Situating Privacy Online:
Complex Perceptions and Everyday Practices

Ana Viseu
Human Development and Applied Psychology
University of Toronto / OISE
252 Bloor St. West, 9th Floor, Toronto, ON; M5S 1V6 Canada
http://fcis.oise.utoronto.ca/~aviseu
ana.viseu@utoronto.ca

Andrew Clement, Jane Aspinall
Information Policy Research Program
Faculty of Information Studies, University of Toronto
140 St. George St., Toronto, ON; M5S 3G6 Canada
clement@fis.utoronto.ca, aspinal@fis.utoronto.ca

http://www.fis.utoronto.ca/research/iprp/

Forthcoming in *Information Communication and Society (iCS)*

2003

Abstract

Media and research reports point to the issue of privacy as the key to understanding online behaviour and experience. Yet it is well recognized within privacy-advocacy circles that "privacy" is a loose concept encompassing a variety of meanings. In this article we view privacy as mediating between individuals and their online activities, not standing above them, and as being constantly redefined in actual practice. It is necessary to examine, therefore, what individuals are reacting to when asked about online privacy and how it affects their online experience.

This article is based on data generated in the Everyday Internet study, a neighborhood-based, ethnographic project being conducted in Toronto, Canada, that investigates how people integrate online services in their daily lives. We propose that there are three organizing "moments" of online privacy: the moment of sitting in front of the computer, the moment of interaction with it, and the moment after the data has been released in "cyberspace." We argue that, while the third moment has been given much media coverage, the first two have not been sufficiently researched. This may be crippling the formulation of effective privacy principles and practices by policy makers and the public.

INTRODUCTION

Privacy is a buzzword in the media these days. Accounts of the loss or invasion of privacy, threats to and worries about privacy, and even the death of privacy appear daily. Likewise, there are reports of privacy-enhancing technologies and calls for legislation to defend privacy. At the same time, however, privacy is a slippery concept. It has been categorized as a countervailing force to the development of the Information Society and e-commerce, denounced as an outdated and defunct concept, and called the civil-rights issue of the twenty-first century.

The one constant in the privacy debate are public-opinion surveys indicating that the overwhelming majority of people are "very concerned" about their privacy. Yet empirical evidence suggests that there is a significant discrepancy between privacy principles and privacy practices. Furthermore, given the many definitions and interpretations of privacy, it is important to investigate what meanings of privacy are involved in the practice of being online.

This study[1] explores the perceptions and practices of online privacy. It draws

[1] Previously presented at the Association for Internet Researchers (AoIR) conference in October 2002.

upon qualitative, empirical data generated in the Everyday Internet study, conducted in Toronto, Canada, the goal of which is to investigate how regular internet users experience online services in the context of their daily lives.

BACKGROUND

Privacy is a far-reaching concept that encompasses, and can be applied to, a variety of core rights and values such as freedom of thought, freedom of expression, freedom from surveillance, personhood, human dignity, identity and anonymity, secrecy, and so on.[2] So hard is it to define that Alan Westin, a noted privacy scholar, observes that "no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests and power" (Westin 1995; quoted in Gellman 1998: 194). Others have argued differently, saying that defining privacy is unnecessary since the concept itself serves no function, merely standing in for other primary interests (Thompson 1984; quoted in Solove 2002).

Within the policy discourse, however, privacy has been consistently discussed in terms of "fair-information practices" based on the principle of "informational self-determination." The concept of fair-information practices, which constitutes an attempt to regulate the collection, usage, security, and dissemination of personal data[3] (Gellman 1998; Cavoukian & Tapscott 1995), originated almost simultaneously in the United States and United Kingdom in the early 1970s (Flaherty 1999). Thereafter, the need for transnational data-protection policies was quickly identified (Bennett 1998), and in 1980 the Organization for Economic Cooperation and Development (OECD) issued its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the first attempt to "harmonize national privacy legislation without interrupting the free flow of information between borders" (CDT n.d.). Since then, a number of countries have passed data-protection legislation in an effort to regulate the collection of personal information, notably the European Union's Data Protection Directive,[4] introduced in 1995, and Canada's Personal Information Protection and Electronic Documents Act

---

[2] There is a large literature offering diverse perspectives on privacy. For a legal treatment, see Gellman (1998) or Solove (2002); for a philosophical inquiry, see Schoeman (1984); for a policy-grounded analysis, see Bennett (1992); for a sociological perspective, see Lyon (2001a); and, finally, for a historical view, see (Flaherty 1999).

[3] For more on the subject of fair-information practices see, for instance, the Center for Democracy and Technology <http://www.cdt.org/privacy/guide/basic/fips.html>, Junkbusters <http://www.junkbusters.com/fip.html> or OECD's report <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

[4] Directive on the Protection of Personal Data and on the Free Movement of Such Data (Directive 95/46/EC).

(PIPEDA), passed in 2000 (Privacy Commissioner Canada n.d.). Finally, the term "informational self-determination" was used in 1983 by the German Federal Constitutional Court to assert privacy protection as a fundamental human right. The expression points to the right of every individual — not the government — to determine and control what happens to his/her personal information (Cavoukian & Tapscott 1995) and to know who knows what about him/her at what time (Virtual Privacy Office, n.d.).

Nonetheless, it is commonly acknowledged that the privacy landscape is riddled with ambiguities. For instance, surveys routinely show that an overwhelming number of people are "very concerned" about their privacy: the 2001 Internet Report of the University of California at Los Angeles (UCLA) puts this figure at 95 per cent, while AOL/Roper Starch's 2000 Worldwide Adult Cyberstudy gives a figure of 94 per cent.[5] Yet these surveys are accompanied by what could be called counter-surveys, that is, factual demonstrations of a disconnect between privacy perceptions and practices. Daniel Solove (2001) presents the example of the survey conducted, in 1998, by Conde Nast Publications. Conde Nast "sent out a booklet of 700 questions concerning detailed information about an individual's hobbies, health (including drugs used, acne problems, vaginal/yeast infections, etc.), shopping preferences, etc. … In return for the data, the survey said: 'Just answer the questions below to start the conversation and become part of this select group of subscribers to whom marketers listen first.'" Almost 400,000 people responded. Another example of the privacy-gap is described by Lyon (1994). He writes: "In the mid-1980's passers-by on a New York street were asked one day their opinion concerning the 'invasion of privacy' by 'modern technology.' Ninety percent expressed concern. But the next day, when offered a credit card with a favorable interest rate, ninety percent of passers-by on the same street filled, in their entirety, application forms requiring Social Security number, bank account numbers and information about other credit cards" (Lyon 1994: 140).

Given the varied interpretations of privacy, it is important to investigate what individuals are reacting to when asked about privacy online, as well as how they act upon their perceptions and how these perceptions affect their online practices. The need for a contextualized approach to privacy is well documented in the literature. In 1996 Alan Westin found that 50 per cent of consumers were pragmatists in their approach to privacy (FTC 1996). Other researchers, such as Sheenan (2002), Hine & Eve (1998), Schoeman (1984), and Regan (1995), have also argued in favour of such an approach. In this article we base our analysis on the framework set out by Daniel Solove (2002). Solove criticizes contemporary privacy theories and proposes new methods for analysing the issue. He argues that, rather than trying to find a one-size-fits-all definition of privacy, we must search for a pragmatic approach that allows us to emphasize and explore the situated and dynamic nature of privacy. Privacy must be viewed within the

[5] For the latest privacy` surveys, see <http://www.privacyexchange.org/iss/surveys/surveys.html>.

practices that constitute it and give it meaning, and studying threats to privacy means studying the types of disruptions to these particular practices (Solove 2002). Privacy, then, should be viewed as a concept that stands, not above individuals and their activities, but between them, and as one that is constantly being (re)defined in actual practice.[6]

RESEARCH DESIGN

The Everyday Internet project,[7] an ongoing research study initiated in the summer of 2001, is informed by a variety of contemporary information-policy issues, of which privacy is an example. By not focusing specifically on privacy, we attempt to diminish the risks of biasing our sample towards individuals who are not concerned about privacy, and are thus following a strategy that has been previously adopted by researchers such as Hine and Eve (1998). This approach also fits our objective of discussing privacy from a grounded perspective, that is, seeing if, and how, privacy concerns shape online experience and vice versa. In addition, because we aim to obtain a better understanding of the integration of networked services in everyday life, we take a "holistic" approach towards our participants. Privacy studies frequently sectoralize individuals as consumers (e.g., Earp & Baumer 2003; Phelps, Nowak & Ferrel 2000; Miyazaki & Fernandez 2001), but in this study we treat them as multifaceted, active citizens.

In our recruiting strategy, we attempt to include participants from those socio-demographic categories that are repeatedly identified as lagging behind in internet access: low income, low education, English as a second language, and seniors. We define the regular internet user as someone who logs on to the internet on average at least once per week. Taking advantage of Toronto's cultural and ethnic diversity, we utilize a "geography-based" recruiting strategy similar to that used by Miller and Slater (2000). Through census data and internet-access data, we have settled on a downtown multicultural neighborhood as the focus of our investigation.

In order to be consistent with the situational dimensions of our ethnographic study, we have recruited and interviewed participants at their regular access site, whether that is at home or at a public facility. Relying on in-depth, semi-structured interviewing and participation-observation methods to collect data, we have invited participants to give us a demonstration of their online activities and show us their familiar websites, while also structuring our interviews as informal conversations based on the interviewee's online practices. (See Clement et al. [2002] for a more detailed description of the

---

[6] As Solove (2002) notes, some privacy expectations can also be instigated by the law. For instance, letters became private means of communication only when, in 1877, the U.S. Supreme Court held that letters were protected by the Fourth Amendment. Until that time, letters were seen as insecure and there was no expectation of privacy in personal correspondence.

[7] <http://www.fis.utoronto.ca/everydayinternet/>.

Everyday Internet project.[8]) Most participants have been interviewed twice, with an interval of two to four months between interviews.[9]

Participants have been recruited through two methods. To find home internet users, we used a door-to-door strategy. If nobody was home, we left a brochure with information about the project and a questionnaire which the person could send to us if he/she was interested in becoming involved.

Since we wanted to talk to both home internet users and individuals reliant on public facilities for their access, we approached St Christopher House, a community centre located in our study area, to help us with the recruitment process. We spoke to the person in charge of their internet services and left some questionnaires in the computer room. One day later we returned to find that more than twenty-five individuals had volunteered!

We have so far interviewed a total of fourteen participants, ten of whom are mentioned in this article. These ten participants were selected on the basis of the pertinence of their observations, which we assessed after a careful reading of the interview transcripts. Of the ten, half were interviewed in public facilities and the other half in their homes. Their socio-demographic characteristics are summarized in the table below. To protect the participants' anonymity and privacy, we have used pseudonyms throughout this article.

Table 1: Overview of Participants

Pseudonym	Access type (interview location)	Language	Age	Education
Barbara	Home	Portuguese*/English	40-50	Low
Camila	PF**	Portuguese	Over 60	High
Danielle	Home	English	20-39	High
Ignacio	Home	Spanish*/English	Over 60	Mid
Julia	Home	German/English*	20-39	High

[8] This article can be found online: <http://www.fis.utoronto.ca/EverydayInternet/oxford.html>.

[9] The first interview consisted of a general discussion of the participant's online activities. In the second interview, participants were asked to keep a record of their online activities and these were discussed in detail.

Marianna	PF	English	20-39	High
Nicholas	Home	English	40-59	High
Tammy	PF	English	20-39	High
Ursula	PF	German/English*	Over 60	Low
Xavier	PF	Portuguese*/English*	40-59	High

* Denotes the language in which the interview was conducted
** Public facility

The small size of our participant sample is countered by the potential for depth offered in our interactions with participants. The contacts with participants were designed to be as "naturalistic" as possible, offering them the opportunity to express their opinions and demonstrate their abilities in familiar settings. We recognize, however, the inherent and insurmountable "artificiality" of our interactions with participants and acknowledge that their opinions were expressed in a specific context, that of a conversation with a stranger, often perceived as an expert.

The participant pool is rich in experience — from professionals to novices — and diverse in character — immigrants, youth, and seniors. In fact, a noteworthy characteristic of this sample is the number of immigrants for whom English is a second language.[10] The scope of internet experience among our participants ranges from six months to more than five years. All participants use the internet regularly, ranging from several times per day to two or three times a week.

All interviews conducted during this project have been transcribed and then carefully read and revised by several members of the research team. The interviews done in languages other than English have been transcribed and then selectively translated by Ana Viseu.

For the analysis presented here, the research team reviewed and coded the interview transcripts. A cluster of privacy-related concepts — for instance, security, surveillance, identity, control, and seclusion — were then employed, in our first round of analysis, to flag and code all comments regarding privacy within the context of each individual transcript. Through this method, we selected a total of ten respondents — out of the fourteen who have been interviewed to date — for further analysis. After this initial selection, topics and patterns among transcripts were identified and quotes were organized thematically.

PRIVACY PERCEPTIONS AND ONLINE PRACTICES

[10] The presence of a fluent speaker of Portuguese and Spanish (Ana Viseu) on the research team allowed us to accommodate the linguistic needs of participants.

Privacy-related conversations were held with all participants in the study, making it the only topic about which all participants had an opinion. This resulted not only from our interest in the issue but also from the extremely varied meanings of the term privacy itself. With the exception of one or two participants, the topic of privacy surfaced "naturally" in the course of our conversations. For instance, if discussing issues of financial security, we would probe for connections with the safety of personal information. Hence, at no point did we provide a guiding privacy definition — nor were we asked to do so — although at times we did guide the discussion in a specific direction.

Considering the broader goals of the study, and the ambiguous nature of the term privacy, we found it significant that none of our participants seemed surprised to be asked privacy-related questions and that no one requested clarification about our understanding of the concept. In fact, participants seemed to view our interest in privacy issues as a natural extension of our interest in their internet usage, even when they objected to the concept itself. This indicates that the debate has moved beyond the scholarly, activist, and legal realms to reach the larger public.

When the interview transcripts were coded by different research members and the quotes were organized thematically, three interwoven "moments" of online privacy stood out: sitting in front of the computer, interacting with it, and releasing data. In the present study, these moments are not organized sequentially or temporally, nor are they mutually exclusive; for instance, the moment of sitting in front of the access point extends throughout the entire interaction. However, taken together, the three moments are constitutive of the experience of being "online" and are helpful in understanding the different factors at play during this experience.

The Places and Spaces of Going Online

Characteristics of physical space, associated with life stories and experiences, affected participant's perceptions of privacy, suggesting that the first "moment" of privacy online is shaped not only by the immediate surroundings of the individual but also by his/her overall experience. For example, Barbara and Marianna access the internet both from home and from public facilities.[11] Although their life stories are very different, they share a concern over the privacy issues involved in the use of public computers for financial transactions. Barbara is in her forties and is barely literate. Three years ago, she was pressured by her teenage children to buy a computer and get high-speed internet access. However, until recently, Barbara could not use the computer because she did not know how to. Six months before our first interview, she had an accident that still prevents her from working, and, with the free time available to her, she started taking computer classes

[11] Mainly for financial reasons, Marianna has recently started to rely on public facilities only.

at St Christopher House. Barbara does not explore the web — she mainly visits websites of entities that are already familiar to her. She readily admits to not knowing much about the internet, and her main online activity consists of financial transactions — shopping and banking — which are traditionally associated with high privacy and security concerns. Barbara speaks of the internet as a twenty-four-hour mall, a great improvement over catalogue and telephone shopping. When probed further about her views of online banking, Barbara praises the service's convenience but says that, if she did not have home access, she would not be willing to use it. The reason for this is that it would not be safe to bank with a computer that is not hers. Barbara's feeling of security does not come from an understanding of the internet's workings — she knows nothing of "cookies" left in the computer's hard-drive or network hackers — but rather from a sense of ownership: the terminal used for access is hers and is located in her private space, and therefore it is safe. Previous studies (e.g., Earp and Baumer 2003; Gronroos 1994; Rogers 1996; Pitkow and Kehoe 1996) have shown that privacy concerns decrease when individuals are familiar with the collecting entity. What our study seems to show is that familiarity, or indeed ownership, of the instruments used for access can be just as equally important.

Marianna is the youngest of our participants. She is doing her BA and started using the internet five years ago. She describes herself as someone who does not like computers but has a fair understanding of the language of the web. She says that this is because she grew up with it. She started using the internet for chatting and has now "moved on" to using it for research and e-mail. Marianna explains that her father is trying to push her to do her banking online, but she is reluctant to do so. "I think it's because I don't have access at home," she says, "and I don't really feel like banking in a public place, like, more so than I already do."

The amount of privacy (here associated with security) that is granted by the access site — public or private — is one of the factors that shape online activities.12 Online banking, owing to its sensitive nature, is assumed to be a personal activity, one that should be conducted in a private space or at least with the support of a private access point.

The issue of the intersection of private and public spaces and activities was reflected in areas other than financial transactions. Several participants spoke about the need to keep their public and private personas separate, to establish boundaries between personal and work life. Tammy, a PhD student at the University of Toronto, relies on public facilities for her internet access. She has a modem-less laptop that she refuses to take home.

> I don't want to bring either my work and all those outside concerns into a space which, for me, is a bit of a refuge.

[12] For more on the issue of the blurring of public and private spaces see, for example, Marx 2001 and Shapiro 1998.

> Somehow [the laptop] speaks to me of work, it speaks to me of obligation, it speaks to me of so many things I don't want to have when I come home.

Personal life stories also affect perceptions of online privacy. Camila and Xavier — recent Brazilian immigrants to Canada — describe the existence of two internets, one Canadian and one Brazilian. Camila, a retired nutritionist who started using the internet three years ago, while she was still in Brazil, discusses the difference between the Brazilian internet and the Canadian internet, and how in Canada it is possible to do a variety of things that would be unthinkable in Brazil.

> In Brazil, it's hard … many people are robbed, things get stolen, they steal your personal data, in Brazil it is not advisable … There they take advantage of anything to be able to clone your personal data.

> Now, here, the little I heard from people here is that, bank accounts included, everything, everything, payments and everything, is done through the web and that there is … I mean, if there are problems they are minor.[13]

This point of view, whether valid or not, points to the importance of place and cultural practices in the understanding of online privacy, or at least to the perception that the physical location of online access matters.

Releasing Personal Information

The second privacy moment has to do with how the study's participants understand the process of releasing their personal information online. It refers to the dynamic interaction between the goal of the individual's online activity, his/her perception of the medium, and the strategies used in his/her self presentation.

In August 2000 the Pew Internet and American Life Project released *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, which described the results of a telephone survey. Researchers found that about a quarter of "internet users have provided a fake name or personal information in order to avoid giving a Web site real information" (Pew 2000). Lying came ahead of the two other privacy-protection strategies mentioned in the report, e-mail encryption software (9 per cent) and anonymizing software (5 per cent). This report caused quite a stir in the media (e.g., Charny 2000) and even prompted some zealous business executives to argue that lying when releasing personal information should be made illegal and punishable by law!

[13] Original interview in Portuguese. Translated into English by Ana Viseu.

When we started our study we assumed that the number of users employing deception strategies when releasing personal information would have grown since the Pew report and that using pseudonyms to protect one's identity would be common practice. We were therefore surprised when none of our participants reported using fake identities online, not even when specifically questioned about it. (Marianna did tell us that in her old chat-room days she used a nickname, but now she no longer chats.) We found that respondents were selective when releasing their personal information, but when they did so they always gave their real identity.

The reasons given by our participants for releasing their real identity in their online interactions ranged from a certain innocence that comes from lack of experience in a new environment — their not realizing that, in internet communications, lying is not only possible but also extremely easy — to a desire for customization and minimization of the information flow and a need to establish trust.

Barbara, our shopping enthusiast, falls into some of these categories. She is selective in her release of personal information in the sense that her online experiences are circumscribed to a limited number of businesses that she already knows and trusts. Since we often give away our identity when paying in "real life," this is business as usual for her. But there is more to it. Barbara enjoys the "value-added" touch that comes with personalization: with not having to introduce her credit-card number again, with having her preferences displayed on the screen. Because she does not know much about the technicalities of the internet, she is not aware of where her personal information is stored, or to what uses her information is put. Furthermore, she is not affected by spam because she does not have an e-mail address. To her, the usefulness of personalization is clear in that it simplifies her internet interactions.

Danielle, a human-resources consultant and writer who works from her home, uses the internet both in dealing with people and as a research tool. She explains that she has only one e-mail account (with real identity) as a strategy to try to reduce the incoming data flows. She uses it in her internet exchanges but is selective when registering at a site because she does not want to be inundated with spam. That is why she does not have a Hotmail account; "those [kinds of e-mail accounts]," she says, "are the true spam." In the second interview, Danielle is even more explicit. She is growing irritated by our questions about privacy, a concept that she deems useless. She says: "[Being reluctant to release personal information is] more a concern about viruses [than a privacy issue] ... I don't sign up for lots of services because: a) I don't want lots of e-mail, and I don't want lots of e-mail even if I ask for it, and I don't want spam — period. So that's just to not be annoyed rather than not to have my privacy invaded." Although openly resisting the association between privacy and personal information, Danielle is embracing another facet of privacy, that of solitude and control of access to one's personal space. She recognizes that her desire for control of her personal space may have to do with privacy, but she is also adamant in her belief that she does not care for privacy per se. This refusal to accept the *idea* of privacy has not been studied enough by researchers.

Xavier arrived in Canada in late 2000 and, aside from the odd job, has since been unemployed. He relies on public access for his internet use and goes to St Christopher House every day, spending three or four hours doing nothing but looking for jobs. He estimates that, in the last year and a half, he has sent out about one hundred résumés. In our conversations, Xavier described some of the constraints he is subjected to when releasing personal information.

> Interviewer: [Let me ask you a couple of questions about privacy] Are you concerned about information you gave to others about yourself?
>
> Xavier: Yes. Of course. I give good information, real information about me, and I would like if people on the other side believe my information.

Xavier goes on to argue that establishing a solid and truthful identity in his online search for work is crucial. Finding a job depends on, among other things, his ability to convince others that he is who he is claiming to be, and so his release of personal information is vital if he is to be able to participate fully in the job market and, thus, in society at large.

These constraints are not much different from those that Xavier would have in "real life," but they do point to the flaws of resting a privacy argument on "freedom of choice," which is made explicit in the recurrent "opt-in/opt-out" debate. This debate involves at least three unproven assumptions: that one is indeed free to choose and that acting upon one's preferences is easy; that one is aware of the dangers; and that the context in which one chooses will remain stable over time (Viseu 2001).

Until now we have discussed matters of conscious presentation of self; however, not all personal-information disclosure is conscious and/or active. In fact, one of the often-cited online privacy threats is the monitoring ability of the internet, specifically of cookies.[14] Cookies run in the background, seamlessly part of the "normal" functioning of the web, and are operated by a party other than the user.

Contrary to what we expected, after years of public controversy — the Doubleclick story[15] that started in late 1999 is an example — only half of our participants were aware of cookies, a number strikingly similar to the results obtained by

---

[14] Cookies are small text files sent out to the user's computer when visiting a website. These text files are stored on the computer's hard drive and help track that user's browsing activities. Cookies are composed of a unique identifier that identifies that computer to the website that is sending out the cookie.

[15] In November 1999 DoubleClick, an internet advertisement company, and Abacus Direct, a direct-marketing agency, announced that they were going to merge. Public concern emerged when DoubleClick announced (in February 2000) that it was going to change its privacy policy and start correlating personal information with its cookie identifiers. This information would be gathered in a database of consumer profiles which would include each user's name and address, online surfing habits, online purchase history, and demographic data. Consumers would be able to "opt-out" by going to the company's website.

the Pew report. Furthermore, only two participants ever acted upon their fears of cookies and they now say that these fears are behind them. Our designer participant, Nicholas, emphatically states, "I used to really worry about cookies, but I don't really care anymore."

What Happens to Data in "Cyberspace" and Does It Really Matter?

The third online privacy "moment" — when personal data is released, whether voluntarily or not, into "cyberspace" — is at the core of policy discussions on privacy. In the policy- setting discourse, privacy is generally understood as the rights of individuals vis-à-vis those who collect their personal data, and the responsibilities of the collector entities towards these individuals (Agre 1998; Gellman 1998). These rights and responsibilities are assembled under codes of fair-information practices.

Though they are a favourite subject of scholars and activists, fair-information practices have not made their way into the public consciousness. In our study, participants seemed oblivious to them. In their view, once personal data has been released, there are no expectations that it will be treated with their interests in mind. Moreover, as we describe below, participants' privacy perceptions seem to be associated with an attitude of resignation and even of total disregard for the whole subject of privacy.

One of the clearest features of our subjects' privacy perceptions and practices was their passivity towards the issue. Of the participant sample discussed in this article, only one participant said that he used privacy-enhancing technologies, and he was not sure if the software was still working. This passivity seems to derive, to a large extent, from the argument that, if you have nothing to hide, you have nothing to fear. It is an argument that has been well documented in the privacy literature (e.g., Agre 1996; Marx n.d.; Marx 2003; Lyon 2001b) as a stumbling block to the development of pragmatic privacy-protection strategies, and it, too, is related to the ambiguous and symbolic nature of the term privacy itself. Privacy, as a value, becomes a concern only once it is lost. (Marx n.d.) This abstract, yet real, concept is best understood with an ecological analogy. While most people are aware of the problems of global warming and ozone depletion, the immediate gains of driving the car to work, or putting on hairspray, outweigh the often invisible losses of polluting the environment.

Nicholas summarizes the "nothing to hide, nothing to fear" argument when saying, **"**I'm not worried about [privacy] and I'm not doing anything about it, and no issues have come up about it either. You don't worry about being broken into until someone breaks into your house ... or some people do things. So, I think if I ever did get hacked I would start worrying about it, but at this point I don't have anything to hide, and don't know why anyone would want to hack into my system anyway."

But the abstract character of privacy does not fully account for the range of responses participants had towards the issue. Other frequently mentioned — and often

related — attitudes were resignation, dismissal, and annoyance.

Resignation was the most common feeling among the participants. This is not surprising given the reasons set out above, but what is noteworthy is the inclination of the participants to associate their resignation with a lack of knowledge. Camila says that she has never read a privacy policy because she is a novice with computers. Ignacio, an immigrant from Latin America who is now unemployed, makes similar remarks. He is a self-instructed computer aficionado who spends most of his time assembling and repairing old computers, yet he, too, believes that when it comes to privacy he does not know enough about it to protect it.

Xavier also displays an attitude of self-blame and resignation. He comments that the personal information he discloses on his résumé has been sold to third parties and that he receives a lot of junk mail and marketing phone calls. When asked about how he feels about this, Xavier says, "I don't know. I didn't give my information to be sold but it's a risk." We then ask him if he is aware of the existence of Canadian federal data-protection legislation. Xavier says that he is not, but he believes that his mishaps are his own fault. After all, when signing on to a new service he never reads the privacy policy. "I have never read this information, so I'm wrong to ... I'm not the kind of person to complain because I didn't read this."

Julia is working towards her PhD in social and political thought. She has resigned herself to using the internet in general, and in particular to the risks involved in online banking. She discusses her resignation in terms of lack of knowledge and lack of options: "I guess I didn't know how secure [online shopping] was. I don't really know how the internet works exactly, or I don't really know much about computers ... And I'm not particularly interested in finding out in detail. I have other things I want to spend my energy on."

The dismissal of privacy issues and annoyance at our questions were a surprise to us. The conviction with which some participants dismissed privacy concerns altogether is an issue that has not been sufficiently explored in privacy studies.

Ursula is in her mid-sixties and is a self-described obsessive compulsive with a tumultuous personal life, financial difficulties, and a daughter with serious drug-addiction problems. For her, the internet (she has a home computer and regularly uses public facilities) is a tool for personal growth and empowerment. It allows her to look for information on topics that concern her, which in many cases are rather delicate ones, such as sites on drugs or gay and lesbian issues. Given the nature of her online explorations, we expected Ursula to be worried about privacy in general, and specifically about the monitoring of her activities and the information that could be drawn from it.

In fact, however, Ursula dismisses privacy concerns, equating them with hiding, with a lack of the openness and transparency that she believes is an essential value in society: "You know something, it wouldn't upset me if someone made up their mind whether I'm a drug user or whether I ever used drugs, or whether I was gay or heterosexual, it doesn't bother me ... I mean the idea is that it is not to bother us, that's

why those [social and community] programs are available, the idea is to be comfortable with ourselves, certainly concealing drug use is not making it better, and certainly not acknowledging or not coming out is not making their life any better, so the whole idea is to be out there, period."

Furthermore, for Ursula, privacy concerns are nothing short of arrogance, an unjustified feeling of self-importance: "And really, when you think about it, why would anybody be interested [in what I do online]? I mean what does somebody want to know what you think of your mother, or what your argument was? ... I think there's something arrogant or something wrong with thinking that everybody's interested in what I'm doing, for starters."

Danielle and Nicholas — the two most internet-literate participants in our study — also associate privacy concerns with a paranoid mindset. Danielle is our most conspicuous example of the rejection of privacy concerns. She is annoyed at our questions on the subject and defends her position by saying that what she does online is simply not interesting enough to justify a paranoia about privacy. Her dislike for the concept of privacy is such that she mentions that she once "dated a programmer who was obsessed with internet privacy and had firewalls and all sorts of *crazy crap* because he's one of those people that can go into people's computers" (emphasis added).

What we may be observing here is an effect similar to that documented by Schneier (2000) in the *Secrets and Lies: Digital Security in a Networked World*. Schneier points out that a classical problem in the field of security systems is that the more alerts are generated, the less valuable they become. This may well be what is happening with our participants, since, after years of constant media exposure, we have yet to develop concrete solutions to concerns about privacy. As a result, it is possible that people are becoming immune to the problem. Also contributing to this is the belief of most of our participants (aside from Xavier, who thinks that his personal data has been sold to third parties) that their online experiences have been free of privacy hazards (at least as far as they can tell).

CONCLUSIONS

Given the small size of our sample, we do not intend to draw final conclusions about the state of privacy online. We also acknowledge that, owing to the sensitive nature of the topic, it is possible that our sample is biased towards those who are not concerned about privacy.[16] This type of bias is insurmountable and will always be present in studies of privacy. By focusing on the experience of using networked service, rather than on privacy *per se* — a technique that was previously used by Hine and Eve (1998) — and

[16] Our main concern at the start of the study was that the number of people who claim to be "very concerned" about privacy would be inflated. We expected participants to want to please us by seeming concerned about privacy.

by offering anonymity to participants, we have attempted to minimize any potential bias.

With these caveats in mind, the patterns and themes identified here are useful to understanding the broader issues involved in the field of privacy. In the first place, some of this study's findings confirm what is frequently asserted in popular and scholarly literature, for instance, the significant reach of the privacy debate, the ambiguity of the concept itself, and the gap between people's worries about privacy and the concrete actions they take, or do not take, to defend their privacy. Others, however, run counter to the prevalent assumptions. We found, for example, that privacy had a minimal impact in shaping our participants' online activities, and that their understanding of fair-information codes is close to nil. This indicates that, at best, the privacy "movement" is failing to meet its objectives, and that, at worst, it is misguided.

In our study we found that all participants interviewed understood the term privacy without a need for further explanation. This indicates that the privacy debate has reached beyond the policy and advocacy circles and become an inseparable part of the online experience. It is equally evident that individuals approach privacy from the context of their own actual practices, associating it with their individual experiences and concerns, such as place of access, spam, security, and personal boundaries. This confirms the need for empirical, situated analysis of the meanings of privacy, rather than overarching definitions (c.f. Solove 2002; Sheenan 2002; Hine & Eve 1998; Schoeman 1984; Regan 1995).

In a sense, this constitutes the paradox of privacy: in order to be effectively studied, it should be approached from a situated, often singular, context, making it hard to devise coordinated, global actions. We believe that one of the reasons for the slippery character of privacy is that the word itself points in the direction of the individual rather than the social. It is almost a misnomer, since it steers the discussion towards personal, individual preferences. This bias towards the individual makes it hard, if not impossible, to find a common approach and to make visible its value as a social good.[17]

The individual character of privacy is revealed in our participants' predominant mode of approach to privacy, a "nothing to hide, nothing to fear" attitude. This posture emphasizes a short-term vision of individual interests rather than a broader societal perspective.[18]

"Nothing to hide, nothing to fear" behaviour is best understood through our analogy between privacy and environmental concerns. Both entail risks that are abstract,

---

[17] The individualistic character of privacy has been widely debated in the privacy literature (e.g., Schoeman 1992). Among the attempts to shift the discourse towards a more social approach are that of Raab and Bennett (1998), who argue for a "sectoral approach" to the subject, that is, the search for identifying patterns among certain social groups.

[18] This is not to imply that individual responses to privacy are not important. In "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance," Marx (2003) details the significance of individual responses to surveillance.

dispersed, and distant, and benefits that are immediate and personal. In the same way that the benefits of driving one's car to work are immediately felt, so the gains of releasing personal information are immediately realized on the internet.

What is lacking, from a policy standpoint, is knowing where to go next. To continue with our ecology analogy, just as once it was very difficult for an individual to make progress towards more ecologically sound practices with household waste, it is now very difficult (and perhaps frustrating for some) to make progress towards a privacy ideal that is neither well defined nor perceived as attainable. But in the same way that the communal ideal of a cleaner environment has been "inscribed" in the daily practice of separating recyclables with thoroughgoing education and an enabling mechanism (recycling bins and fortnightly pickup), so the ideal of more socially sound privacy practices may be inscribed through education, legislation, and practical mechanisms by which people can take steps for their own and the communal good. It is necessary to create a "cyberspace" where an individual knows (and can verify) that, when he/she releases personal information, it is processed the appropriate way by the appropriate entities.

As things stand so far, however, this constitutes a critical failure of the privacy movement. Efforts to frame privacy discussions as an issue of fair-information practices have been unsuccessful in establishing accountability mechanisms that convey to individuals the knowledge of how, when, and where to release personal information, and how to enforce their rights to their own data.

In this article we describe online privacy as being constituted by three moments, each with its own meanings. However, online-privacy discussions are hardly ever directed at the first two moments — that of sitting in front of the computer and that of the actual interaction with it. Instead, attention is focused almost exclusively on the third moment, when the personal information has already been released into "cyberspace." The emphasis is not on the actions that can lead to a better understanding of privacy, but on the effects. Privacy becomes an effect rather than a process, a result rather than a continuum. The physical context and the specific characteristics of the individual who holds the personal information are lost.

Focusing on this third moment has succeeded in keeping the media's attention on the topic of online privacy, a fact that explains why most individuals are aware of the issue. Yet it has also fostered the recurrent association of privacy with the creation of a Big Brother society, and thus with a catastrophic all-or-nothing game. In this approach, individuals have privacy if they do not go online, and lose it once their personal data is in "cyberspace." Privacy becomes a risky choice: being online or not, opting in or opting out. Activists and policy developers have not been able — or perhaps willing[19] — to counter this view, which is best represented by the (in)famous statement of Scott

[19] A look at the privacy literature shows that a number of privacy advocates frequently use the Big Brother metaphor to justify privacy fears in an online world. See, for instance, Simon Davies (1992), *Big Brother: Australia's Growing Web of Surveillance*.

McNealy, Sun's Microsystem's chief executive officer: "You have zero privacy anyway. Get over it." The black-or-white approach to privacy has made the issue a media darling, and in a society that values sound bites over substance, this is seen as more than half the battle. However, the victory, if such it is, might come at the cost of losing the privacy war.

We speculate that another unexpected consequence of the emphasis on the third moment — the attempt to maintain a high state of alert — is the privacy backlash we observed in our participants. It is possible that, after years of constant media exposure, in combination with minimal experience of personal privacy problems, people are reaching a saturation stage and becoming inured to the issue. For privacy advocates, the next great challenge will be to counter this backlash.

Our study suggests that online privacy is best understood as an environment that simultaneously contains and is contained in people's activities. Borrowing from Francisco Varela's (1999) explanation of the nature of reality, we could say that privacy is neither pre-given nor constructed but rather is interpreted through one's personal experience. We must re-evaluate the privacy discourse to comprise all the moments that are involved in the practice of being online, while also creating better accountability mechanisms that make clear the options of those releasing the information and that expose the responsibilities of those involved in the process of data collection.

REFERENCES

Agre, P.E. (November 1996). "Arguments against Privacy and What's Wrong with Them." Available online: http://dlis.gseis.ucla.edu/people/pagre/arguments.html [30 Aug. 2002].

— (1998). "Introduction." In P.E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (1-28). Cambridge, Mass.: MIT Press.

America Online (AOL)/Roper Starch. (2000). "The America Online/Roper Starch Worldwide Adult Cyberstudy 2000." Available online:: http://www.corp.aol.com/PDF/Cyberstudy2000.PDF [30 Aug. 2002].

Bennett, C.J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, N.Y.: Cornell University Press.

— (1998). "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" In P.E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (99-123). Cambridge, Mass.: MIT Press.

Cavoukian, A., and D. Tapscott. (1995). *Who Knows: Safeguarding Your Privacy in a Networked World*. Toronto, Canada: Random House.

Center for Democracy and Technology (CDT). (n.d.). "Privacy Basics: Fair Information Practices." Available online: http://www.cdt.org/privacy/guide/basic/fips.html [26 Sept. 2002].

Charny, B. (22 Aug. 2000). "Protect Your Internet Privacy ... by Lying." *ZDNet News.*

Available online: http://dailynews.yahoo.com/h/zd/20000822/tc/protect_your_internet_privacy_by_lying_1.html [22 Aug. 2000].

Clement, A., J. Aspinall, A. Viseu, and L. Suchman, L. (2002). "The *Everyday Internet* Project: A 'Neighbourhood Ethnography' Informed by Current Canadian Policy Concerns." Paper presented at conference on Ethnographies of the Internet: Grounding Regulation in Lived Experience, Oxford University, U.K., 8 March. Available online: http://www.fis.utoronto.ca/EverydayInternet/oxford.html.

Davies, S. (1992). *Big Brother: Australia's Growing Web of Surveillance*. Sydney, Australia: Simon and Schuster.

Earp, J. B. & Baumer, D. (April 2003). "Innovative Web Use To Learn About Consumer Privacy And Online Behavior." *Communications of the ACM*, 46 (4): 81-83

Federal Trade Commission (FTC). (1996). Consumer Information Privacy Hearings. Available online: http://www.ftc.gov

Flaherty, D.H. (1999). "Visions of Privacy: Past, Present, and Future." In C.J. Bennett and R. Grant, *Visions of Privacy: Policy Choices for the Digital Age* (19-38). Toronto: University of Toronto Press.

Gellman, R. (1998). "Does Privacy Law Work?" In P.E. Agre, and M. Rotenberg, *Technology and Privacy: The New Landscape* (193-218). Cambridge, Mass.: MIT Press.

Gronroos, C. (1994). "From Marketing Mix to Relationship Marketing: Towards a Paradigm Shift in Marketing." *Management Decisions*, 22 (March), 4-20.

Hine, C. & Eve, J. (1998). "Privacy in the Marketplace." *The Information Society*, 14 (4): 253-262.

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

— (2001a). *Surveillance Society: Monitoring Everyday Life*. Buckingham, UK and Philadelphia, PA: Open University Press.

— (2001b). "Terrorism and Surveillance: Security, Freedom, and Justice after September 11 2001." Paper given at the Privacy Lecture Series, University of Toronto, 12 Nov. Available online: http://privacy.openflows.org/pdf/lyon_paper.pdf [12 Nov. 2001].

Marx, G.T. (n.d.). "Privacy and Technology." Revision of material that appeared in *The World and I*, September 1990, and *Telektronik,* January 1996. Available online: http://web.mit.edu/gtmarx/www/privantt.html [30 Aug. 2002].

— (2001). "Murky conceptual waters: The public and the private." *Ethics and Information Technology*, 3, 157-169.

— (2003). "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues*, 59 (1).

Miller, D., and D. Slater. (2000). *The Internet: An Ethnographic Approach*. Oxford, UK and New York, NY: Berg.

Miyazaki, A. D. & Fernandez, A. (2001 Summer). "Consumer Perceptions of Privacy and Security Risks for Online Shopping." *The Journal of Consumer Affairs*, 35 (1): 27-44.

Pew Internet and American Life Project (PEW). (2000). "Trust and Privacy Online: Why Americans Want to Rewrite the Rules." Available online: http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf [30 Aug. 2002].

Phelps, J., Nowak, G. & Ferrell, E. (Spring 2000). "Privacy Concerns and Consumer Willingness to Provide Personal Information." *Journal of Public Policy & Marketing*, 19 (1): 27-41.

Pitkow, J. E. & Kehoe, C. (1996). "Sixth WWW User Survey." Available online: http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996

Privacy Commissioner of Canada. (n.d.). The Personal Information Protection and Electronic Documents Act (official version). Available online: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html.

Raab, C. D. & Bennett, C. J. (1998). "The Distribution of Privacy Risks: Who Needs Protection?" *The Information Society*, 14, 263-274.

Regan, P. (1995). *Legislating Privacy: Technology, Social Values and Public Policy.* Chapel Hill: University of North Carolina Press.

Rogers, J. L. (1996). "Mail Advertising and Consumer Behavior." *Psychology and Marketing*, 13 (Winter), 211-33.

Schoeman, F.D. (ed.) (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, U.K.: Cambridge University Press.

Schoeman, F. D. (1992). *Privacy and Social Freedom*. New York, NY: Cambridge University Press.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley and Sons.

Shapiro, S. (1998). "Places and Spaces: The Historical Interaction of Technology, Home, and Privacy." *The Information Society*, 14, 275-284.

Sheenan, K. B. (2002). "Toward a Typology of Internet Users and Online Privacy Concerns." *The Information Society*, 18, 21-32.

Solove, D.J. (July 2001). "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stanford Law Review*, 53, 6: 1393-1462. Available online: http://law.shu.edu/faculty/fulltime_faculty/soloveda/Database-Privacy%20FINAL%20VERSION.doc [5 Sept. 2002].

— (2002). "Conceptualizing Privacy." *California Law Review*, 90 (4): 1087-1155.

Thomson, J.J. (1984). "The Right to Privacy." In F.D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (272-289). Cambridge, U.K.: Cambridge University Press.

University of California at Los Angeles (UCLA) Center for Communication Policy.

(2001). "The UCLA Internet Report 2001: Surveying the Digital Future." Available online: http://www.ccp.ucla.edu/pdf/UCLA-Internet-Report-2001.pdf [30 Aug.2002].

Virtual Privacy Office. (n.d.). "Informational Self-Determination — What Does That Mean?" Available online: http://www.datenschutz.de/recht/grundlagen/ris.xml [26 Sept. 2002].

Varela, F. J. (1999). *Ethical Know-How: Action, Wisdom, and Cognition*. Writing Science Series. Stanford, CA: Stanford University Press.

Viseu, A. (2001). "Privacy and Freedom of Choice." Posted on Nettime-l. Republished by *Noema.* Available online: http://www.noemalab.com/sections/ideas/ideas_articles/viseu_privacy.html.

Westin, A. (1995). "Privacy in America: An Historical and Socio-Political Analysis." Paper presented at National Privacy and Public Policy Symposium, Hartford, Connecticut.

Acknowledgements

We appreciate the willingness of our informants to let us into their homes and lives, spending hours with us answering our many questions. Randall Terada of St Christopher House helped us greatly in recruiting many of our informants. We found the suggestions of the anonymous reviewers useful in improving the paper. The Social Sciences and Humanities Research Council has supported this research financially.