seniors with clear information on the costs and services affiliated with mobile telephones. It is important to remember that these citizens have spent most of their lifetimes negotiating 'new' media: from listening to the first radio broadcasts, to watching black and white and then colour television, to adopting and using inexpensive long distance calls to family around the world. We should not second-guess their experiences and observations of the 'latest' technologies. The best way to do this is to make them active subjects and agents in the process of how they consider and negotiate privacy within their own contexts.

Finally, it is worth considering how they understand the law and government. The law is not seen as having the ability to work for them and government agencies are looked upon with some suspicion. If this is the case amongst other marginalized groups, it will make privacy advocacy work from within these sectors a challenge. It is not enough that the information be available to them: trust in the law and institutions are at issue before information is disseminated.

REFERENCES CITED

Aquisti, Alessandro and Ralph Gross, "Imagined Communities: Awareness, information sharing, and privacy on the Facebook." *Proceedings of 6th Workshop on Privacy Enhancing Technologies*. Cambridge, UK: Robinson College, 2006.

Boyd, Diana and N. B. Ellison. "Social network sites: Definition, history, and scholarship." *Journal of Computer-Mediated Communication* 13:1 (2007): 219.

Canadian Bankers Association, "How Canadians Bank", available online: http://www.cba.ca/en/media-room/50-backgrounders-on-banking-issues/125-technology-and-banking (last accessed: 26 March 2011)

Canadian Broadcasting Corporation, Marketplace, 2010. "Canada's worst cell phone bill." 24 Aug. 2010. <http://www.cbc.ca/marketplace/2010/canadas_worst_cellphone_bill/main.html>.

Canadian Institute of Health Research. *The future is aging: The CIHR Institute of aging strategic plan 2007-2012.* Vancouver: Institute of Aging, 2006. 16 Aug. 2010. <http://www.criugm.qc.ca/fichier/pdf/plan_strategique_IRSC_anglais.pdf>.

Canadian Wireless Telecommunications Association. *2008 Wireless Attitudes Study*. Ottawa: Harris-Decima, 2008.

Cavoukian, Ann. "Reference Check: Is your Boss Watching? Privacy and You Facebook Profile. 24 Oct. 2007; Revised June 2010: 2.

<http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=672>.

Denham, Elizabeth. "Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic(CIPPIC) against Facebook Inc. Under the personal Information Protection and Electronic Documents Act." Ottawa: Privacy Commissioner of Canada, 2009.

Delacourt, Susan. "Facebook gets poked by Canada over Privacy." *The Star* 17 Jul. 2009. <http://www.thestar.com/News/Canada/article/667700>.

Dishman, Eric. "Inventing wellness systems for aging in place." *IEEE Computer Society* 37:5 (2004): 34-41.

http://ebaystrategies.blogs.com/ebay_strategies/2009/12/fun-ebay-math-what-does-14-million-cyber-monday-transactions-mean.html (last accessed: 28 March 2011)

www.euronetworldwide.com/our_company/businesses.cfm (last accessed: 26 March 2011)

Engel, David and Frank Munger. "Rights, Remembrance, and Reconciliation of Difference." *Law & Society Review* 30:7 (1996): 7-54.

Ewick, Patricia and Susan Silbey. "Conformity, Contestation, and Resistance: An Account of Legal Consciousness" *New England Law Review* 26 (1992): 731-742.

Ewick, Patricia and Susan Silbey. The *Common Place of Law*. Chicago: The University of Chicago Press, 1998.

"Facebook '09 revenue neared $800million. *The Economic Times.* June *18,* 2010. Reuters. <http://economictimes.indiatimes.com/infotech/internet/Facebook-09-revenue-neared-800-mn-Sources/articleshow/6063819.cms>.

Facebook website. *Statistics.* <http://www.facebook.com/press/info.php?statistics>.

Farmer, Paul. *Pathologies of Power: Health, Human Rights, and the New War on the Poor* Berkeley CA: University of California Press, 2005.

Financial Transaction and Reports Analysis Centre of Canada, "Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MCBs)" (July 2010), p. 3, available online at http://www.fintrac-canafe.gc.ca/publications/typologies/2010-07-eng.pdf

Geist, Michael. 2008. "iPhone shines spotlight on our wireless flaws."*Toronto Star* (May 5). 23 Aug. 2010. <http://www.thestar.com/sciencetech/article/421352>.

Government of Canada, Canadian e-Policy Resource Centre, online: http://www.ic.gc.ca/eic/site/ceprc-ccrcp.nsf/eng/00025.html

Griswold v. Connecticut, [1965] 381 U.S. 479

Hartley, Matt. "Privacy watchdog mulls fresh Facebook probe." *The National Post.* 18 Oct. 2010. <http://www.nationalpost.com/related/topics/Privacy+watchdog+mulls+fresh+Facebook+probe/3689323/story.html>.

Hermes, Joke. *Reading Women's Magazines: An Analysis of Everyday Media Use*. Cambridge, Massachusetts: Polity Press, 1995.

"How Teens Use Media: A Nielsen report on the myths and realities of teen media trends." < http://blog. nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf>.

International Telecommunications Union. "The world in 2010: ICT facts and figures."23 Feb. 2011. <http://www.itu.int/ITU-D/ict/statistics/>.

"Investors bet on price of Facebook IPO." *The Wall Street Journal.* 4 Mar. 2010. 26 Mar. 2011. <http://blogs.wsj.com/digits/2010/03/04/investors-bet-on-price-of-facebook-ipo/>.

Irving, Jacqueline, Sanket Mohapatra & Dilip Ratha, *Migrant remittance Flows: Findings from a Global Survey of Central Banks*, (Washington, D.C.: Office of the Publisher, The World Bank, 2010).

Jacobs, Lesley. "Differentiated Corporate Legal Consciousness in International Human Rights Disputes: Security and Transnational Oil Companies in Sudan." *APDR Research Notes* 1:3 (Oct 2008): 37-49. <http://apdr.iar.ubc.ca/publications/ejournal/APDR_1.3/APDR_1.3_LJ.pdf >.

Jacobs, Lesley. "Legal Consciousness and the Promise of Law and Society." *The Canadian Journal of Law and Society* 18:1 (2003): 61-66.

Jacobs, Lesley. "Mapping the Legal Consciousness of First Nations Voters: Understanding Voting Rights Mobilization." Ottawa: Elections Canada, May 2009. <http://www.elections.ca/med/eve/APRC/vot_rights_e.pdf>.

Jacobs, Lesley and Kaitlyn Matulewicz. "Protecting Privacy Rights in the Emerging Digital Economy: Canada's Regulatory Scheme, Its Adaptability, and Its Future" *Joint Industry*

Canada/ SSHRC Presidential Initiative on Research on Canada's Emerging Digital Economy, November 2010.

Jacobs, Lesley. *Pursuing Equal Opportunities.* New York: Cambridge University Press, 2004.

Office of the Privacy Commissioner of Canada. *Mandate and Mission*. 27 Nov. 2010. <http://www.priv.gc.ca/aboutUs/mm_e.cfm#contenttop>.

Jacobs, Lesley. "Rights and Quarantine During the SARS Global Health Crisis: Differentiated Legal Consciousness in Hong Kong, Shanghai, and Toronto." *Law & Society Review* 4:1/3 (Sept. 2007): 511-553.

Jacobs, Lesley. 'Securer Freedom For Whom? Risk Profiling and the New Anti-Terrorism Act', *UBC Law Review* 36:2 (2003): 375-384.

Jacobs, Lesley. *Securing Better Access to Justice: Country Report Canada.* New York: Vance Center for International Justice, March 2011. <http://www.abcny.org/citybarjusticecenter/vancecenter-overview/>.

Kerr, Ian, Valerie Steeves and Carole Lucock, eds. *Lessons from the Identity Trail: Privacy and Identity in a Networked Society*. New York: Oxford University Press, 2009.

Krewen, Nick. "Social media more than just a fad: studies." *Media in Canada.* 16 Dec. 2009. <http://www.mediaincanada.com/articles/mic/20091216/socialmediastudies.html>.

Larson, Erik. "Institutionalizing Legal Consciousness: Regulation and the Embedding of Market Participants in the Securities Industry in Ghana and Fiji." *Law & Society Review* 38 (2004):711-736.

Law Commission of Ontario, "Fees for Cashing Government Cheques Final Paper"(November 2008), which is available at http://www.lco-cdo.org/en/cheque-cashing-fees-final-paper (last accessed: 27 March 2011).

Lee, Y. S. "Older adults' user experiences with mobile phones: User cluster identification." *Proceedings of the 21st International Symposium: Human Factors in Telecommunications, User Experiences of ICTs*. Kuala Lumpur, Malaysia, 2008.

Ling, R. "Should we be concerned that the elderly don't text?" *The Information Society* 24 (2008): 334-341.

Madden, Mary. "Older Adults and Social Media." *Pew Internet & American Life Project* <http://pewinternet.org/Reports/2010/Generations-2010/Trends/Social-network-sites.aspx>.

Murdoch v. Murdoch [1975] 1 S.C.R. 423.

Merry, Sally Engle. *Getting Justice and Getting Even: Legal Consciousness Among Working-Class Americans*. Chicago: University of Chicago Press, 1990.

"People from Cossette." 8 Dec. 2009. Press Release. <http://www.cossette.com/data/impact-social-press-release.pdf>.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press, 2010.

Office of the Privacy Commissioner of Canada. *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act.*

Ottawa: Office of the Privacy Commissioner of Canada, 2008. <http://www.priv.gc.ca/information/pub/lbe_080523_e.pdf>.

Office of the Privacy Commissioner of Canada. "Privacy Commissioner completes Facebook review." News Release. <http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.cfm>.

Office of the Privacy Commissioner of Canada. "Privacy and Social Networks, What does a friend of a friend need to know about you?"< http://blog.privcom.gc.ca/index.php/privacy-on-social-networks/; and http://www.youtube.com/Privacycomm>.

Office of the Privacy Commissioner of Canada. *Organizational Structure.* 27 Nov. *2010.<http://www.priv.gc.ca/aboutUs/au_org_e.cfm#contenttop>*.

Office of the Privacy Commissioner of Canada. *My Privacy. My Choice My Life.* <http://www.youthprivacy.ca/en/>.

Office of the Privacy Commissioner of Canada. "Raising awareness about youth privacy." *Privacy Perspectives: News from the Office of the Privacy Commissioner of Canada*. Issue 8 <http://www.priv.gc.ca/newsletter-bulletin/2011-8/index_e.cfm>.

Oliveira, Michael. Facebook not just for friends anymore as businesses makes it marketing network," *The Canadian Press*. 23 Mar. 2001. Canadian Business Online. <http://www.canadianbusiness.com/ markets/ headline_news/article.jsp?content=b6340152>.

Ortutay, Barbara. "Facebook to end Beacon tracking tool in settlement." *USA Today* 24 Oct. 2007; Revised June 2010. *Associated Press.* 21 Sep. 2009. < http://www.usatoday.com/tech/hotsites/2009-09-21-facebook-beacon_N.htm>.

Potter, Jonathan, and Margaret Wetherell. *Discourse and Social Psychology: Beyond Attitudes and Behaviour*. London: Sage, 1987.

PIPEDA Case Summary # 2009-008. CIPPIC v. Facebook Inc. <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>.

Protection of Personal Information and Electronic Documents Act, 2000, c. 5 *(PIPEDA).*

R. v. Dyment, [*1988*] 2 S.C.R. 417

Roe v. Wade, [1973], 410 U.S. 113

Sawchuk, Kim, and Barbara Crow. "Talking 'Costs': Seniors, Cell Phones and the Personal and Political Economies of Telecommunications in Canada." *Telecommunications Journal of Australia* 60:4 (2010): 55.1-55.11.

Shade, Leslie. "Reconsidering the right to privacy in Canada." *Bulletin of Science, Technology & Society* 28:20 (2008): 80-91.

Statistics Canada. *A portrait of seniors in Canada*. Ottawa: Government of Canada, 2007. 23 August 2010. <http://www.statcan.gc.ca/ads-annonces/89-519-x/index-eng.htm>.

Statistics Canada. "Deaths, 2007." *The Daily* (February 23, 2007): 2–3.

Steeves, Valerie. "Data protection and the promotion of health research." *Healthcare Policy Journal* 2:3 (2007): 26-38.

Steeves, Valerie. 2006. “It’s not child’s play: The online invasion of children’s privacy.” *University of Ottawa Law and Technology Journal* 3:1 (2006): 169-188.

Steeves, Valerie. “Privacy and new media.” *Mediascapes: New Patterns in Canadian Communication*. 2nd edition. Eds. eslie Regan Shade and Paul Attallah. Toronto: Nelson, 2006a.

The Early Show. *Facebook Faux Pas Leads to Teacher Losing Job*. 20 Aug. 2010. <http://www.cbsnews.com/stories/2010/08/20/earlyshow/main6789897.shtml>.

Trubek, David M. “Where the Action Is: Critical Legal Studies and Empiricism” *Stanford Law Review* 34:1/2 (January 1984): 575.

Uppal, Sharanjit. "Labour market activity among seniors.” *Statistics Canada: Perspectives on Labour and Incomes* 7 (2010): 5–18.

Zickuhr, Kathryn. “Major Trends in Online Activities.” *Pew Internet & American Life Project* < http://pewinternet.org/Reports/2010/Generations-2010/Trends/Social-network-sites.aspx>.