STUDENT NOTE

PRIVACY WARS IN CYBERSPACE: AN EXAMINATION OF THE LEGAL AND BUSINESS TENSIONS IN INFORMATION PRIVACY

JEANETTE TEH[†]

[†] University of Toronto, JD/MBA Candidate 2002. Special thanks to the *University of Toronto Centre for Innovation Law and Policy* for providing me with a publication grant, Professor Lisa Austin (University of Toronto, Faculty of Law) and John Beardwood (Fasken Martineau LLP) for their assistance and guidance, as well as my family and friends for their support.

PRIVACY WARS IN CYBERSPACE: AN EXAMINATION OF THE LEGAL AND BUSINESS TENSIONS IN INFORMATION PRIVACY

Jeanette Teh

For all its remarkable attributes, the explosive growth in e-commerce and Internet use has had deleterious consequences for the privacy of participating individuals, who are often unaware of the tremendous amount of information about them that is collected and analyzed These disparate bits of data are amalgamated to yield very identifiable consumer profiles, which are subsequently sold to other organizations, depriving the consumers of their ability to control what they divulge about themselves to others, potentially resulting in a loss of individuality and creativity. Through the use of cookies, which provides numerous benefits to both consumers and retailers, the many advantages of e-commerce applications and business models are realized. However, the reliance on industry self-regulation has led to a plethora of privacy infractions in cyberspace, resulting in the enactment of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and the U.S. plan under Bush to introduce privacy legislation after the Federal Trade Commission's recommendation. The task of drafting legislation is wrought with the complexities of balancing the interests of both parties, while attempting to address the tension of employing either overly or under-inclusive language. This difficulty is demonstrated in the analysis of PIPEDA's ambiguities, which is instructive for U.S. states seeking to implement similar laws, who should note that privacy legislation ought to mandate full, informed consent through an express and explicit opt-in approach.

INTRODUCTION

The Internet revolution that has occurred over the last few years has produced astounding repercussions worldwide. Through its ease of use and widespread functionality, the Internet has created novel business opportunities, new technical and vernacular jargon, while simultaneously transforming the manner in which everything is executed and performed. Today, many everyday affairs are conducted in cyberspace, where people interact with virtual customer service representatives, virtual business partners and virtual friends. The World Wide Web (Web) has turned us into Internet citizens (Netizens) who engage in electronic-commerce (e-commerce), electronic-mailing (e-mailing), online-banking, online-learning, and even cybersex.

The Internet's capabilities are infinite because the network produces endless information, delivering whatever we command at the click of a mouse. However, its remarkable attributes are precisely the ones that can result in dire consequences for information privacy since it also enables extensive data collection about its users. While the Internet (Net) provides tremendous opportunities for information discovery, it also reduces the ability to remain anonymous, since "clickstreams" provide a detailed map of one's Web-browsing activities.[1] All this translates into the disconcerting fact that there is almost no limit to the amount of data which may be stored indefinitely, and that can be recorded, analyzed and utilized, all potentially to one's detriment.

[1] Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1625 (1999).

A. "Big Brother is Watching You"

This is the caption written underneath the ubiquitous posters featuring Big Brother's ominous face in George Orwell's *Nineteen Eighty-Four*,.[2] It refers to the omnipotent and omnipresent surveillance of the Thought Police. PWinston describes the dystopian Oceania:

> "There was no way of knowing whether [one was] being watched at any given moment…. It was even conceivable that they watched everybody all the time. But at any rate they could plug in [one's] wire whenever they wanted to. [One] had to live… in the assumption that…[one's] every movement [was] scrutinized."[3]

Some fifty years after its initial publication, Orwell's fictitious account of the future has materialized, except that unlike the citizens of Oceania, however, the Netizens of the new millennium are often ignorant of the government's and other organizations' surreptitious surveillance of them. Recently, it has come to be known that some of the American federal government sites, such as the National Technology Transfer Center and the National Science Foundation sites, have default settings in their browsers which plant cookies[4] on the computers of Web users who access their sites, completely unbeknownst to them[5].

Furthermore, global surveillance networks operated by the National Security Agency and allied intelligence bureaus, run programs like Echelon and Carnivore[6] that track telephone

---

[2] GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

[3] *Id,* at 6.

[4] *See* Privacy.net, *Bake Your Own Internet Cookies*, *at* http://www.privacy.net/cookies/ (explaining how cookies function) (last visited Mar. 27, 2002).

[5] *See* OMB Watch, *A Delicate Balance: The Privacy and Access Practices of Federal Government World Wide Web Sites*, *at* http://*ombwatch*.org/info/balance/result.html (last visited Dec. 3, 2002).

[6] Jeff Howe, *Global Eavesdroppers*, YAHOO! INTERNET LIFE , Oct. 2000, at 103 (reporting that the Federal Bureau of Investigations developed Echelon, a software-based tool, to facilitate the interception of electronic communications).

calls, faxes and e-mails of private citizens and government agencies and listen for specific words, including "bombs," "narcotics," or "President."

B. Glass Houses

Not only are private individuals subject to governments monitoring their activities, they are also faced with surveillance in the private sector from corporations who are measuring the effectiveness of their marketing tactics, and even from their fellow Netizens. Today, in our technologically dependent lives, everything we do either online, over the telephone, or over any other electronic apparatus, is subject to monitoring and scrutiny. In effect, every e-mail or conversation we have online or over the telephone line can be analogized to a postcard, an open invitation to be read or listened to by anyone. Technological advances, for all their plentiful benefits, have deprived us of our privacy by eroding the distinction between private and public affairs, so that we live in glass houses for all the world to see.

C. The Need for Comprehensively "Balanced" Privacy Legislation

It is indisputable that the Internet has completely transformed and improved our lives at the expense of our privacy. As the introduction illustrated, there exists the potential for Internet technology to completely eradicate the privacy of our communications, creating an Orwellian society in which privacy is obsolete. This potential will be made clearer in the subsequent sections on how cyberspace's technical and lucrative business aspects have resulted in deleterious effects on consumer privacy.

As will be discussed in Part VI, the failure of proposed mechanisms to protect the privacy of individuals has created the possibility that our ability to control the type of information we disseminate about ourselves will become non-existent. Part I outlines how the loss of our ability to control our information will have dire consequences for us as individuals and as a society. For instance, it could lead to a loss of individuality as we seek to expose only what we perceive to be socially

acceptable, displaying only our public personas as if we were actors on a stage every minute of our lives. This would result in a society devoid of individuality and of each person's idiosyncratic uniqueness, a society in which each and every personality begins to mirror those of others.

The erosion of privacy does not only have negative repercussions for creativity, individuality and unique personalities, but it also has fundamental ramifications for democracy as well as for social and technological progress. A society where privacy is non-existent would result in citizens' fears of being faced with criticism, social sanctions or prejudice should their private lives not meet the expectations or conform to the views held by others. Self-censorship will ultimately lead to the demise of free speech, independent thought and dissenting voices, all of which are the underlying premises of a democracy. Fears of appearing foolish or having one's failures in experimental procedures become public knowledge would hinder and impede the creation of novel ideas and inventions.

Due to the failure of self-regulation and technological solutions, comprehensive legislation is required to protect the interests of individuals in order to preserve their privacy rights in cyberspace, since these fundamental rights should be given priority over the rights of those who seek to invade their privacy. According to George Radwanski, the Privacy Commissioner[7] of Canada, the notions of permission, choice and consent are crucial in this new "culture of privacy," which refers to the widespread recognition that our personal privacy is

[7] The Privacy Commissioner of Canada, an Officer of Parliament who reports directly to the House of Commons and the Senate, acts as an advocate for Canadians' privacy rights. The Commissioner has the power to investigate complaints and conduct audits, publish information about personal information-handling, and conduct research and promote public awareness of privacy issues. The Office of the Privacy Commissioner is divided into five branches: the Investigations and Inquiries Branch, the Privacy Practices and Reviews Branch, the Communications and Strategic Analysis Branch, Legal Services, and Corporate Services. The preferred approach in investigating complaints is through negotiation and persuasion, e.g., by employing mediating or conciliatory approaches. Office of the Privacy Commissioner of Canada, *About Us*, *available at* http://www.privcom.gc.ca/au_e.asp (last visited Mar. 27, 2002).

now under threat as never before[8]. There are presently a plethora of privacy infractions precisely because there is no permission and especially no informed consent provided.

Informed consent requires knowledge as well as an understanding of the collection, use and dissemination of information, the repercussions thereof, and the existence of available alternatives. Freedom of choice is critical to privacy. The current information asymmetries that exist between consumers and the organizations that collect their data necessitate legislation mandating informed and explicit opt-in consent. However, as will be later illustrated using the recently enacted Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), difficulties which arise in drafting legislation that is not overly or under-inclusive result in vaguely-worded provisions. The analysis of the ambiguities and interpretive issues that arise in PIPEDA will be instructive for U.S. states seeking to draft similar privacy legislation since explicit definitions of certain concepts are central to the protection of consumer privacy. A further challenge exists in drafting a statute that will satisfactorily address the competing interests of both businesses and individuals alike, as fully informed consent is essential to properly protect the privacy of individuals. This complexity may be diminished by offering consumers a "menu" of various levels of privacy, in order to address the interests of those who are more or less privacy-sensitive.

I. INFORMATION PRIVACY OVERVIEW

The Canadian Privacy Commission has defined information privacy as the right of individuals "to determine what information about them is disclosed to others, and encompasses the collection, maintenance and use of identifiable

[8] George Radwanski, Address by the Privacy Commissioner of Canada Delivered to the Institute of Canadian Advertising (Feb. 27, 2001), *in* SPEECHES (Institute of Canadian Advertising, 2001) *available at* http://www.privcom.gc.ca/speech/02_05_a_010227_e.asp (last visited Dec. 3, 2002).

information.[9] Hence, privacy is deemed to be the ability and the right of an individual to control what is done to their personal information.

Traditional legal literature has tended to focus on the privacy of the individual from the government. However, as the widespread adoption in the use of technology and its increased monitoring capabilities enable individuals within the private sector to play the role of Big Brother, it is not entirely clear which principles of privacy borrowed from the public sector would apply in these situations. There are currently differing perspectives on why privacy is important, each of which will be examined in turn, as to the values that privacy protects as well as the notion of privacy as a legal right.

A. Different Types of Privacy

1. Privacy as control

The notion of privacy as having control over the type of personal information that is disseminated to others was first fully formulated by Samuel Warren and Louis Brandeis just before the turn of the twentieth century. Warren and Brandeis's concept of privacy stemmed from their observation that "the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others." [10]

This perspective is clearly reflected in the Privacy Commission's definition of information privacy. Other commentators have identified privacy as differing from the mere control of data. For instance, writer Esther Dyon believes that the latter refers to the determination of *whether* and *if* data should be collected and disseminated about oneself while the notion of privacy is more difficult to define since it differs with

[9] Communications and Society Program, Aspen Institute, *An Information Bill of Rights and Responsibilities*, *at* http://aspeninstitute.org/c&s/ibrr1.html, (on file with author) (last visited Dec. 3, 2002).

[10] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890).

each individual[11]. The example she provides is that some people discuss sex freely, but consider their salaries private, while others may think exactly the opposite. In other words, the first group would not consider their sex lives to be private but might object to how the information about their sex lives is collected and disseminated (e.g., through an interception of an e-mail between friends and then broadcast to a public chat forum). However, as Part IB will illustrate by the assertions of several theorists and examples in Part IB, this right is not absolute and ought to be balanced against societal interests to determine whether privacy will be preserved in a given context[12].

The notion of choice, which is subject to different interpretations, is crucial to the concept of privacy as control. Choice may be seen as the ability to *decide between* alternatives, or it may be defined by the *act* of choosing one alternative. The Ontario Privacy Commission defines choice as the "freedom to choose among alternatives or options, on an informed basis, and in the absence of coercion."[13] Implicit in this definition are the assumptions that individuals have sufficient knowledge or information to be able to make a choice, that the alternatives are positively valued, that they believe they own their personal information, and that have the corresponding rights to decide how it is collected, used or disclosed. Hence, choice must include bargaining power and the presence of alternatives in each situation.

The view of privacy as control has been accepted in many Canadian courts,[14] primarily in criminal cases where privacy

---

[11] Esther Dyon, *Privacy Protection: Time to Think and Act Locally and Globally*, RELEASE 1.0, Apr. 1998, *available at* http:// www.edventure.com/ release1/ 0498body.html (last visited Mar. 27, 2002).

[12] *See* John Higgins, Privacy and the Internet, Presentation at the University of Toronto Faculty of Law (Oct. 17, 2000); Information and Privacy Commissioner/Ontario, *Privacy as a Fundamental Right vs. an Economic Right: An Attempt at Conciliation* (Sept. 1999) *available at* http://www.ipc.on.ca/english/pubpres/papers/pr-right.htm (last visited Mar. 27, 2002).

[13] Information and Privacy Commissioner/Ontario, *supra* note 14.

[14] The complete list of cases holding this view is too long to enumerate. The following cases are mere examples: British Columbia Securities v. Branch, 2 S.C.R. 3 (Can. 1995); R. v. Mills, 3 S.C.R. 668 (Can. 1990); Hunter v. Southam, Inc., 2 S.C.R. 145 (Can. 1984).

has been characterized in terms of a Section 8 Charter-protected liberty to control the dissemination of confidential information, and the freedom not to be compelled to share our confidences with others. The ability to control what and how much information we give out about ourselves is a necessary precursor to fostering the values of dignity, integrity and autonomy, all of which contribute to the fundamental freedoms protected by the Charter to ensure a free and democratic society.

2. Privacy as a property right

In the model of privacy as a property right, an individual's privacy would be considered a "possession" that is alienable once sold. Patricia Mell explains that the privacy of the individual would be captured in a file collected by an organization.[15] The file becomes a piece of property that may be sold or exchanged on the market. Who, then, is the owner of this "property?" Jane's persona as an avid buyer of gardening books cannot be said to be owned by her since she did not really compile that information, nor does she have an ownership interest in the physical file or database. Hence, since she does not own the file that holds the collected information about her, she cannot be said to effectively restrict the collection, nor disclosure of this information to anyone else.[16]

Mell suggests that Jane should be the ultimate owner and have "fee simple" ownership of this persona of herself as a gardener, with rights which trump those of other organizations. The individual's property interest in the persona, Mell asserts, would be based on the *identifiability* of the persona.[17] In other words, if a link to Jane has been established, Jane would own that persona, irrespective of who compiled that information.

One could define the electronic persona as being comprised of a number of identifying characteristics, e.g., name and date of birth. By employing the language of property, Mell's

---

[15] Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1 (1996).

[16] *Id*.

[17] *Id*.

reasoning would enable the owner of this persona to be entitled to full compensation or have her consent sought before being deprived of this ownership. This would then provide individual consumers with the legal power to regulate how the information would be used and by whom, while empowering them with the ability to monitor and correct any misinformation.[18] Moreover, as Pamela Samuelson, another legal theorist asserts, the market would provide an efficient device, through the price mechanism, where individuals can bargain for the 'right' price according to their privacy preferences. However, this would likely involve substantial transaction costs since the consumer would have to negotiate separately with each prospective buyer of her data.[19]

Furthermore, this approach would force companies to internalize the social costs now borne by consumers from the widespread collection and use of personal data, which may influence firms to make better investment decisions about what data to collect and what uses to make of the data.[20]

As in the "privacy as control" model, the notion of choice also surfaces here. The Ontario Privacy Commission has asserted that reliance upon the economic self-interest of individuals to make the appropriate decisions regarding privacy is practicable *only* insofar as the mechanisms used actually strengthen the individual's ability to control and make choices about the collection, use and disclosure of that information.[21]

3. Privacy as preserving individuality

In his response to Dean Prosser, who categorizes privacy intrusions into four types of torts,[22] Edward Bloustein

---

[18] *Id*.

[19] Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125 (2000), *available at* http://www.sims.berkeley.edu/~pam/papers.html (last visited Mar. 27, 2002).

[20] *See id*., for a more detailed discussion of the application of property law to privacy.

[21] Information and Privacy Commissioner/Ontario, *supra* note 12.

[22] William Prosser, *Privacy*, 48 CAL. L. REV. 338 (1960) (discussing how the law protects privacy and suggesting that the privacy of an individual is infringed when one of the following four torts is committed:

maintains that the value of privacy has psychological, social and political dimensions beyond property or reputational interests. According to Bloustein, this is due to the fact that, unlike other torts,[23] the harm caused to privacy is not easily repaired or made good by an award of damages. Bloustein further asserts that a person who is subject to constant scrutiny, having his every thought, need or desire made known to the public would be:

> deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.[24]

The concept of privacy as a human right is related to the notion of privacy as preserving individuality. This approach, advocated by universal covenants and international human rights groups,[25] espouses the view that privacy is a moral value

---

1)intrusion into the plaintiff's seclusion or solitude, into his private affairs;

2)public disclosure of embarrassing private facts;

3)publicity which places the plaintiff in a false light in public eye; or

4)appropriation, for the defendant's advantage, of the plaintiff's name), *cited in* Edward J. Bloustein, *Privacy As An Aspect of Human Dignity: An Answer to Dean Prosser* 39 N.Y.U. L REV 962, (1964).

[23] Denis C. Kratchanov, *Personal Information and the Protection of Privacy*, 1995 UNIFORM LAW CONFERENCE OF CANADA *available at* http://www.law.ualberta.ca/alri/ulc/95pro/e95m.htm (last visited Mar. 27, 2002) (reporting that several common-law provinces in Canada, such as British Columbia, Saskatchewan, Manitoba and Newfoundland, have adopted legislation establishing a tort of invasion of privacy. However, there has not been much judicial consideration and the laws have been difficult to enforce).

[24] Bloustein, *supra* note 25, at 965.

[25] It is noteworthy that Bill S-27 ("An Act to guarantee the human right to privacy"), proposed by the Senate of Canada in order establish an act guaranteeing the human right to privacy, only passed the first reading in June 2000 and was ultimately never passed. *See* Bill S-27, Senate of Canada, 2nd Session, 36th Parliament (1999-2000), *available at*

since it supports the development of individual dignity and autonomy, thereby providing benefits to society as it strengthens an individual's capacity for autonomous action and thought.[26]

The invasion of this type of privacy would result in a profound chilling effect upon a person's thought and behavior, leading to a complete loss of her individuality and an ultimate decrease in societal diversity. This suggests that privacy should receive a lot of protection. However, Bloustein qualifies this by stating that not every threat to privacy would warrant civil liability, since living in society requires at least some scrutiny by our neighbors. Moreover, even where there is a clear violation of privacy, it still needs to be balanced with countervailing public policy or social interest, as it is not an absolute right.[27]

4. Privacy as a relational interest

Privacy has not only been viewed as protecting individual interests but also as being crucial to preserving relationships. James Rachels[28] and Helen Nissenbaum[29] both maintain that privacy is necessary in order to nurture relationships with different people, as there are definite patterns of behavior associated with different social relationships. It is our relationships with certain people that entitle them to know particular facts about us. For instance, we might be absolutely mortified if our colleagues had access to the personal e-mails that we send to our romantic partners, since information appropriate in the context of one relationship might be entirely inappropriate in others. In order to preserve the distinction of each, it might be appropriate if certain information, like our romantic e-mails, be withheld from our colleagues as it may

---

http://www.parl.gc.ca/36/2/parlbus/chambus/senate/Bills/Public/s-27/s-27_1/S-27_text-e.htm (last visited Dec. 3, 2002).

[26] Information and Privacy Commissioner/Ontario, *supra* note 12.

[27] Bloustein, *supra* note 23.

[28] James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFF. 323 (1975).

[29] Helen Nissenbaum, *Protecting Privacy In An Information Age: The Problem of Privacy in Public*, 17 LAW AND PHIL. 559 (1998).

interfere with their perceptions of us and affect our interactions with them.

5. An Ethical Framework of Information Technology

To fully appreciate the issues of information privacy, it is helpful to employ the framework introduced by Mason[30] to organize the ethical issues pertaining to information technology. This model is composed of four main categories of issues. The first is *privacy*, which refers to the collection, storage and dissemination of information about individuals. This would presumably deal with the individual's control over whom she will allow to collect and use information about her. *Accuracy* pertains to the authenticity, fidelity and accuracy of the information collected and processed, while *property* concerns the ownership and value of information as well as intellectual property issues. Finally, *accessibility* denotes the right to access information and the payment of fees associated with access. This category would also encompass *confidentiality*, which refers to a third-party obligation, akin to a duty of care, of a custodian to protect the personal information with which it has been entrusted, disclosing only to those with the right to access it.[31]

It is noteworthy that the aforementioned Canadian PIPEDA explicitly addresses each of these issues, with the exception of property, although reference to the ownership of data is arguably reflected in the consent provisions (as will be more fully discussed in Part VI). These clauses stipulate that the individual's consent is required before the collection or use of the data, implying that she has ownership of that data.

---

[30] EFRAIM TURBAN ET AL., INFORMATION TECHNOLOGY FOR MANAGEMENT 286-287 (1999).

[31] Brian Foran, *Privacy and Technology: Notes for an Address to Federal/Provincial/Territorial Social Services Information Technology Managers*, *available at* http://www.privcom.gc.ca/speech/archive/archive_e.asp (last visited Mar. 27, 2002).

B. Disadvantages of Privacy

As with any other right, asserting the right of privacy may come at the expense of other rights. The previous discussion acknowledged, the need to balance the interests of others and of society at large. Fred Cate takes a different view from the aforementioned scholars by suggesting that privacy is not an absolute benefit as it imposes real costs on society.[32]

According to Cate, privacy may serve as a mechanism of communicating false information by making it difficult to uncover such falsities while simultaneously protecting the withholding of true information, for instance, keeping information from one's employer that may be relevant to one's job performance. Further, privacy interferes with the collection, organization and storage of information that may assist businesses in making rapid, informed decisions and in efficiently marketing their products and services, thereby leading to reduced productivity and higher prices. This will be further discussed in the 'E-Commerce' section.

In addition, privacy could be an impediment to informing people of opportunities and dangers of which they would otherwise be aware, since privacy would deter what he calls "voyeuristic curiosity". Finally, and related to the latter assertion, privacy may even threaten physical safety by interfering with people's ability to access information required to protect themselves, such as whether an individual has a history of child abuse or molestation, sexual offences, or communicable diseases.

A case in point is the recent Ontario case of Peter Whitmore, a convicted pedophile. After his release from prison, his residential address was published and as a result of neighborhood outcry, he was forced to move. This time, his privacy interests were protected and his new address was not publicized. In late 2000, he was arrested once again upon being

---

[32] Fred H. Cate, PRIVACY IN THE INFORMATION AGE, 19-22 (1997), *cited in* U.S. West, Inc. v. F.C.C., 182 F.3d 1224 n.7, (10th Cir. 1999).

found with a 13 year-old boy, in violation of court orders.[33] Would this young boy have been spared his experience had Whitmore's whereabouts been publicized?[34] However, what if Whitmore had been rehabilitated and his address had still been published, possibly subjecting him to harassment or assault? At the present time, he is having trouble finding a place to live, even with help from social service organizations, as nobody wants him as a neighbor.[35] Would not his privacy and fundamental rights been severely violated and his dignity impaired had he been truly rehabilitated?

Hence, while there are clear advantages to having one's privacy interests respected, there may be trade-offs involved, as demonstrated in the Whitmore example. Further, as will be shown in subsequent sections, protecting the privacy of consumers may very well come at the expense of more sophisticated products and services that may benefit society as a whole.

C. A Technical Overview of Privacy

There are essentially three main sources of user information in cyberspace: personal computers (PC), Internet Service Providers (ISPs) and the Web sites frequented by the user. Often, completely unknown to the computer user, many bits of personal data are created and stored on these devices. The PC stores cache files that record frequently-used data values like Web pages and IP addresses onto the hard drive and its Random Access Memory (RAM) to increase the speed of connection. Hence, by searching on a PC's browser "history" and Web "cache" files, one can easily ascertain and return to previously visited Web sites. These cache files may even be accessed by computer technicians proficient in programming

---

[33] Kim Bradley, *Pedophile Can't Find a Home*, CNEWS, Oct. 31, 2001, *available at* http://www.canoe.ca/CNEWSlaw0110/31_ped-sun.html (last visited Mar. 27, 2002).

[34] *Id*. Although it is unclear what transpired between Whitmore and the boy, Whitmore has been incarcerated for eight months of a one-year sentence for breach of recognizance.

[35] *Id*.

languages like "Java scripts" and "Java applets" through the Web.[36]

1. The map of cyberspace

When Joshua surfs the Internet, his computer (the client) provides three types of information about the user to the merchant's Web server – his identity, computer configuration, and browsing activity. The user's identity is partially revealed through the IP address[37] that his computer provides to the server it wishes to contact, since a mutual exchange of IP addresses is required for two computers to communicate. However, even if Joshua is using a public computer, e.g., at school, his identity can still be revealed if he were to enter a restricted Web site, since he would have to type in his user identity and password as requested by the merchant server. Further, the computer also discloses the human language of the user, which may (once other languages start to proliferate on the Internet) reveal the user's ethnicity.[38]

Information about Joshua's computer configuration, such as his browser (Netscape Navigator or Internet Explorer), the operating system (Mac OS or Windows) and the hardware platform (e.g., IBM PC or Macintosh), will also be communicated to the server.

Finally, the server will receive details of Joshua's browsing activity, like the time and date of visit, the Uniform Resource Locator (URL)[39] of the requested resource, byte length and the

---

[36] Schwartz, *supra* note 2.

[37] To facilitate recall, this is often converted into a domain name, e.g., "joshua.smith@utoronto.ca," since IP addresses are a string of numbers, e.g., 138.249.15.49.

[38] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1226 (1998).

[39] This location address is used by the World Wide Web (the vast collection of interconnected pages of information stored on computers worldwide that are connected to the Internet) to represent links within HTML (Hypertext Markup Language – the standard Web language) documents, e.g., http://www.yahoo.com. The first part of the URL before the two slashes indicates the method of access, i.e., HTML, and that one is making a request of a Web server, i.e., www, that the name of the organization whose site being accessed is Yahoo and that it is of a commercial nature. *See* TURBAN ET AL., *supra* note 29.

URL of the resource from which the request was made. For example, when Joshua clicks on a link that is provided by a search engine, the server to which Joshua connects can ascertain the search engine used as well as the key words employed. In addition, through matching the IP addresses and identity information to their time-stamps or through cookies, Joshua's clickstream patterns[40] can be analyzed by the server.

2. Internet Service Providers

By providing Internet connection services, ISPs are able to collect fairly detailed information about their clients, who voluntarily provide their names, telephone numbers, addresses and credit card numbers in order to subscribe to the service. In addition, ISPs are also privy to information, such as surfing patterns and cyberspace activities, that their customers are not even necessarily aware of, much less have explicitly consented to disclose. Hence, ISPs are a powerful source of valuable and private consumer behavioral information, especially since ISP records can be used to identify and link Internet users to their online behavior by connecting their aliases.

A 1998 American case, *McVeigh v. Cohen,*[41] illustrates an ISP's ability to profile its client and the nefarious problems that may arise if the proper mechanisms to protect the client's rights are not in place. In this case, a volunteer coordinator of a toy drive received an e-mail supported by AOL from a donor regarding the drive, and sought to find the identity of the sender. A search for his alias in the AOL profile directory

[40] The following are sample clickstream factors recorded by Oracle's Clickstream Webhouse: site statistics (number of hits per page and the total number of site hits), Visitor conversions (number of visitors who have become registered customers and number of abandoned shopping carts), ad metrics (number of clicks that result in orders and the effect of size, color and location of ads on sales), partner links (effect of partner links on orders), site navigation (most common navigation paths taken through the site resulting in orders), site improvements, and customer analysis. All these factors are then analyzed to determine how they relate to such criteria as customer demand and promotional effectiveness. James P. Togher, *Clickstream Webhouse—The Critical Business Intelligence Tool for E-Businesses*, *in* 9 WHAT WORKS? (Data Warehousing Institute, May 2000), *at* http://www.dw-institute.com/research/display.asp?id=5304 (last visited May 6th, 2002).

[41] 983 F. Supp. 215 (D.D.C. 1998).

yielded subscriber information that linked the plaintiff McVeigh to a specific account, revealing that he was a member of the military, lived in Honolulu, was gay, and was interested in collecting pictures of "other young studs" and "boy watching".[42] The toy-drive coordinator then proceeded to forward the e-mail to her husband, who was also in the army. To learn more about this soldier, a Navy paralegal contacted AOL's toll-free customer service line and requested the identity of the subscriber who used the alias. The caller, who did not even identify himself as being with the Navy, was provided with McVeigh's personal information, which led to lawsuits against McVeigh for openly identifying himself as being homosexual, contrary to military laws. It was also later ascertained that AOL had sold different kinds of subscriber information to direct marketers.[43]

3. Web sites and cookies

Although offered as an example in the introduction, governments are not the only ones who have programmed their Web site servers to store and plant cookies[44] onto visitors' hard drives. A study conducted by the Electronic Privacy and Information Center (EPIC) revealed that that 85% of Web sites surveyed employ cookies to track the behavior of their customers.[45]

Cookies are bits of encrypted information deposited on a computer's hard drive by Web sites it has accessed, and which store details of the user's activity on that site. This enables the site's server to recognize the computer the next time it visits, so that the user will be provided with the same layout, shopping cart, search information, personalized greetings and settings.

---

[42] *Id*.

[43] Schwartz, *supra* note 2.

[44] It is rumored that cookies were named after the crumbs Hansel and Gretel left in the forest to find their way home, although theirs was actually a trail of bread crumbs, and not cookie crumbs.

[45] John Schwartz, *Internet Privacy Eroding, Study Says*, WASH. POST, Dec. 17, 1999, at E4.

Some cookies even track the activities of the user from site to site.[46]

Netscape created cookies in 1994 as a special browser feature to simplify the lives of its users by allowing them to bypass all the preliminary steps they had already undertaken previously. In essence, cookies were supposed to be akin to preference files, keeping track of how a user wants a site to look or function so that she is not required to input routine information each time she visits.[47] Of course, this also provided retailers with the perfect window to observe every movement their customers made on their sites through their clickstreams. Netscape consumers were not initially informed about these cookies on their browsers, and Netscape clearly did not anticipate the public outcry that has occurred as a result.

Two years after the birth of its first cookie and the resulting negative publicity, Netscape added a disabling tool for the next browser version. However, this was merely an opt-out scheme,[48] which required the user to affirmatively reject the cookies, a process which itself required navigation through a number of different screens. Hence, only the most technologically savvy of users have been able to detect and disable these cookies.

4. "I spy with my little UNIX"—Big Brothers Everywhere?

Thus far, this paperhas sought to establishthat governments and corporations have been tracking the activities of those who frequent their Web sites. This "living in a glass house" analogy can be broadened even further. Users who access the Internet using UNIX (an operating system like NT or Windows)[49] can

---

[46] Susannah Fox et al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, *in* PEW INTERNET PROJECT (Aug. 20, 2000), *available at* http://www.pewinternet.org/reports/toc.asp?Report=19 (last visited Mar. 27, 2002).

[47] *Id.*

[48] A negative default option. In this case, the negative default allows third-party websites to plant cookies on the user's PC unless (s)he specifically clicks or checks off the "opt-out" box. This is contrasted to the "opt-in" approach, which will only collect data if the user affirmatively selects the "opt-in" box.

[49] The use of UNIX on servers is widespread, especially in large companies. However, UNIX is not as popular amongst ordinary users, amongst whom Microsoft

perform monitoring functions on the browsing activities of their fellow surfers.[50] Simply by entering the "w" command, any user on UNIX can receive a system report of the activities of all other users on that system.[51] For example, the report may indicate that user 123C is reading "alt.politics.radical-left." The curious user can then use the "finger"[52] function to ascertain the real identity of 123C, since it provides the users' real names, when they logged in, and from where.[53] After that, the user would then be able to use the phone book function to determine what 123C does and where 123C lives.[54]

The realization that lay people without any substantial technological skills can so easily accomplish such surveying activities is rather startling and disconcerting. This concern is somewhat mitigated by the fact that the use of UNIX is fortunately not too widespread.[55] Given the ease with which such surveillance can be done by ordinary citizens, one can only imagine the surveillance capabilities of large commercial corporations and governments with access to the latest and most sophisticated technologies.

II. E-COMMERCE

As a consequence of its remarkable capabilities and the infinite opportunities it continues to create, the Internet has rapidly become a dominating force in the new millennium,

---

Windows accounts for the majority of the operating system market share. UNIX operating systems are primarily used by more technically oriented users. Interview with Ian Lopez, Systems Administrator, Microsoft Certified Systems Systems Engineer, (Mar. 12, 2002).

[50] Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 47 (1998).

[51] *Id*.

[52] The "finger" command is a protocol that uses UNIX to retrieve information, such as e-mail address, name, address and phone number, from the administrative system on particular users of a system. *See* INFORMATION RESOURCES AND TECHNOLOGY, DREXEL UNIVERSITY, *The Finger Command in UNIX*, *in* UNIX TIP SHEET SERIES, *available at* https://www.drexel.edu/IRT/helpcentral/finger.html (last visited Mar. 27, 2002).

[53] *Id*.

[54] Byford, *supra* note 54.

[55] A friend of a UNIX user, without any real technical skill, could borrow the user's UNIX terminal and use all of these functions.

resulting in a surge in new business models and industries. More interestingly, the Internet unleashes its full potential by cannibalizing and transforming the nature and core operations of many old economy businesses and products, while simultaneously creating new ones.

E-commerce consists of the buying and selling of products, services and information via computer networks, including the Net.[56]. E-commerce can be generally categorized into two broad groups: business-to-consumer (B2C) sales, where retailers sell to individual customers, e.g., Chapters.ca, and business-to-business (B2B) sales, where retailers sell to other businesses,[57] e.g., e.g., Procuron is Canada's largest B2B site, providing a marketplace of procurement services for business products/services. For the rest of the paper, e-commerce will be used synonymously with B2C retailing on the Internet (e-retailing).

E-commerce provides numerous advantages for both retailers and consumers. For instance, the Internet decreases the costs of conducting businesses by cutting administrative expenses as well as through the reduction of inventories and overhead. Likewise, customers benefit through the increase in choices of products and vendors worldwide as well as the flexibility of shopping at any time of day.

A. The Virtual Business Space

The Internet has become a mediating technology between private consumers and retailers, dramatically reducing the transaction costs of interactions for both parties. For businesses motivated primarily by profit margins, the lower cost of sales is one of the dominant reasons for going online. For example, the operating cost of an Internet banking transaction is about one

---

[56] TURBAN ET AL., *supra* note 29, at 211.

[57] However, there are also two additional forms of e-commerce involving consumers. Consumer-to-business (C2B) commerce is the opposite of B2C. In C2B, consumers state their price and companies can either accept or reject the offers, e.g., at www.priceline.com, potential customers name their prices for flights, and airlines accept or reject them. In, consumer-to-consumer (C2C) commerce, consumers sell to consumers, e.g., eBay, which mediates between consumers who want to buy or sell. *See* ALLAN AFUAH & CHRISTOPHER L. TUCCI, INTERNET BUSINESS MODELS AND STRATEGIES (2001).

penny (US) as compared to 5 cents for telephone banking and US$1-2 at a branch.[58] Further, online banks and other retailers are cutting costs and shifting the actual service work to the customers who check their own account balances or search for what they need on the web site. This can be contrasted to *paying* a paid teller to serve these same customers at a brick-and-mortar branch or store. In other words, the online marketplace ameliorates the manner in which retailers perform the information, communication, distribution, and transaction functions of business.[59]

B. 24/7 CyberShopping

Similarly, customers are embracing online commerce for the advantages of convenience and personal control, since e-retailing empowers them by providing them the ability to organize shopping or browsing around their schedule, as opposed to being dictated by mall hours, with the benefits of quick and efficient price comparisons. Furthermore, the sheer simplicity and low cost of using the Internet decreases the informational asymmetry that used to exist between consumers and businesses, thereby making it possible to diminish the power imbalance. The Internet provides the consumer with the freedom to choose from the wide array of options on the Web, resulting in a power shift from the producers to the consumers.

In the era of *mass customization*[60] created by technology, businesses strive to meet the customers' exact needs, tastes and preferences, thereby allowing consumers to be in control of the

---

[58] Harriet Johnson Brackey, *To Banks' Disappointment, People Aren't Flocking to Pay Their Bills Online*, FLORIDA TIMES UNION, Oct. 1, 2000.

[59] *See* Albert Angehrn. *The Strategic Implications of the Internet*, *at* http://www.insead.edu/CALT/Publication/ICDT/strategicimplication.htm (last visited Mar. 27, 2002) (discussing the implications of the Internet for businesses).

[60] Mass customization creates a feedback loop between customers that enables companies to react quickly to changing customer demand. *See* Eric Torbenson, *As You Like It*, CIO ENTERPRISE MAGAZINE, Feb. 15, 1998, *available at* http://www.cio.com/archive/enterprise /021598_mass_content.html (last visited Mar. 27, 2002). *See generally* Managing Change, *Mass Customization*, *at* http://www.managingchange.com/masscust/overview.htm (last visited Mar. 27, 2002).

retail relationship. The *push strategy*[61] of marketing, where the seller attempts to push its goods onto the customers may soon become anachronistic in a time where customer demands dictate what products are offered for sale (*pull strategy*). This has naturally led to a bourgeoning of novel strategies, models and concepts in business, as retailers struggle to remain viable players in this New Economy.

C. Customer relationship management

One of the latest phrases in the business world is *customer relationship management* (CRM).[62] In this business model in managing customer relations, customers define the value chain and decide how the relationship should proceed, on the basis of their interaction, responsiveness, and personalization. Businesses are no longer concerned solely with customer *acquisition*, but also with customer *retention*, through nurturing long-term relationships with them since the profit is in the *relationship* with consumers and not merely the transaction.[63]

In an era where price comparisons between various suppliers and switching costs for buyers entail a mere click of the mouse, customer retention is no longer as simple as it used to be. In fact, many Netizens are still browsing without purchasing, with only 7.1% of all hits (visits) resulting in a purchase, and only 19% of total transactions turning into loyal customers. In other words, only 1.3% of total hits become repeat customers.[64]

---

[61] A push strategy involves the manufacturer using sales promotions to induce its intermediaries to carry, promote and sell its products, whereas a pull strategy involves using advertising and consumer promotion to induce the customers themselves to ask the intermediaries for the products. *See* PHILIP KOTLER ET AL., MARKETING MANAGEMENT 521, (Canadian 10th ed. 2001).

[62] For more information on CRM, see generally PATRICK SUE & PAUL MORIN, LGS GROUP, INC., A STRATEGIC FRAMEWORK FOR CRM *at* http://www.crm_forum.com/library/art/art_100/brandframe.html, (Feb. 2001) (last visited Mar. 27, 2002); JOHN G. FREELAND, ACCENTURE, *The Evolution of CRM: Revitalizing Sales, Service and Marketing*, 2 CRM PROJECT, *at* http://www.crmproject.com/documents.asp?d_ID=756 (last visited Mar. 27, 2002).

[63] Peter G.W. Keen, Speech at the CIO Summit 2000, *in* ROB MAG. (Advertising Supplement), Oct. 2000 (on file with author).

[64] *Id.*

As a result, there are tremendous efforts made by retailers to learn about what it takes to get the first sale, such as whether physical features or banner advertisements (ads) have any effect on their buying behavior. Further, upon inducing customers to make their first purchase, companies aim to please their clients by providing them with precisely what they demand (pull strategy). This is done through sending them discount vouchers on items in which they are interested, providing various service packages depending upon their usage patterns, and even creating or building products according to their specifications, e.g., Dell custom-designed PC's.

It is thus crucial to determine what it takes to be a successful e-retailer. It has been suggested that the best electronic-business (e-business) players include those who collect their customers' personal histories through planting cookies, and using this data to provide customized information/offers to them.[65] This is done through clickstream analysis such as that performed by Oracle's Clickstream Webhouse. In fact, one of the top recommendations for CRM is to profile one's profitable customer segmentation to target the best customers and reward them while simultaneously learning how to transform the unprofitable ones into becoming profitable.

Moreover, it has been suggested that retailers embed their business processes into creating personalized sites that provide for customer self-management by turning their expensive administrative back-office tasks into the customer's valued front-office, enabling the customer to actively make their purchases and to track the status of their orders. Consumers can further define their preference options to customize their shopping experiences according to their personal tastes or to remember their account numbers, all of which are only made possible with cookies.

D. Data warehousing

The plethora of data collected about customers for CRM is stored in a data warehouse where business intelligence or data

[65] *Id.*

analytics[66] is then performed. This refers to the process of analyzing data produced and captured within businesses to enhance operations and to support strategic decisions about customers, products, expenses, and promotions.

Retailers can also use tools such as those provided by MicroStrategy Inc., which specializes in electronic-CRM (eCRM), employing customer-centric information and analysis to provide businesses with a 360-degree view of their customers as well as personalization engines to personalize the entire customer experience by incorporating real-time data analysis.[67] The real-time analysis is necessary for another novel marketing technique called interactive marketing (intermarketing), a customized relationship between vendors and buyers for advertisement and sales transactions.[68] This enables personal contact through customized, one-on-one advertising with customers while providing the merchant with a greater ability to understand the customer, market and competition. MicroStrategy also performs other tasks like specialized direct mail campaigns for certain customer segments and store or Web site rearrangements. All this is undertaken through the analysis of the data[69] collected from source systems such as the points of sale, customer demographics, vendors, and corporate financial information.

Intermarketing and direct (i.e., one-to-one personalized) marketing are deemed to be far more effective than what DoubleClick's founder Kevin O'Connor calls "closed-loop marketing," which are not aimed at a particular market segment. DoubleClick best exemplifies the technique of intermarketing through its 100 million cookies scattered

---

[66] Other names for this new business model component include: "data mart," "webhouse," and "decision support system." *See* Togher, *supra* note 44.

[67] *Id*.

[68] TURBAN ET AL., *supra* note 29, at 223.

[69] Advertising metrics collected and analyzed include: the number of hits, page views, click-throughs (response to an ad), length of stay, and repeat visitors. *See supra* note 60.

worldwide throughout its network of 11,500 sites[70]. DoubleClick's stated focus is to eliminate junk mail and to provide customers with information about the products that they want. This is done through collecting and remembering their unique responses in order to serve them better.

E. Data Mining

In addition to what consumers actively verbalize to them, vendors are also busy trying to ascertain what their clients need and desire, even if the customers themselves are not aware of these needs. Instead of merely collecting bits of isolated information, businesses are now analyzing correlations and amalgamations of seemingly unrelated data attained from various collectors and databases. Data mining, the process of searching for unknown information or relationships in large databases using tools such as neural computing or case-based reasoning[71], has emerged as yet another crucial practice in order to achieve a competitive advantage, or even to simply achieve competitive parity with one's rivals. In effect, data mining can yield five main types of information: "associations" where occurrences are linked by a single event or trait; "sequences" linking events over time; "classification" when characteristics of customers are employed to categorize them into various groups; "clustering" when different groupings of data are uncovered, and "forecasting," which estimates future values of continuous variables.[72]

An example with which every marketing student is acquainted is the initially puzzling positive correlation between the sales of beer and baby diapers. It turns out that both items are often purchased together as young fathers sent out to buy diapers would just happen to pick up a case of beer while they

---

[70] Courtney Macavinta, *Privacy Fears Raised by DoubleClick Database Plans*, CNET, Jan 25, 2000, *at* http:news.cnet.com/news/0-1005-200-1531929.html (last visited Mar. 27, 2002).

[71] TURBAN ET AL., *supra* note 29.

[72] ANN CAVOUKIAN, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER/ ONTARIO, *Data Mining: Staking a Claim on Your Privacy,* (Jan. 1998), *at* http://www.ipc.on.ca/english/pubpres/papers/datamine.htm (last visited Mar. 27, 2002).

were already in the store. With findings such as these, marketers can cleverly arrange the items in their stores or Web sites to strategically take advantage of such correlations.

Data mining thereby improves business knowledge by transforming large volumes of random data into meaningful, interpretable information, which enables the amelioration of customer service and satisfaction. It also streamlines business processes by enabling the automated prediction of trends and behavior through the use of previous promotional mailings to identify the most profitable consumers. This then assists in marketing through sales, promotions and pricing policies; trend and profitability analysis; inventory control; and customer service, which further facilitates the product development, operations, and distribution functions.

Hence, due to its ability to create and add value by empowering consumers while concurrently increasing merchant profitability through direct marketing, the Internet is rapidly embraced by both parties. There appears to be no end to the Net and e-commerce's wondrous potential, except perhaps at the cost of the individual's privacy.

III. THE WAY THE COOKIE CRUMBLES

A. Personalized Cookies: A Marketer's Dream

It would perhaps be trite to assert that retailers have benefited immensely from the advent of cookies. Precisely because of the advantages that cookies offer their clients, vendors reap the rewards gained by higher customer satisfaction through increased speed of shopping online (e.g., through bypassing passwords). A further illustration is the finding that surfers who receive personalized services tend to be the customers who actually make purchases.[73]

---

[73] For example, one study found that 68% of Web users who frequented personalized sites made purchases, whereas only 19% of those who did not have personalized sites made a purchase. Michael Pastore, *Customization Leads to E-Commerce*, *in* CYBERATLAS: INTERNET STATISTICS AND MARKET RESEARCH FOR WEB MARKETERS (Apr. 8, 1999), *at* http://cyberatlas.internet.com/big_picture/demographics/article/0,1323,5911_150721,00.html (last visited Dec. 3, 2002).

The detailed records of consumer behavior produced by cookies present infinite business and marketing possibilities. The information retailers typically collect are both voluntarily and involuntarily provided by the customer. The first three, which are crucial for the transaction to occur, are those that the customer voluntarily provides namely contact or locator information (e.g., name, postal and e-mail addresses), billing information (e.g., financial accounts and credit card numbers), and transactional information (e.g., data on purchases).[74] Other kinds of data that are of interest to marketers include information of which the consumer may not be aware, such as navigational information (revealing consumers' preferences of products, services or sites and the times of day purchases are made) and the content of correspondence directed to a marketer.[75]

Consumer profiling, yielded by the amalgamation of the above data, can help create new products and services by using the profiles to identify and assess their demand. Online profiling practices are those in which ad server companies like DoubleClick engage in by analyzing the surfing patterns of Internet users to target advertising and content to their interests and needs, epitomizing the pull strategy of marketing.

These targeted or "micro" marketing strategies have been touted as enabling greater efficiencies in advertisement, production and sales.[76] Third-party advertising networks like DoubleClick track "mouse droppings," traces left by Internet users each time they click the mouse, to determine their surfing activities and to feature advertising according to the users' interests. The goal is to target advertisements in a manner that elicits the best consumer response, as ascertained by proprietary software that determines which products and services surfers would be inclined to use, and then posts advertisements on their computer screens, significantly increasing ad

---

[74] *See generally* Direct Marketing Association, *at* http://www.the-dma.org
[75] *Id*.
[76] Byford, *supra* note 54.

effectiveness.[77] For example, since cookies planted by Chapters indicate that Jane has consistently demonstrated an interest in purchasing the latest gardening books, she is more likely than her neighbor Sam (who despises getting his fingers soiled) to subscribe to the new gardening magazine. Thus, Chapters should target the marketing of its new gardening magazine to Jane while focusing its travel magazine marketing advertisements to Sam, increasing the probability that each consumer will purchase a magazine.

Companies such as CDNow and Amazon.com are also employing "collaborative filtering",[78] a technique that involves comparing an individual's browsing and buying data to collected data in their databases, enabling them to infer the individual's interests based on other individuals' profiles.[79] For instance, Amazon e-mails its clients a list of books that similar readers have enjoyed, potentially increasing its sales while simultaneously benefiting the consumer. The filtering technique further allows companies to ultimately determine who the profitable consumers are and to invest greater efforts in catering to their needs.

B. Not The Average Cookie-Cutter Service: The Surfer's Perspective

In the face of current public outrage over cookies' potential ability to violate consumer privacy, the notion of clandestinely planting cookies on unsuspecting customers' PCs in the interests of greedy, profit-motivated companies sounds quite reprehensible. However, cookies do not provide advantages just for the retailers, but are also beneficial to Internet users.

Cookies are beneficial to Netizens because they enable custom tailoring of content, advertising, speed ordering and

---

[77] Ralph King, *Kevin O'Connor Gives People the Willies*, ECOMPANY, Oct. 2000, *available at* http://www.business2.com/articles/mag/0,1640,7184,FF.html (last visited Dec. 3, 2002).

[78] This has been likened to an automatic word-of-mouth process which produces personal recommendations by computing similarities between one's preferences and those of others. *See* F. Heylighen, *Collaborative Filtering*, *in* PRINCIPIA CYBERNETICA WEB (F. Heylighen et al., eds.) (Jan. 31, 2001) *at* http://pespmc1.vub.ac.be/COLLFILT.html (last visited Dec. 3, 2002).

[79] Robert O'Harrow, Jr. *Private or Not?*, WASH. POST, May 17, 2000, at G22.

product suggestions.[80] More specifically, cookies facilitate a one-time entry of password, registration, shipping information and indicate previously seen pages or items by highlighting them, enabling quick navigation across multiple zones of e-commerce sites. In other words, instead of re-entering one's user name and password each time one accesses a particular site, cookies "remember" the user, which enables the user to bypass all the normal access requirements. Furthermore, personalization features such as stock portfolio tracking, customized lay-out of sites and the storage of one's shopping cart or previously purchased items are possible only with cookies.[81]

In addition, cookies can control the number of times a user sees a given ad (ad frequency), and can also deliver ads targeted to user's interests, as determined by previous browsing activity, saving surfers time and freedom from unnecessary annoyance. Retailers also make customized recommendations to customers about products in which they may be interested, based on previous purchase habits and clicktrails.[82]

In spite of the numerous advantages for the consumer, the use of cookies should only be supported insofar as the consumer is provided with sufficient notice and explanations of how cookies work, as well as of the potential repercussions, as described below, that may result. In other words, consumers should be presented with the *choice* of *opting into* having cookies planted on their hard drives after they have been informed of the relevant and pertinent facts of such technology and its implications on their privacy.

C. Cookie Monsters: The Dangers Of Cookies And Profiling

For all the remarkable opportunities they present, the prevalent use of cookies can have and indeed already has had deleterious consequences. The comprehensive and ubiquitous

---

[80] See www.privacychoices.org/content_optout.htm (last visited Dec. 3, 2002), which allows visitors to opt out of DoubleClick's cookie network, but which explains the utility of cookies.

[81] *Id*.

[82] *Id*

collection of data makes it relatively easy to identify individuals. Although the case of *McVeigh v. Cohen* does not involve cookies specifically, it illustrates how easily detailed records can be retrieved and matched to a specific individual identity, merely by asking the ISP.

The recent notoriety of certain organizations in the media provides yet more data. All of the information generated by DoubleClick, which has a network of over 11,500 Web sites, was kept anonymous until it merged with a company called Abacus Direct in 1999.[83] Abacus had collected detailed data about the catalog shopping habits of approximately 90% of Americans, 99 million names and addresses, in a database of two billion consumer catalog transactions, most of which were collected almost entirely without consumer consent. In late January of 2000, the news was leaked that DoubleClick had assembled 100,000 user profiles from various Web sites and was intending to sell them to advertisers. DoubleClick suspended its plans when confronted with consumer and regulatory outcry.[84] DoubleClick CEO Kevin O'Connor's last press release on this matter on March 2, 2000, stated that the company would not link personally identifiable information to anonymous user activity across Web sites until there is agreement between government and industry on privacy standards.[85]

Although DoubleClick now provides notice of the possibility that it may link non-personally identifiable data with identifiable information, and presents its users with an opt-out opportunity in its privacy policy, it does not explain the consequences of cookies.[86] A noticeable improvement over its previous policy, it now states that information may be transferred to a company that provides services that "may assist

---

[83] King, *supra* note 84.

[84] *Id.*

[85] Kevin O'Connor (CEO of Doubleclick), Statement, (Aug. 25, 2001), *in* Center for Democracy and Technology website, *at* http://www.cdt.org/privacy/000302doubleclick.shtml (last visited Dec. 3, 2002).

[86] See Doubleclick's privacy policy, at http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=& (last visited Dec. 4, 2002).

it in its business," which is still very general and ambiguous language. However, details of who or in what business the recipient of the information may be are not provided. This broad statement will likely not enlighten the less sophisticated surfer of the consequences of what her data may be used for or what it may reveal about her. DoubleClick also reserves the right to change its privacy policy at any time in the future. Hence, users may consent to the present privacy policy, but DoubleClick could unilaterally change their operating procedures at a later date without providing recourse to the consumer. To be fair, the company now provides surfers with the opportunity to be included on an e-mail notification list to be informed of any such changes, although it is unclear how and if consent may be withdrawn.

A related problem occurs when a consumer consents to the collection of his data by Web site XYZ, but may not realize that XYZ sells or otherwise outsources its data management to ABC. This was seen most recently in the Toys-R-Us fiasco, in which Coremetrics, a rival of DoubleClick, received customer information from Toys-R-Us, which explains on its site that it collects data and allows customers to opt-out of data collection.[87] However, many retail sites like Toys-R-Us do not notify customers that their data is sent to Coremetrics, who then uses the data to build demographic information for the vendor Web sites, showing the company which pages and promotions are popular. Some companies even do so in contravention of explicitly stated policies of not sharing

[87] *Net MarketingFirm Receiving Personal Information*, ASSOCIATED PRESS, Jul. 31, 2000, *available at* http://www.privacydigest.com/2000/08/01. For more information on these companies, see Keith Perine, *End in Sight for Toysmart Data – PrivacyFight*, INDUSTRY STANDARD, Jan. 11, 2001, *at* http://www.thestandard.com/article/0,1902,21425,00.html (last visited Mar. 27, 2002); Greg Sandoval, *FTC Says Toysmart Violated Child Net Privacy Law*, NEWS.COM, Jul. 21, 2000, *at* http://news.com.com/2100-1017-243497.html (last visited Dec. 4, 2002); Linda Rosencrance, *Sharing of Personal Data by Web Sites Sparks New Privacy Controversy*, COMPUTERWORLD, Aug. 1, 2001, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47902,00.html (last visited Dec. 4, 2002); and Lori Enos, *Toys 'R' Us Sued for Net Privacy Violation,* E-COMMERCE TIMES, August 4, 2000, *available at* http://www.ecommercetimes.com/perl/story/3957.html (last visited Mar. 27, 2002).

personally identifiable data to third parties. For instance, boo.com, Toysmart, CraftShop.com, Lucy.com and Fusion.com have all been recently featured in the media for violations of their own privacy policies.[88] After declaring bankruptcy, Toysmart advertised the sale of its customer list and database, its most valuable assets, stirring much public debate and outcry.[89]

High-profile cases such as Toysmart and DoubleClick that result in strong consumer fears of online monitoring may lead to a chilling effect on Internet use. If we were to live in glass houses where constant surveillance was possible and even probable, we would certainly be vigilant about how we act by putting our public faces forward, even though we may very well be alone and unwatched. Hence, these widely publicized breaches of trust by online retailers could have a chilling effect on the activities of Web users. This may end up discouraging valuable Internet use that may be important to the surfer's wellbeing. For instance, a hyper-vigilant surfer may be worried that her insurance company may be notified (thereby leading to higher premiums) if she were to search out 'HIV' on a Web site, deterring possible preventive measures or positive treatment.

Collaborative filtering is also very much a double-edged sword: while it provides both consumers and companies with ample benefits, it could lead to inequitable results. Of primary concern is "weblining,"[90] in which companies use profiles to determine prices and terms upon which important goods and services (e.g., life insurance) are offered to individuals. In other words, products would be offered at higher prices to people whose profiles indicate that they are wealthy or have an

---

[88] *Id.*

[89] *Id.*

[90] Weblining is the cyberspace version of redlining, which would limit consumer choices in products and services or force consumers to pay higher prices. However, businesses such as Levi's sing its praises, enabling it to sell 35% more jeans and to increase its repeat visitors on its web site: Marcia Stepanek, *Weblining*, BUSINESS WEEK, *available at* http://www.businessweek.com/2000/00_14/b3675027.html (last visited Mar. 27, 2002). *See Is the Internet ripe for discrimination in 'weblining'?, at* http://www.eccins.com/html/ofinterest_news21.html (last visited Mar. 27, 2002) for a discussion on weblining in the insurance industry.

inelastic demand (i.e., are not price sensitive) for a certain product.

It has also been contended that targeted advertising is inherently unfair and deceptive. It is manipulative and preys on consumers' weaknesses by creating consumer demand that might not otherwise exist, thereby undermining consumers' autonomy.[91] This has resulted in a power shift away from the transparent, predictable consumer to omniscient corporations who now have the ability to effectively determine what the consumer will ultimately buy, through manipulations of their preferences and dislikes. Hence, because Jane is constantly swamped with gardening and home-related products, she may very well never learn about new mystery novels or the latest travel ideas. Likewise, just because Sam does not have a green thumb, this does not preclude him from developing an interest later on or from enjoying other aspects of home décor, which he could be missing out upon if Chapters continues to feature only ads pertaining to travel. This type of micro-marketing could result in pigeonholing consumers into one type of buyer and restrict their consumption patterns.

This in turn restricts the ability of individuals to define themselves, and may lead to "data predestination," where personal data becomes a self-fulfilling prophecy for consumers, defining the types of offers they receive and profoundly limiting their knowledge of available alternatives. The lack of awareness of the full array of available options would effectively rob consumers of the choice to decide for themselves what they would like to purchase, whether or not they have previously expressed interest in such products.

Further, as Katrin Byford argues, while the bits of information collected by corporations are relatively permanent and long-lasting, personal preferences and self-constructs are

---

[91] SPECIAL COMMITTEE ON INFORMATION PRIVACY IN THE PRIVATE SECTOR REPORT, REPORT TO THE LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA (4th Sess., 36th Parliament, Mar. 20, 2001), *available at* http://www.legis.gov.bc.ca/cmt/36thparl/priv_ps/Reports/report010320.htm (last visited Mar. 27, 2002).

not.[92] Instead, they are very dynamic and continuously change in response to the fluctuating environment. Being bombarded with an external image of oneself (Jane as a gardener and Sam as an avid traveler) may impede one from altering this defined conception of self, depressing creativity and autonomy and stifling one's growth.[93] This constitutes an invasion of one's "expressive privacy," which is the freedom from coercion and discrimination when making personal decisions, thereby impeding the free development of one's self-identity.[94]

Once again, the trade-off between the benefits and disadvantages of technology is underscored. Cookies and the Internet, in general, have provided us with many novel applications and enhancements in both our business and personal lives. However, they may very well exemplify Pandora's Box, providing the enticement of wonderful gifts at the very expensive price of privacy, and perhaps even individuality.

IV. PROBLEMS IN CYBERSPACE

The problem of collection and sharing of personal data is not unique to the New Economy. However, the Internet's widespread adoption, universality and seemingly infinite capabilities have enabled direct marketing to operate at an unprecedented level. It was not until 1997 that the general public began to realize the deleterious effects the Internet has on privacy.[95] In fact, it is even questionable today just how much of the population fully comprehends the nature of the threat cyberspace poses to one's privacy.

A. Web Privacy Unmasked: The Current Situation

It was reported in April 2000 that of 30,000 Web sites surveyed over nine months by enonymous.com, a Web privacy

---

[92] BYFORD, *supra* note 49.

[93] *Id.*

[94] *See* Emir A. Mohammed, *An Examination of Surveillance Technology and Their Implications for Privacy and Related Issues – The Philosophical Legal Perspective*, JOURNAL OF INFORMATION, L. & TECH., *available at* http://elj.warwick.ac.uk/jilt/99-2/mohammed.html (last visited Mar. 27, 2002).

[95] Keith Perine, *The Persuader*, THE INDUSTRY STANDARD, Nov. 6, 2000.

rating company, and research firm PC Data, only 3.5% qualified for a four-star rating.[96] This rating meant that the site never shared personally identifiable information with third parties, or used the data to contact a user without permission. More perturbing was the fact that 73% of the sites surveyed did not have a privacy policy at all.[97] Furthermore, it was found that the privacy policies of sites changed frequently. As many as 27% of the sites surveyed changed their policies in the span of nine months and changed them significantly enough to warrant a new rating.[98]

One example is Amazon's unilaterally changed privacy policy, posted on August 31, 2000, and which resulted in an onslaught of letter-writing and protests by privacy advocacy groups.[99] The change would have been more acceptable had Amazon e-mailed its clients regarding its amended policy, asking their permission.

Amazon's policy now classifies information as a business asset that would be transferable if Amazon or one of its business units were sold.[100] Furthermore, its previous promise that it would never rent or sell information, and the opt-out provision no longer exist in its new policy.[101] Of course, there are other companies who go so far as to directly contravene their stated privacy policies, such as the aforementioned case of Toysmart whose privacy policy stated that "personal information voluntarily submitted by visitors to our site….is never shared with a third party".[102] Instead, in the face of

---

[96] *Web Privacy Report: Yay, Boo* (April 11, 2000), *at* http://www.wired.com/news/print/0,1294,35594,00.html (last visited Mar. 27, 2002).

[97] *Id.*

[98] *Id.*

[99] Keith Perine, *Privacy Centers Have Their Eyes on Amazon,* (Dec. 4, 2000), *at* http://www.thestandard.com/article/0,1902,20586,00.html (last visited Mar. 27, 2002).

[100] *See* http://www.amazon.com for its privacy policy.

[101] *Id.*

[102] See supra text accompanying note 94.

impending bankruptcy, Toysmart put its customer database up for sale as its most valuable and liquid asset.[103]

Even when companies act in good faith by providing prior notice to their customers and receive their consent to collect what is, at the outset, anonymous (i.e., nameless) data, sometimes these can be linked to personally identifiable information. For example, a network advertising company could operate its own Web site at which consumers are asked to provide personal information, which could then be linked to the identification number of the cookie placed on their computer by that company, making all data collected through that cookie personally identifiable.[104] This is precisely what DoubleClick does through its DART technology. Another possibility is that a corporation may end up acquiring another company that has a whole warehouse full of personally identifiable data. An amalgamation of the two databases would produce some very detailed and personally identifiable profiles, which is what DoubleClick attempted to do in its acquisition of Abacus Direct.[105] Hence, even where there is informed consent in which consumers choose to accept cookies and to partake in transactions with full knowledge of the companies' stated intentions, such consent would no longer be valid where there are unilateral changes to the policies or in situations such as the DoubleClick-Abacus acquisition.

The enonymous.com and PC Data findings substantiate an earlier study by EPIC scrutinizing 100 of the most popular online shopping sites for compliance with "fair information practices," the American industry standard.[106] EPIC discovered that none of the sites met all the basic criteria for privacy protection. The criteria included providing notice of the type of information collected and how it is used, providing consumers

---

[103] *Dead Site? There Goes Privacy* (Jun. 30, 2002) *at* http://www.wired.com/news/print/0,1294,37354,00.html (last visited Mar. 27, 2002).

[104] FEDERAL TRADE COMMISSION, ONLINE PROFILING: A REPORT TO CONGRESS, (July 2000), *available at* www.ftc.gov./os/2000/07/onlineprofiling.htm (last visited Mar. 27, 2002).

[105] KING, *eupra* note 78.

[106] SCHWARTZ, *supra* note 44

with some choice over its use, allowing consumers to correct the data, and implementing proper security measures to ensure that information is not given to third parties.[107] Furthermore, 35% of the sites featured profile-based advertising while 87% used cookies.[108] In addition, although 82% of sites surveyed by EPIC posted a privacy policy, they tended to be confusing, incomplete and inconsistent.[109] It is noteworthy that there are a multitude of studies that yield very similar findings, pointing to the lack of notice about the collection of consumer data and a record of poor adherence to their posted privacy policies.

To further aggravate the violation of consumer privacy, consumers are not only being monitored by cookies planted through the Internet, but may also be observed by the electronic eavesdroppers that come attached to *purchased* software installed on their PCs. Thus, when a user connects to the Internet, these programs use the opening port to send information that has been stored on the hard drive, such as surfing habits or identifying personal information, to the manufacturer of the software or marketer so they may develop new products or advertising campaigns.[110] One Web site has identified more than 400 of these data-gathering and tracking programs.[111] Although most of these are free "shareware" that people download off the Web, there are an increasing number of mainstream similar programs that people actually pay for.

This stealthy "spyware" has been found in more than 100 titles of Mattel Interactive's Learning educational programs such as Reader Rabbit, Arthur Reading Games, and Intuit Inc.'s financial planner Quicken, which has acknowledged that it used tracking programs to target ads .[112] A computer technician, whose job is to specifically remove such stealthy programs, reported that many of his clients have become afraid to use their computers due to the fear of the computer sending

---

[107] *Id*.
[108] *Id*
[109] *Id.*
[110] Ariana Eunjung Cha, *Your PC is Watching*, WASH. POST, July 14, 2000.
[111] *Id.*
[112] *Id.*

out personal information.[113] Furthermore, he says that some of these tracking programs crash computers, clog up their telephone or cable lines, or are impossible to remove. [114]

B. Cyber-distrust

The Pew Internet & American Life Project undertook a study of over 1,000 Internet users this spring to ascertain how Americans felt about privacy and trust online.[115] The main finding of the study indicated that users preferred a privacy-friendly default on the Internet. Specifically, 84% of users were concerned that their personal information would be divulged to businesses to which they had not granted permission.[116] Another significant finding revealed that most Internet users did not know the basics of how their surfing activities were observed, nor did they use any tools to protect their privacy. An overwhelming majority, 86% of respondents, preferred an "opt-in" approach to consent as opposed to the "opt-out" model preferred by businesses.[117]

According to a Business Week Survey in March 2000, 89% of consumers were not comfortable with having their browsing habits and shopping patterns merged into a profile linked to their real name and identity.[118] In addition, 63% of consumers opposed profiling even when data were not personally identifiable and 92% of Internet users opposed wholesale dissemination of personal information.[119]

The level of consumer distrust of online retailers has had demonstrably negative repercussions for businesses. 80% of 2000 Canadians surveyed shop less online because of privacy

---

[113] *Id.*
[114] *Id*
[115] FOX ET AL, *supra* note 45.
[116] A survey by the National Angus Reid Report in November 1999 demonstrated a similar figure (80%) when asked this question to 1500 adult Canadians: ERNST AND YOUNG 1999 PRIVACY ISSUES SURVEY, *available at* http://www.ey.com/global/vault.nsf/Canada/PrivacyIssues_1999/file/privacyissues.pdf (last visited Mar. 27, 2002).
[117] *Id.*
[118] FEDERAL TRADE COMMISSION, *supra* note 104.
[119] *Id.*

concerns.[120] Jupiter Communications estimates that privacy concerns could put a 45% dent in the projected e-commerce revenue.[121]

However, while people seem to worry about their privacy on-line, they are ironically oblivious to just how much information they give over the Net, especially in the hopes of winning free trips or discounted merchandise. What is even more surprising is that this carelessness prevails even amongst those who are technologically-savvy and are actually aware of privacy infractions.

C. A Brave New World: A Culture of Compliance?

Perhaps the fact that even those of us writing papers on the invasion of online privacy continue to disseminate information about ourselves either inadvertently or in order to receive certain services, such as journal articles over the Internet, suggests a culture of compliance. As Ursula Franklin explains:

> [T]oday's real world of technology is characterized by the dominance of…technologies…. [that]are exceedingly effective and efficient, [but] come with an enormous social mortgage [which means] that we live in a culture of compliance, that we are ever more conditioned to accept orthodoxy as normal, and to accept that there is only one way of doing it.[122]

In other words, we have all become socialized to accept that whenever we enter certain Web sites, we will be required to provide our e-mail addresses and personal information, which we actually give as consideration, in order to receive the services they offer "for free". For instance, the author of this

---

[120]Showwei Chu, *Online lies cast doubt on e-biz databases*. (Aug. 10, 2000), *at* http://globetechnology.com/search97c…ts%26Resultstart%3D21%26ResultCount%3D10& (last visited Mar. 27, 2002).

[121] HIGGINS, *supra* note 11.

[122] Ursula Franklin, THE REAL WORLD OF TECHNOLOGY 25 (House of Anansi Press 1992) (on file with author).

paper recently registered at a writer's Web site as that was the only way she could receive a very helpful article for her essay. The registration policy indicated that:

> [T]his site requires registration in order to access the content. In order to register, your browser must accept cookies…[which are used] to expedite future login operations and for content reporting purposes only….Unique identifiers (such as user ids) are collected to verify the user's identity. Demographic and profile data is also collected at our site. [123]

She put in as little legitimate information as possible and then, like a growing number of her fellow Netizens, fudged other personal details about herself and put down a false e-mail address. A recent survey of 200 Internet users in British Columbia indicated that more than one third falsified personal data due to privacy concerns. This presents an obvious problem to businesses who rely on this information to market products to the appropriate market segments.[124] This is the "social mortgage" referred to by Franklin– information has now become a very valuable form of currency.

On the other hand, while we abhor the notion of corporations invading our privacy, some of us also embrace the personalization features. The implanted cookies eradicate the need to re-enter our passwords each time we enter the site, or preserve the highlighting of articles that one has already downloaded when one's computer crashes in the midst of a big research endeavour. The benefits conferred by cookies in the realm of service personalization remain undisputed. Perhaps life is now imitating the art in Aldous Huxley's novel *Brave New World* in which people accepted daily totalitarian intrusion as something beneficial to them.

---

[123] *See* www.mohansawhney.com (last visited Mar. 27, 2002).
[124] CHU, *supra* note 120.

V. INFORMATION AS CURRENCY

Many Internet companies have not yet realized real earnings and investors are using various alternative criteria to assess the future potential and growth of businesses. Some of the factors include the number of hits or users a Web site has, as well as the quantity and quality of information that a company has about each user, the ultimate tools in marketing.[125] Information is an incredibly valuable form of "non-monetary currency" that can be resold to other organizations, illustrating how information has now become an incredibly valuable asset in itself.[126]

Perhaps online tracking of consumer behavior is the price that we pay for a free Internet, since companies will have to make revenue through other means, the most viable of which is advertising. Online marketers have asserted that without the revenues gained from targeted advertising, most of the content on the Net would not be free, nor would e-commerce have grown as much as it has.[127]

Economic activities are increasingly being dominated by the production, distribution, and the consumption of information. In effect, information has become a commodity which Web surfers use to exchange for free products or services, either implicitly through discounts or customized content, or explicitly through financial payment. It has been reported that more than 80% of users would provide personal information (including name, education level, age and hobbies) in exchange for customized content.[128] Regular online purchasers, defined as those who have made an average of 7.5 purchases in the last six months, prefer to give out information when they receive

---

[125] Dave Steer, *Privacy Practices Help Build Trust, Get and Retain Web Customers* (Oct. 29, 1999) *at* http://ecmgmt.com/Nov1999/feature.article.htm (last visited Mar. 27, 2002).

[126] *Id*.

[127] *e-Business Watch*, E-TRADE CANADA (Aug. 25, 2000) *at* http://198.96.119.54/archives/article.cfm?articleId=46&where=article (*on file with author*)

[128] Michael Pastore, *Privacy Issues Dividing Internet Customers* (Apr. 24, 2002), *at* http://cyberatlas.internet.com/markets/advertising/print/0,5941_346371,00.html (last visited Mar. 27, 2002).

specific benefits for sharing it, including a chance to win free goods.[129] In fact, 30% of online shoppers will give out some data to their favorite retailers even when they are not buying.[130]

Perhaps this seemingly contradictory result, which appears to be at odds with the surveys discussed in the preceding section in which consumers stated that they were opposed to profiling or having their surfing activities observed, may be explained by the notion of fair consideration or *quid pro quo*. It may be that consumers are more likely to be receptive to being monitored or may voluntarily provide personal information or preferences if they feel that they are receiving tangible benefits in return. Alternatively, it could be that targeted survey questions about privacy influence the consumers' actual perception of their concern. This could explain the apparent failure to realize or fully appreciate the potential repercussions of providing personal information on the Net.

A. Cash-for-Clicks

A new marketing technique has emerged amidst the privacy firestorm whereby companies employ a permission-based model, "cash-for-clicks", where users are paid to surf the Net. For example, Advertising.com Inc. and AllAdvantage Inc. each pay members US$0.20 to $0.50 for every hour spent on the Internet.[131] These firms require members to download a program that sets up a small advertising window at the bottom of users' computer screens each time surfers go online. The windows are rented to advertisers and display a constant stream of small ads, providing the advertisers with access to customized audiences of Internet surfers. These advertisers pay fees based on the number of times they want their ads shown in the window or how often their ads are clicked on. Internet

---

[129] *Id.*

[130] Michael Pastore, *Consumers Fear for their Online Privacy* (Nov. 1, 1999), *at* http://cyberatlast.internet.com/markets/retailing/print/0,,6061_228341,00.html (last visited Mar. 27, 2002).

[131] Sean Holman, *Get paid to surf by cash-for-clicks firms*, GLOBAL TECHNOLOGY, Jun. 9, 2000, *at* http://news.globetechnology.com/archive/20000609/ECSURF.html (last visited Mar. 27, 2002).

advertising (Web-vertising) which reaches a specific, targeted audience is more advantageous than advertising that reaches mass audiences.[132] These electronic ads are clicked on two to three times more frequently than regular banner ads, and since these ads enable consumers to link to an advertiser's Web site by merely clicking on an ad, they facilitate and increase the likelihood of purchases.[133] LifeMinders, a rival of DoubleClick, which has a database of 18 million members, is an example of permission-based marketing in which their members specifically "opt in".[134]

However, although these consumers have freely consented to having their browsing activities monitored, they probably do not fully appreciate the consequences of divulging too much of their personal information since they may be broadcasting anything from their personal habits and interests to their sexual preferences.

B. A Consumer Data Exchange

A fairly recent announcement has advanced the movement toward the commodification of personal information even further. Several dozen e-commerce companies, including IBM and MicroStrategy, are creating the Customer Profile Exchange Standard (the Exchange), a common language system designed to facilitate their ability to share names, identification numbers and behavioral patterns.[135] The resulting faster transmission of information will enable companies to buy demographic consumer information from data retailers or to have data mining analyses performed, thereby decreasing the time required to develop and market new personalized products.

The Exchange specifications will include instructions on maintaining consumer information details such as names,

---

[132] *Id.*

[133] *Id.*

[134] John Schwartz, *'Opting In': A Privacy Paradox,* WASH. POST, Sept. 4, 2000, at H01.

[135] Robert O'Harrow, Jr. *Internet Firms Act to Ease Sharing of Personal Data*, WASH. POST, Dec. 5, 2000, at E01.

taxpayer identification numbers, national identifiers, passport numbers, primary residences, telephone numbers, addresses, e-mail, educational history, marital status, birth dates, income levels, occupations, hobbies and even information like whether the subjects smoke.[136]

Supporters of the Exchange suggest that it will protect privacy since it allows companies to attach a consumer's privacy preferences to each record. However, privacy advocates are raising concerns that the corporations' abilities to compile records about individuals will be far ahead of what consumers will actually comprehend or be able to restrain.[137] In other words, while a consumer may not mind providing isolated bits of data, e.g., she e-mails the name of her favorite author to Retailer A, and the name of her high school to Retailer B, she may not realize that these two separate bits of information could be combined to create a more comprehensive profile about her.

For instance, Acxiom Corp. stores records of 200 million Americans, including such information as their purchase histories and the value of their homes.[138] It then combines data from different sources and displays such information to its business partners.[139] It is very possible that bits of previously anonymous information that customers had provided, end up being aggregated to yield very identifiable and detailed profiles.

VI. PRIVACY SOLUTIONS

Over the last few years, approximately five categories of mechanisms to protect or address the privacy concerns have surfaced:[140] self-regulation (a laissez-faire approach of governance), private sector initiatives, government regulations, technological solutions and consumer education, each of which will be examined in turn.

---

[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] DON TAPSCOTT, THE DIGITAL ECONOMY: PROMISE AND PERIL IN THE AGE OF NETWORKED INTELLIGENCE 279-81 (1996).

A. Laissez-faire: Letting Cyberspace Govern Itself

The "invisible" hand notion of Adam Smith's laissez-faire theory is not a practicable reality in the privacy realm of the Internet. This is perhaps most clearly illustrated by the fact that several resolutions have been introduced in the United States Congress seeking to protect consumer privacy,[141] even though the Clinton Administration had previously advocated self-regulation.

Until 1998, the Federal Trade Commission (FTC) had supported self-regulation. However, in June of that year, the FTC delivered a report to Congress outlining the absolute failure of the online industry to protect consumer privacy in gathering and using personally identifiable data.[142] After examining 1400 Web sites, it found that few sites had privacy policies or disclosed how information would be used, resulting in a call for regulation.[143] In response, a trade group representing more than 11,000 companies requested another chance at self-regulation with the following proposed guidelines:

1) **Choice:** letting consumers opt-out of data collection and informing them when their information will be shared by third parties;

2) **Access and Accuracy:** giving people access to their digital profiles so that corrections may be made when necessary;

---

[141] See, for example, the "Consumer Internet Privacy Enhancement Act", the Consumer Internet Privacy Enactment Act, H.R. 237, 107th Cong. (2001); the Consumer Privacy Protection Act, H.R. 2135, 107th Cong. (2001); and the Online Privacy Protection Act, H.R. 89, 107th Cong. (2001).

[142] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (Jun. 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Mar. 27, 2002).

[143] Courtney Macavinta, *Net Industry Reacts to FTC Threat*, CNET NEWS, Jun. 3, 1998, *at* http://news.com.com/2100-1023-211867.html

3) **Accountability and Recourse:** setting a clear mechanism enabling individuals to seek recourse for violations of a stated privacy policy;

4) **Notice:** requiring that a policy for collection, use and disclosure of any personal data collected from people must be prominently posted;

5) **Disclosure:** not disclosing data to third parties unless they have adopted practices to protect privacy;

6) **Collection:** only harnessing and using personal data that is "appropriate and needed";

7) **Security:** shielding consumers' data from unauthorized parties; and

8) **Enforcement:** supporting strong enforcement of consumer protection laws.[144]

However, as has been illustrated throughout this paper, there are a plethora of privacy infractions that have violated not only the above principles but the companies' own stated policies. Online businesses have the most to gain from the absence of legislation and would benefit by being able to collect information about their clients unimpeded by laws protecting the consumer. Hence, the online industry, in spite of their proposed guidelines, has "use[d] collective action to lock in a poor level of privacy at a societal level."[145]

---

[144] *Id*.
[145] Schwartz, *supra* note 2 at 1690.

An outrageous illustration of the need for government regulation involves Pharmatrak, a Boston technology firm that placed two invisible lines of HTML Identity Codes on computers that visit its eleven pharmaceutical client Web sites.[146] These cookies were planted through a software code called a "Web bug", which is programmed to send information back to the originating Web site.[147] The bug cannot be detected unless the browser is set on a mode to alert the user of this specific process. Web bugs collect such information as whether the same computers have downloaded information about HIV or a particular type of drug. This aggregated information is then shared with clients such as Pfizer, SmithKline Beecham and Glaxo Wellcome, even though privacy policies are not posted on these client sites. Pharmatrak discloses on its site that it plants cookies.[148]

Pharmatrak's officials have stated that they can predict if their visitors are consumers, physicians, journalists or government officials based on the cookies and what they access; however, what was shocking was Pharmatrak's suggestion that they might develop products that would directly identify individual Web site visitors: "in the future, [Pharmatrak] may develop products and services which collect data that, when used in conjunction with the tracking database, could enable a direct identification of certain individual visitors."[149] However, as a result of a lawsuit reported on August 18, 2001, this language was removed from the policy.[150] Instead, the current statement pledges that Pharmatrak will never collect personally identifiable information without explicit authorization from the subject.[151]

---

[146] Robert O'Harrow, Jr., *Firm Tracking Consumers on Web for Drug Companies*, WASH. POST, Aug. 15, 2000, at E01.

[147] *Id*.

[148] *Id*.

[149] *Id*.

[150] Gavin McCormick, *Privacy II: California Man Sues Pharmatrak*, BOSTON.INTERNET.COM, Aug. 18, 2001, *at* http://boston.internet.com/news/print/0,,2002_44821,00.html (last visited Mar. 27,2002)

[151] *Id*.

The above examples as well as the slew of DoubleClick and Toysmart-type lawsuits demonstrate that self-governance is clearly inadequate. While most of the privacy violations have not yet resulted in such dire consequences as the Pharmatrak case, they certainly demonstrate what could happen without more regimented regulation and protection measures.

B. Other Voluntary Private Sector Initiatives

The private sector has come up with three main types of voluntary regulatory regimes – codes, standards and privacy seal programs.

A "voluntary code" is a "commitment made by one or more firms to abide by a stated set of practice principles".[152] Similarly, a "standard" is a "formal voluntary code setting out a documented agreement containing technical specifications or other criteria that a product, process or service must meet".[153] Examples of industry standards include the Platform for Privacy Preferences (P3P)[154] and the Direct Marketing Association's (DMA) guidelines.[155]

A "privacy seal program" ensures that there is proper disclosure of a Web site's privacy and security practices and that a trusted third party is monitoring the sites' compliance

---

[152] Allan McChesney, *Feasibility Studies for New Standards Relating to Consumers and Electronic Commerce (For the Office of Consumer Affairs, Industry Canada)* (2000) at http://strategis.ic.gc.ca/SSG/ca01275e.html (last visited Mar. 27, 2002).

[153] *Id.*

[154] The P3P is an Internet protocol designed to be an automatic privacy-protection agent proposed by the World Wide Web Consortium (W3C) which is composed of over 400 member organizations. The P3P would provide a warning on the screen when the surfer enters a site that does not meet her privacy requirements, as determined by the standardized multiple-choice questions about privacy policies. While this may benefit some users, it will be confusing for less technically-savvy users who may not realize that they are supposed to change the default user settings to more privacy-sensitive settings. Further, the P3P does not implement basic privacy threshold standards: Chris Oakes, *Privacy Protocol Lauded, Sort Of*, WIRED NEWS, Jun. 22, 2000, *at*. http://www.wired.com/print/0,1294,37145,00.html (last visited Mar. 27, 2002); John Schwartz, *'Opting In': A Privacy Paradox*, WASH. POST., Sept. 4, 2000, at H01.

[155] The DMA requires that its members provide notice to their customers regarding the information collection. It will also assist in the resolution of disputes although there is no minimum threshold prescribed for privacy requirements nor is there explicit mention of auditing of its member sites, which mean that non-compliance may not be detected. *See* http://www.the-dma.org (last visited Mar. 27, 2002).

with their stated policies, e.g., TRUSTe.[156] Furthermore, through educating consumers and providing them with recourse in the event of breaches of privacy policies, these programs seek to increase consumer confidence in e-commerce.[157]

The advantage of these initiatives for consumers is that they may be used as a benchmark against which consumers can make online comparisons between various retailers.[158] They may also build consumer trust. However, given that Toysmart and others who have violated their privacy policies have been TRUSTe-approved, it is clear that these private sector programs do not sufficiently protect consumer rights, making them wary and even suspicious of voluntary arrangements as compared to legislation. In addition, with the onslaught of privacy seal programs, the adoption of a standard may not impress or mean anything to a customer without a strong public awareness campaign, endorsement by government and well-known consumer groups. Further, it is often very difficult for consumers to ascertain whether a voluntary code is adequate to protect their interests or to recognize that businesses have carved out ample loopholes for themselves.[159] Finally, the P3P and other technologically based solutions will not only

---

[156] TRUSTe is a non-profit organization that acts as a guarantor of privacy, endorsed by the Internet Content Coalition (an alliance of content providers). The TRUSTe seal is provided to companies that meet its privacy guidelines which should disclose the type of information gathered, how the information is used, with whom the site shares information, whether users can correct and update their personally identifiable information, whether users will be deleted or deactivated from the site's database upon request, and whether users may opt-out of giving specific information to third parties. *See* TRUSTe, THE TRUSTE PROGRAM: HOW IT PROTECTS YOUR PRIVACY, *at* http://www.TRUSTe.org/consumers/users_how.html (last visited Mar, 27, 2002). However, TRUSTe does not appear to be that effective in its monitoring or enforcement since the aforementioned boo.com, Toysmart, Lucy.com and Fusion.com, all of whom have been featured in the media for privacy violations, were TRUSTe guaranteed. Perine, *supra* note 88. See the following web sites for other seal programs: http://ftp.aicpa.org/public/download/webtrust/privacyexp.doc (last visited Mar. 27, 2002) and http://www.bbbonline.org (last visited Mar. 27, 2002).

[157] Dave Steer, *Privacy Practices Help Build Trust, Get and Retain Web Customers*, ECMGT.COM, Oct. 29, 1999, *at* http://ecmgt.com/Nov1999/feature.article.htm (last visited Mar. 27, 2002).

[158] OAKES, *supra* note 155.

[159] *Id.*

empower the individual, but also the organizations that collect this data, resulting in a game of survival of the technologically fittest, with the ultimate winners being those with the deepest pockets – most likely the retailers.

Businesses naturally prefer voluntary arrangements such as codes and standards, rather than laws, as they afford more control and flexibility. Voluntary standards and seals further provide good publicity and marketing, which is associated with heightened media and consumer recognition and trust. It can also add legitimacy to smaller players who will benefit from the association with a well-acknowledged brand like BBB Online,[160] the Internet equivalent of the well-known Better Business Bureau, membership in whom lends credence to businesses.

From the government's perspective, implementing a standard may be faster and more cost-effective than drafting and enacting a law, thereby enabling the standard to respond to the dynamic field of e-commerce.[161] Moreover, it would be quicker to implement standards across many countries at once than to negotiate an international treaty. Internationally recognized standards can circumvent many trans-border issues, while simultaneously raising expectations for acceptable conduct by online businesses that sell to and from Canada.[162]

C. Legislating the Wild Wild Web

Since the market and self-regulation alone are not sufficient, businesses and consumers require government intervention for guidance and solutions. There are several key benefits of legislation. Primarily, it will prevent a lock-in of poor privacy standards, such as in the present situation. In addition, government regulation can constitute a necessary floor of preconditions for effective market and self-regulatory contributions to privacy protection.[163] For example, it was found that 51% of 300 Canadian leading Web sites did not post

---

[160] *Id.*
[161] *Id.*
[162] *Id.*
[163] *Why Legislation Instead of Self-Regulation?* RETAIL COUNCIL OF CANADA'S INSTORE NEWS VOL.2, ISS.3. (on file with author).

a privacy policy online.[164] With legislation requiring them to do so, companies would have a legal obligation to provide notice to and receive consent from their customers about any collection of customer data.

Further, privacy legislation will facilitate trade with countries with stronger privacy legislation in place. It is noteworthy that Canadian Industry Minister John Manley tabled the Personal Information Protection and Electronic Documents Act (PIPEDA) on October 1, 1998, just prior to the Organization for Economic Co-Operation and Development (OECD) summit meeting.[165] This was also merely a month before a European Union (EU) privacy directive came into effect that banned data transfers to non-EU countries that did not have adequate and enforceable privacy protection.[166] It is estimated that if privacy and other conditions for e-commerce are improved, e-retailers could add another CDN$156 billion to the Canadian economy by 2003, underscoring the impact consumer privacy concerns has on decreasing business revenues.[167]

From the consumer perspective, laws have the advantages of certainty and the force of the state behind them. Most customers would prefer to have privacy legislation, as it would impose penalties for violations of their customers' privacy or provision of poor service. Relevant areas of legislation would include contract formation, contract cancellation rights, and misrepresentation and fraud.[168] For instance, PIPEDA includes provisions about the collection, disclosure and use of information, and discusses issues of consent and access, remedies, the investigatory capacity of the Privacy Commissioner to perform audits, as well as the obligations of organizations in establishing procedures for the collection of information.

---

[164] *Id*.
[165] *Id*.
[166] *Id.*
[167] MCCHESNEY, *supra* note 153.
[168] *Id*.

However, even with legislation in place, the pursuit of small complaints regarding online sellers may not be a priority activity for regulators and it may not be worthwhile for consumers personally to pursue a minor legal dispute with a large online business. Moreover, it would be extremely difficult to implement a network of effective laws to cover global Internet transactions.

Businesses naturally prefer voluntary standards or self-regulation to legislation. The latter would bring an end to the practice of compiling consumer profiles without their knowledge and without compensating them, while reaping the rewards that personalization and marketing revenues bring. Further, legislation would restrict their freedom to pursue and develop innovative business models and impair their ability to do as they wish with consumer data. Finally, government regulations might unduly burden smaller companies who cannot afford the legal expenses of complying with law. For instance, a New York law firm estimates that costs of legal compliance could be as much as US$290,000 per year for the average business.[169] In fact, some big businesses may actually prefer laws to standards in order to maintain their competitive advantage over smaller players as well as to curb unscrupulous retailers who would ruin the image and reputation of e-commerce. For instance, boo.com's transgressions have given online businesses in general a bad reputation. Highly publicized stories such as this have had a chilling effect on consumer shopping online, fuelling their fears of privacy invasions.

D. The Technological Arms Race

A new industry of technological products to prevent privacy invasions has burgeoned in response to publicity about the lack of online privacy. There are different categories of solutions, ranging from more complex hardware structures such as the Public Key Infrastructure (PKI) which are based on encryption,

[169] Keith Perine, The Persuader, The Standard, Nov. 6, 2000, *at* http://www.thestandard.com/article/0.1902,19875,00.html (last visited Mar. 27, 2002).

and firewalls[170] to proxies (e.g., Anonymizer[171]) and software (e.g., Cookie Crusher[172]).

However, as has been noted by various industry watchers, these technological advancements are also improving corporations' abilities to track and circumvent the very tools that were created to protect consumer privacy in the first place. Companies like Global Track, a supplier of targeted advertising, are circumventing cookie disablers like the option in Netscape Communicator to reject third party advertiser cookies (e.g., which only accepts cookies that are returned to the domain that the user is currently logged onto). Global Track has set up forwarding domains, enabling the profiling cookie to look like it comes from the primary site instead of the third party site, tricking the user's server.[173]

As aptly noted by Jerry Kang, investing in these products merely leads to an arms race between parties to see who can come up with the best solution or loophole in these solutions.[174] The winner will be the party with the deepest pockets, inevitably benefiting the large corporations in the end.

E. Cyber-ducation

Finally, another alternative which ought to be used to supplement any of the aforementioned solutions is to educate consumers about what online businesses do, or may do, with their information. Education should incorporate the fact that publicly available information from government registries and

---

[170] Available in software version like Norton's Personal Firewall 2000.

[171] Free proxies can be downloaded from http://www.anonymizer.com

[172] Advisor software programs can be downloaded free from http://www.enonymous.com which also rates the stated policies of 30,000 web sites. See http://privacy.net/software to learn more about other software programs that delete cookies. See http://www.junkbusters.com, http://www.epic.org, and http://www.cookiecentral.com to learn more about disabling cookies

[173] For instance, when you go to Dejanews site, you are set a cookie that is allocated with a unique ID number which is used for user profiling by third party Global Track from a third domain called gtp.globaltrack.com. Now, to foil Netscape's third party cookie rejector, it is now set from gtp.dejanews.com through a forwarding option and accepted by your browser so this Netscape tool is now useless. Source: http://www.cookiecentral.com/content.phtml?area=2&id=2

[174] Kang, *supra* note 37.

telephone directories is and will be merged with the anonymous data, to the collection of which they may have consented. As discovered in the aforementioned surveys, Internet users know surprisingly little about Internet technology. Thus, they should be informed of basic technology concepts like cookies, basic technological solutions like changing the default on their browsers to opt out of cookies, and software that helps to reduce the privacy invasions that occur online. While education may have a chilling effect on online behavior, the decrease in privacy invasions would arguably outweigh any repercussions from the decrease in Internet participation.

Employing tort language, one can assert that there ought to be a necessary threshold of reasonable consumer behavior, a type of duty to mitigate losses, should litigation be pursued. In fact, section 3 of the PIPEDA provides that the Act governs the exchange of information for "purposes that a reasonable person would consider appropriate in the circumstances".[175] In other words, defendant companies may counter that the use or collection of information was reasonably expected and thus ought to be permitted. Should this happen, the consumer should at least be equipped with some basic knowledge of what she is participating in as well as of the consequences of not opting out.

VII. GOVERNING CANADIAN CYBERSPACE

The preceding sections have demonstrated how the absence of legislation has created a landscape in which privacy infractions are rampant. It is often thought that consumers have a choice in their interactions with businesses because of the diversity of products and services in the marketplace. However, information privacy committees and initiatives have found that individual consumers are tremendously disadvantaged compared to the organizations with whom they do business, due to the asymmetries of information, preferences and

[175] Personal Information Protection and Electronic Documents Act, S.C. 2000, ch.5, §3 (Can.).

bargaining power that exists between them.[176] The disparity of bargaining power and lack of consumer knowledge is particularly salient with respect to the consumer's ability to obtain information about the organization's business practices, how their personal information may be used, and how they may challenge any unfair information practices of an organization. As a result, individuals end up giving up more of their personal information than desired or than they realize in exchange for goods and services.[177]

The information asymmetry that exists between uninformed consumers and the organizations that collect their data mandates the enactment of legislation entrenching consumers' rights to informed consent. Laws stipulating informed consent and, more specifically, opt-in consent, for the collection, use and dissemination of personal information are necessary to provide consumers with choice and the tools with which to make their decisions. However, the drafting of legislation is itself wrought with difficulty, including the risk of being overly or under-inclusive. The recently enacted Canadian privacy legislation, PIPEDA, is already facing interpretation problems.

After years of supporting industry self-regulation, the American government, following last year's FTC recommendation, will be passing new laws to protect consumer privacy online.[178] As the Bush administration prepares to draft policies on technology-related issues, including Internet privacy, in the upcoming months after the legislature's August recess,[179] the current outstanding issues in the Canadian

---

[176] *Special Committee on Information Privacy in the Private Sector Report*. 4th Sess., 36th Parl., Legislative Assembly of British Columbia (2001), *available at* http://www.legis.gov.bc.ca/cmt/36th parl/previouscmts/priv_ps/Reports/report010320.htm

[177] *Id*.

[178] *Bush High-Tech Policy Coming Soon, Official Says, at* http://www.privacy2000.org/archived_headlines/index_2001.09.shtml (last visited Mar. 27, 2002).

[179] Brian Krebs, *Bush Administration To Target Privacy, Spam & 3G*, NEWSBYTES, Sept. 5, 2001, *at* http://www.newsbytes.com/news/01/169780.html (last visited Mar. 27, 2002).

PIPEDA may prove instructive. Further, American businesses online may wish to comply with Canadian legislation in order to diminish their Canadian clientele's fears of privacy infractions while simultaneously establishing goodwill with them.

A. Personal Information Protection and Electronic Documents Act

The Industry Minister introduced PIPEDA, known previously as Bill C-6, in October of 1998 in response to international privacy protection and to improve the Canadian e-commerce landscape.[180] With the surge in privacy violations, it was clear that cyberspace could not be self-regulated. Realizing the dire economic repercussions for e-commerce should consumer fears and distrust continue to escalate, the Canadian government decided to implement federal privacy legislation, six years after the Quebec provincial government enacted theirs.[181]

PIPEDA is scheduled to come into effect in three stages. Beginning January 1, 2001, it is only applicable to federally regulated companies such as banks, phone and cable companies, and most transportation companies. This deadline also applies to those companies who disclose personal data for consideration across provincial or international borders. Next, in January 1, 2002, those organizations that collect personal health data in the private sector in course of commercial activity (e.g., pharmaceutical companies that would have otherwise been caught by Stage One) will have to be PIPEDA-compliant. Finally, by January 1, 2004, where each local provincial government has not yet enacted "substantially similar legislation", the Act will apply to collection, use and

[180] Most notable of which is the European Union's *Data Protection Directive* (on the protection of individuals with regard to the processing of personal data and on the free movement of such data), 95/46/EC, 1995.

[181] For general information on Canadian constitutional law, see PETER W. HOGG, CONSTITUTIONAL LAW OF CANADA, LOOSELEAF (1997); P. MACKLEM ET AL., CANADIAN CONSTITUTIONAL LAW (2d ed. 1997*)*; DAVID BEATTY, CONSTITUTIONAL LAW IN THEORY AND PRACTICE (1995).

disclosure of personal information in a commercial setting in that province.[182]

B. Purpose and Principles

The stated purpose of the Act is "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions."[183] It is noteworthy that PIPEDA encompasses more general e-commerce legislation pertaining to issues that are beyond the scope of this paper, thus, the focus of this analysis will only pertain to Part 1 of the Act, which concerns the *Protection of Personal Information in the Private Sector*.

The purpose of Part 1 is to establish "rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a *reasonable person* would consider appropriate in the circumstances."[184] Bruce Philips, the previous Privacy Commissioner of Canada, attempted to describe this "reasonable person":

> "In a sense, I hope to function as a surrogate for that "reasonable person". A reasonable person will not take every business to task for collecting personal information. A reasonable person will welcome the collection of personal information in *some* situations, since it will serve the person in his or her dealings with that business. However, a reasonable person will challenge the excessive and persistent collection of information about them, the indiscriminate or

---

[182] Personal Information Protection and Electronic Documents Act, *supra* note 175 and http://strategis.ic.gc.ca/SSG/ca01458e.html (last visited May 6, 2002).

[183] *Id*.

[184] *Id.* at §3 (emphasis added).

> careless sharing of that information with others and the shrouding of that information-handling process in secrecy."[185]

While this general description is certainly what most people would agree to be fair and appropriate, actually determining what the "some situations" would be in which the collection of information is appropriate is much more difficult in practice. As discussed earlier, some Internet users consider it reasonable to be paid for surfing the Web while marketers collect their clickstream activity. Similarly, others find it reasonable to get a discount in exchange for disclosing certain preferences to their retailers. On the other hand, there are still others who would abhor such surveillance or dissemination of personal information.

It would not be a simple task to identify what purposes may be seen as reasonable, as the reasonable person standard in this contentious issue appears to be fairly divergent depending upon the population surveyed. Hence, this is where the "Identifying Purpose" principle, discussed below, which would require that organizations explain the purposes for which the information is being collected, will be of assistance.

The central premise of this section is to ensure that consumers are accurately informed about their information collection practices. This purpose, set out in section 3 and repeated in subsection 5(3), shows that PIPEDA was expressly enacted to protect the interests of both businesses and consumers by balancing the rights of each in order to improve the current e-commerce landscape in Canada. These provisions act as a substantive restriction that is not found in the original Canadian Standards Association (CSA)[186] Code by stipulating

---

[185] Bruce Phillips, *The Privacy Commissioner of Canada's approach to implementing the Act*, *Speaking Notes prepared for the CENTRUM Conference* (Dec. 10, 1999) *at* http://www.privcom.gc.ca/speech/archive/02_05_a_991210_e.asp (last visited Mar. 27,2002) (emphasis added).

[186] The Canadian Standard Association is a not-for profit, membership-based association that develops standards to serve the needs of businesses, industry, governments and consumers both in Canada and worldwide. CSA acts as a neutral third party in providing a structure and forum for developing standards. A standard is only

that data may not be collected for purposes that are inappropriate in the context at hand.[187]

Part 1 and Schedule 1 of the Act are based on the 10 principles of the CSA Model Code for the Protection of Personal Information (CSA Standards).[188] The CSA Standards were initially intended to be voluntary, demonstrating the Canadian government's intention to rely on private sector and self-governance mechanisms.

C. Definitions and Interpretation

There are two things of paramount importance that determine whether or not the action of an organization falls within the ambit of the Act. The two key terms are "personal information" and "commercial act." The manner in which these two terms are defined and interpreted is crucial to ascertaining whether PIPEDA would govern a specific practice. Different interpretations of these fundamental terms leads to further difficulty in achieving the overall goal of fully informed consumer content.

1. Personal Information

"Personal information" is characterized by several attributes that warrant acknowledgement. First of all, personal information does not necessarily have to be sensitive, private or confidential information.[189] Instead, it is defined as: "information *about* an *identifiable* individual, but does not

---

developed when there is substantial agreement, and not a simple majority, among its committee members. *See* http://www.csa.ca/ (last visited Mar. 27, 2002); http://www.csa.ca/faq/ (last visited Mar. 27, 2002).

[187] David M.W.Young, *Canada's New Information Privacy Law – Bill C-6: An Overview*. PRIVACY: BOURGEOIS FIXATION, COMMERCIAL CONCERN OR LEGAL RIGHT? CANADIAN BAR ASSOCIATION – ONTARIO 2000 INSTITUTE OF CONTINUING LEGAL EDUCATION, Jan. 28, 2000 (on file with author).

[188] *Id*.

[189] Barry B. Sookman, *Privacy in Canada: Putting the Code into Practice and Security of Information Issues*. PRIVACY: BOURGEOIS FIXATION, COMMERCIAL CONCERN OR LEGAL RIGHT? CANADIAN BAR ASSOCIATION – ONTARIO 2000 INSTITUTE OF CONTINUING LEGAL EDUCATION, Jan. 28, 2000 (on file with author).

include the name, title or business address or telephone number of an employee of an organization."[190]

(a) "About"

It is crucial to recognize that the definition of personal information is not only limited to information that may directly or indirectly identify an individual. Instead, it is defined as "information *about* an identifiable individual." This could include information that exists in a non-identifying form for market analysis purposes since the definition is not limited to information about a person from which that person can be identified.[191] The ordinary use of "about" means "concerning, regarding, pertaining to or in relation to an identifiable individual." If this definition is employed, just about any bit of information would qualify as personal information if it pertains to an identifiable individual.[192]

In cyberspace, asserts Barry Sookman, this would apply to clickstream data, cookies, web pages visited and other such data even if this information cannot directly identify the particular user, since it could be linked to other pieces of information to *indirectly* identify an individual. In other words, the broad interpretation of 'about' would include numerous pieces of data that would appear to be anonymous on their own, but may be compiled with other anonymous data to indirectly identify a person. This interpretation addresses the "synergistic effects" of privacy, a concept later discussed in subsection (b)(ii), *infra*. Synergistic threats to privacy refer to a situation in which non-identifiable pieces of data are merged with other non-identifiable data to yield an identifiable profile.

However, if this interpretation is correct, and accepted by the judiciary, the definition of personal information could be potentially rather broad, meaning that everything may be classified as personal information and would thus require consent before collection.

---

[190] Personal Information and Electronic Documents Protection Act, *supra* note 175 at §2 (emphasis added).

[191] Franklin, *supra* note 122.

[192] *Id*.

(b) "Identifiable"

It is unclear why Parliament chose to use a relatively vague[193] word like "identifiable" in its definition of "personal information," as opposed to a more comprehensive listing like in the federal Privacy Act[194] which governs governmental collection of data about private citizens. The Privacy Act outlines a list of information that would fall in that category like race, age, marital status, education, blood type, personal opinions, etc. The Privacy Act goes on to state that the list is not exhaustive by adding the phrase: "without restricting the generality of the foregoing."

If the legislature had been concerned with limiting the scope of personal information by providing a list, it could very well have employed the conventional "without restricting the generality of the foregoing" phrase and by expressly asserting that other categories not included could still be deemed "personal information." Perhaps the failure to take this approach is due to the worry that despite the inclusion of such phrases, the courts might still hesitate to include non-enumerated categories of information. This reluctance has been exhibited in income tax litigation where there has been a judicial reluctance to include non-specified sources of income even though section 3(a) of the Income Tax Act, which defines income, uses that phrase. By defining "personal information" broadly, it is possible that Parliament sought to afford individual consumers the largest scope of protection possible and to empower the judiciary to interpret each situation on a case by case basis. This type of definition would also limit the court's potential to fall prey to the interpretive doctrine of strict construction.[195] whereby the statute is interpreted literally, to the exclusion of other possibilities. This may be especially prudent in a dynamic industry governed by continuously

[193] Vagueness is problematic since it is imperative that there be clear boundaries to which the Act applies to ensure compliance.

[194] Privacy Act, R.S.C., § P-21 (1985) (Can.).

[195] *Supra* note 183.

changing technology which may alter what would be deemed 'identifiable' with every innovation.

This vague definition presents problems for businesses, since it is not entirely clear from the outset where the line will be drawn in interpreting the word "identifiable". The Webster's dictionary definition of the verb 'identify' refers to the determination and/or recognition of a particular person.[196] Similarly, 'identity' is a condition or fact of being a certain person and is recognizable as such. Thus, it would be natural to conclude that if the data cannot be traced back to a particular individual, it is probably exempt,[197] although the challenge arises in determining the threshold of traceability.

For obvious categories of information such as one's name and address, these definitions do not pose a problem, as they would easily fall under the purview of the Act. On the other hand, it is not always simple to distinguish between anonymous (i.e., data that cannot be manipulated or linked to identify an individual) and identifiable data, as will be demonstrated below.

(i) Anonymity is in the eye of the beholder

As Latanya Sweeney puts it, "anonymity is in the eye of the beholder." [198] The organization collecting the data often does not know the identity of the ultimate viewer of the data and the knowledge she possesses to interpret the data. The following example shows just how difficult it is to reach any consensus regarding traceability of data.

Using the 1997 voter list from Cambridge, Massachusetts, Sweeney illustrates how seemingly anonymous data can yield quite identifiable information. By using just the birthdates of 54,805 listed voters, one can identify the name and address of

---

[196] The New Lexicon Webster's Encyclopedic Dictionary of the English Language, Canadian Edition. Lexicon Publications Inc., New York, 1998.

[197] Michael Geist, *Privacy Compliance is the New Priority*, GLOBETECHNOLOGY, Nov. 10, 2000, *at* http://www.globetechnology.com/archive/20001110/ECGEIS.html (last visited Mar. 27, 2002)

[198] Latanya Sweeney, *Weaving Technology and Policy together to Maintain Confidentiality*, 25 JOURNAL OF LAW, MEDICINE & ETHICS 98, 100 (1997).

12% of the voters by linking them to publicly available census data of voter lists.[199] This percentage increases further when more factors are included: adding birth date and gender identifies 29%, birthdate and 5-digit ZIP code identifies 69%, and birth date and full postal code identifies 97% of the voter population.[200] This case study demonstrates how isolated pieces of anonymous data can be easily linked with other pieces of anonymous information to yield very identifiable profiles. Sweeney's illustration also reveals how the concept of anonymity lies on a spectrum, differing according to who applies the standard.

Since PIPEDA specifically excludes publicly available information[201] like that found in telephone directories, census databases, drivers' licenses, credit history registries, court records, subscriptions,commercial mailing lists and other published information, the Sweeney exercise might easily be duplicated in Canada. While a user of an adult Web site may not mind disclosing his sexual practices and preferences anonymously by providing only his age and occupation, a fully comprehensive profile can easily be attained by amalgamating the information found from publicly available databases and other anonymous information. It is noteworthy that Principle 4.3 in Schedule 1 of the Act acknowledges that organizations that do not have a direct relationship with the individual may not always be able to seek consent from them. Hence, the organization providing the information is expected to obtain consent before disclosing the information to a third party.

---

[199] *Id.*

[200] *Id.*

[201] In its broadest sense, 'publicly available information' includes all information that has entered the public realm by any means whatsoever, although the parameters of this concept that is used in federal statutes such as the Access to Information Act (AIA) and Privacy Act have been subject to considerable debate in Canada. Case law interpreting the AIA suggests that the test determining when a piece of information ceases to be private is an objective one. *See* Rick Shields, *Publicly Available Personal Information and Canada's Personal Information Protection and Electronic Documents Act*, (Oct. 12, 2000) *available at* http://www.e-com.ic.gc.ca/English/privacy/doc/regs_doc.pdf (last visited Mar. 27, 2002).

The organization providing the list, here, the adult Web site, would be expected to obtain the user's consent. The adult Web site would not, however, have a legal obligation to seek the user's consent to sell aggregate data to a third party, since the description of "a male financial analyst between the age of 30-40" is arguably not identifiable information. Of course, the third party, unbeknownst to the adult Web site, could very well have purchased several other anonymous aggregate lists in which this customer was also included. By combining these lists through data mining, the third party could easily yield a complete profile of this user as John Smith of 111 ABC Street, a 32-year-old Bay Street analyst at Bank X, who happens to purchase sex toys. This hypothetical illustrates the loopholes that exist under the Act and questions the sufficiency and scope of its protection. On the other hand, it may be administratively impossible for the Act to explicitly contemplate each and every situation, especially when considering the interests of both the organization and the individual.

The fact that John Smith's profile could be created easily even though he may have fairly ordinary attributes illustrates how bits of irregular data can be identifiable. Sweeney maintains that the aggregation of anonymous information creates more possibilities for the identification of unique and unusual information than the actual data.[202] Hence, while we do not usually consider gender to be identifiable information, this may be a distinguishing trait depending upon the population being surveyed. For example, the female students enrolled in a male-dominated mechanical engineering program would be easily identifiable if they were to participate in an anonymous survey on how alcohol consumption differs by gender and field of study. The researchers' good faith intentions to maintain the participants' confidentiality may very well lead to lack of anonymity and detrimental invasions of privacy should these results be published.

---

[202] *See Generally,* Sweeny, *supra* note 195.

(ii) Synergistic threats to privacy

The ease with which any of the aforementioned examples could materialize raises questions about whether the Act will provide sufficient protection for the privacy of individuals. PIPEDA does not explicitly contemplate the aggregation of disparate, isolated bits of data and the possible repercussions that would result from the conglomeration of the information. The merger of DoubleClick and Abacus all too well illustrates just how simple it may be to circumvent the legislative requirement of mandatory consent. More specifically, while DoubleClick may not harbor any personally identifiable data about its users, the amalgamation of such data with data in Abacus about the same consumers would very quickly yield identifiable profiles.

Perhaps the Act should address what Jerry Kang calls the "synergistic threat to privacy."[203] Consider the situation where a person consents to have his grocery purchases monitored by Company A, and his reading material purchases monitored, perhaps under an alias, by Company B, but not both to either one. Does it matter then, that through consumer data exchanges or the use of publicly available records, these different pieces of information end up being linked to create a detailed sketch of this individual? Is his consent now still valid upon the aggregation of disparate bits of information? Through the profiling, is his privacy further and more greatly infringed upon? Is the whole really greater than the sum of its parts?

Jerry Kang believes that there is a qualitative shift when individual bits of data are compiled into profiles, a synergistic threat, since the privacy threat of the profile is greater than the sum of the privacy threats associated with each individual bit of information considered in isolation."[204] In the example given above, Rob may have consented to having grocerygateway.com track his weekly groceries in order to receive a discount. Grocerygateway.com then sells Rob's data to a company like Acxiom Corp., which links his shopping lists to his URL,

[203] Kang, *supra* note 37, at 1240.
[204] *Id*.

derived from the cookies planted from grocerygateway.com. The URL could provide further information as to Rob's user ID, e-mail addresses, ISP and other organizations to which he is linked. Then, as demonstrated in the *McVeigh* case, Acxiom can determine his real identity, if not otherwise found in his e-mail address (which may already be in the form "first name.last name"). His name can then be linked to publicly available data, easily purchased from census bureaus or charitable organizations or found in motor vehicle registries or telephone directories. Hence, Rob's fear of people finding out that he is an avid reader of Salman Rushdie's SATANIC VERSES could easily materialize. This aggregation of information would have the effect of profoundly exposing unsuspecting consumers who would never have imagined that the process of amalgamating isolated, disparate pieces of data from several different parties could be undertaken so easily.

The idea of synergistic effects on privacy was recognized in a 1989 American case involving the Reporters Commission, which was charged with attempting to access an ex-criminal's FBI rap sheet from various jurisdictions.[205] The court held that that there was a privacy interest in the compilation of public records, since the public record of each infraction was in individual jurisdictions. The fact that it was a compilation of individual records made it an "unwarranted invasion of individual privacy" because the aggregated data was more of a persona of the individual than the result of the government's information-collection activities.[206] This decision thus lends credence to Kang's notion that the whole may really be greater than the sum of its parts.

(iii)PIPEDA and aggregated data

Employing a purposive approach, it is prudent to recall that the purpose of Part 1 and of the Act in general is to ensure that individuals' rights to privacy are balanced against the rights

---

[205] United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989) .

[206] *Id.*

of organizations to collect and use the personal information in a manner that people would deem reasonable in the circumstances. Strictly speaking, from the words of the Act, John Smith and the female engineering students would probably not have recourse under PIPEDA. It certainly is reasonable to think that "a male financial analyst between the ages of 30-40" and gender does not fall under "identifiable information." In John Smith's situation, this is especially relevant since the named characteristics in the aggregate data are from a population in a large city like Toronto, which also happens to be a financial district. Further, most reasonable people would consider it appropriate to sell aggregate anonymous data to others since, after all, the information is presumed to be anonymous. However, if the above profiles were actually produced and published, there would undoubtedly be public and moral outrage. John Smith's and the students' ability to control with whom they wish to share certain parts of themselves ("privacy as control") would be diminished, as well as their interpersonal relations ("privacy as a relational interest"). Surely Parliament would not have intended such an egregious consequence in plain violation of an individual's privacy interest.

On the other hand, if one were to include every potential piece of information under the rubric of "personally identifiable," it would be administratively impossible for organizations to operate their businesses and would completely hinder the collection and use of much desired information. Further, even if it were feasible to seek consent for every bit of information, it is doubtful that consumers would ever consent to any anonymous surveillance if organizations disclosed every possibility of profiling. This would naturally diminish the many benefits resulting from such collection. It is indeed difficult to account for all the possibilities by protecting the needs of both parties in a fair and equitable manner.

Perhaps the Act could incorporate a clause stipulating that the organization should inform consumers of any possibility, "to the best of its knowledge," of the aggregation of

information with information from other organizations, even if the present organization would only be disclosing anonymous data. [207] This would introduce the element of consent not only to collection but to aggregation of consumer data.

(c) "Recorded form"

Another noteworthy feature of how "personal information" is defined is the removal of the restriction that the information is "recorded in any form" from the draft versions of Bill C-54, Bill C-6's predecessor.[208] The absence of this qualifier makes the definition of personal information broader than in other pieces of legislation, such as the OECD Privacy Guidelines, the EU Data Protection Directive, and the Canadian Privacy Act. Conceivably, the lack of having a recorded form of the information could mean that information transmitted orally may also be caught in PIPEDA's ambit. This would mean that PIPEDA could possibly govern oral conversations between sales staff and customers. It is unclear, however, if such an issue would even surface in practice.

2. Commercial activity

"Commercial activity" is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."[209] According to the dictionary, "commercial" means that something has the characteristics of commerce, which is the interchange of goods, or that something is done for profit.[210] Since donor information from non-profit organizations would be included if these charitable organizations are engaged in "commercial activities," this may confuse non-profit

[207] As opposed to merely leaving it as interpretive issue where courts are left to read this in, affording broader protection to consumers as well as ensuring that consumers are informed of the uses their information may be put.

[208] YOUNG, *supra* note 188.

[209] Section 2(1).

[210] WEBSTER'S, *supra* note 198.

organizations who do not realize that the Act also applies to them.

The preceding interpretation would be the narrower of the two potential interpretations of the word "commercial," where an explicit exchange or *quid pro quo* transpires. The other construction of "commercial nature" would encompass actions with the intention or a reasonable possibility of purchase or exchange, or what a reasonable person would construe as being of a "commercial nature." However, both interpretations may still be inadequate to fully protect the privacy interests of Netizens. In addition, there may be certain areas of an organization's activities that may be non-commercial and it is unclear whether these activities would be covered by the Act.

Employing the narrow definition, information collected in commercial transactions would begin with data generated in the actual transaction. In a brick-and-mortar store, this would occur when a customer pays for her purchases at the cash register. Employing the same analogy in the cyber-world, the commercial transaction begins when the customer enters the billing information (e.g., customer name, address, credit card number and purchases), and not when goods are placed into the virtual shopping cart since the cart can easily be abandoned, aborting the transaction.

Using this interpretation, browsing activity or Web personalization/customization before purchasing would not be caught since it does not *yet* have a commercial character, i.e., no exchange or profit made yet. It follows, then, that the surfing habits of Internet users who do not actually purchase anything on the Net would not be included here, as it is difficult to conceive of what profit or exchange of goods is made by these browsers. Once again, the brick-and-mortar analogy can be employed. Window shopping and even trying clothing on at a store would not constitute a commercial transaction since there is no consideration given, thus no exchange and certainly no profit. Even where profit is interpreted as the psychic benefit the consumer receives from trying on an outfit or by seeing aesthetically pleasing things, there is still no exchange here

unless the consumer agrees to have her actions monitored in exchange for looking at the goods. However, it is unlikely that the legislature intended for the word "commercial" to mean non-tangible exchanges. This meaning would only lead to a slippery slope where gratitude could arguably be deemed a fungible item of exchange, rendering every possible interaction to be of "commercial nature."

On the other hand, if the broader interpretation of "commercial activity" was adopted, it would cover the surfing consumer who abandons her shopping cart, since it could easily be argued that she had the intent to purchase. However, the Act would still not be applicable to Netizens using Web sites for research purposes without any commercial intent. Government, academic and other non-commercial (as in non-business) Web sites have been known to plant cookies on a surfer's computer without informing the user of such actions. As discussed earlier, the clickstreams and responses of Netizens to ads or Web sites constitute very valuable information for marketers and organizations. However, given the "commercial" requirement, this type of activity may not be protected under PIPEDA, which would do little to dispel consumer fears, contravening the stated goals and purposes of the Act.

D. Application of the Act

Part 1 of PIPEDA applies to

> "every organization in respect of *personal information* that (a) the organization collects, uses or discloses in the use of *commercial activities*; or
>
> (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."[211]

It should also be noted that the Act does not apply to government institutions to which the Privacy Act applies,

[211] All emphasis the author's.

individuals collecting, using, or disclosing personal information *solely* for "personal or domestic purpose," and organizations collecting, using or disclosing personal information *solely* for "journalistic, artistic or literary purposes." Hence, the Act only applies to private sector corporations that are not collecting, using, or disclosing personal information for activities which are not artistic or personal, etc., in nature.

1. Personal or domestic purposes

It is unclear what "personal or domestic purposes" includes. Most likely, the people employing UNIX to spy on their fellow Netizens would be exempt, unless they are collecting data to be sold at a later date. The collection of the data would not be covered under PIPEDA, but the selling of the information to others would be. The thought of these compilations and profiles lying around the homes of these UNIX users is rather disconcerting. The discomfort is further amplified when one considers the endless possibilities of UNIX users disseminating this information to organizations *ostensibly* without remuneration in order to circumvent the commercial aspect of the dissemination, thereby qualifying for exemption under the Act.

Hypothetically speaking, what if these UNIX spies collect this information for blackmail purposes? Would the individual whose privacy was violated then only have recourse through criminal or tortious remedies as per Prosser? Recourse through criminal law may take place through the crimes of extortion or possibly criminal harassment, although it is uncertain whether watching another's clicktrails would be tantamount to stalking. It is noteworthy that under the criminal law route, the action would have to meet a higher standard of certainty, the "beyond a reasonable doubt" standard, as opposed to a "more probable than not" civil standard of proof. Thus, recourse through criminal law renders it more difficult for the victimized parties to protect their privacy or to receive any monetary damages.

Further, under Prosser's four torts,[212] the privacy rights protected would only extend to private or false facts, which would not apply to most regular surfing activities that users may not wish to share with the world at large. It may not even protect an unsuspecting, ordinary person who surprisingly finds a Web site devoted to her. If all the information on the site were comprised of non-private things such as her class pictures from kindergarten until graduation from university as well as her clickstreams or favorite sites, she would not have any redress, according to Prosser's formulation.[213] This is due to the fact that these pictures are arguably not private affairs, as they may have been published in a yearbook, nor are they embarrassing, put her in a false light, or would used to take advantage of her name. However, most ordinary people, stumbling upon such a discovery, would likely find this a little disturbing.

2. Artistic, journalistic or literary purposes

It is also not certain how broadly "artistic, journalistic or literary purposes" would be interpreted, making it difficult for the collector to know her obligations and the subject to know her rights. The exclusion of these categories means that these privacy stipulations would not apply to this information. Thus, consent need not be granted by the subjects of these publications, depending on the type of laws that apply in those fields. If no such legislation or standard exist, or if they are fairly lackadaisical, individual rights may be compromised. Further, this would enable organizations to use this published information to target subjects without having to compensate them for the costs of using their data. Finally, being the subject of an artistic, journalistic or literary endeavour that compromises one's privacy may not necessarily console the subject of such a work. If the woman who finds the Web site

---

[212] Prosser, *supra* note 21.

[213] It is noteworthy that Bill S-27 proposed by the Senate of Canada sought to establish an act to guarantee the human right to privacy. However, this Bill only passed the first reading in June 2000. Perhaps S-27 was intended to capture situations such as this. *See* Privacy Rights Charter, Bill S-27, 36th Parl. (2nd Sess. 2000) (Can.), *available at* http://www.parl.gc.ca (last visited Mar. 27, 2002).

devoted to her in the previous example has all the same information about her published or compiled in a book or magazine article, the fact that she was the subject of an artistic or journalistic work would not compensate for her loss of privacy. It is not clear why the weighing of an artistic, journalistic or literary purpose would necessarily win over the individual's rights to privacy. Perhaps such a purpose would "win" only according to the utilitarian conception, where the publication of such work may benefit more readers than it would the individual. However, since the underlying objective of the Act recognizes an individual's right to privacy and that of the organizations to collect and use information that a reasonable person would consider appropriate under the circumstances, the rationale for this exemption is not readily evident.

PIPEDA would also not apply to the collection, use or disclosure of personal information that occurs within that province where the provinces have enacted "substantially similar legislation."[214] Again, the legislature has chosen an ambiguous phrase without stating if there are minimum threshold requirements (e.g., opt-out requirements) that provincial laws have to meet, making it difficult for businesses to know if complying with their provincial legislation would be sufficient. This may also create differences between provinces, raising compliance issues for inter-provincial business activities.

It is noteworthy that there is no "grand-parenting" provision that exempts an organization from the application of the Act regarding the use or disclosure of information already in its possession.[215] As the law is not retroactive, companies do not need a consumer's consent to continue sending them ads that they are already receiving. However, if the organization starts to add or do something significantly different with the data, it will be unable to use or disclose any personal information that

---

[214] *Supra* note 184.

[215] John Beardwood, *Privacy Issues: An Overview* (unpublished manuscript produced for the First Annual IT Law Spring Training Program, April 27 – 29, 2000) (on file with author).

it already possesses, without the prior knowledge and consent of the individuals concerned. In other words, it would be legal for the organization to *have* the information because consent was not required when it was originally collected, but it would not be legal to make *use* of it or *disclose* it to anyone else without the customer's consent. For instance, the data may be stored in the corporation's database, but the corporation may neither make use of it through processing, marketing or analysis nor may it disclose the information to anyone else without the consumer's consent. This part of the Act will likely cause confusion amongst retailers who may not fully comprehend these complex legislative requirements.

E. Schedule 1: The CSA Principles

The CSA standards[216] were intended to be a voluntary code which member organizations could adopt or modify to suit their needs. In 1996, Canada became the first country to adopt a voluntary code as a national standard.[217] These ten principles (accountability, identified purposes, consent, limiting collection, limiting use/disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance) are now mandatory and set out in Schedule 1 of PIPEDA. Only the principles of purpose, consent, collection and administrative obligations will be discussed since they are relatively unclear and ambiguous. However, it should be noted that all the principles should be considered in conjunction with each other and not in isolation.

1. Principle 2 - Identified Purposes

There are no guidelines provided on how specific the identified purposes must be, although deceit may not be used to

[216] This privacy code is a voluntary national standard for the protection of personal information, with emphasis on the way organizations collect, use, disclose and protect personal information as well as the right of individuals to access their personal information. Canadian Standards Association, *Model for the Protection of Personal Information, available at* http://www.csa.ca (last visited Mar. 27, 2002). *See supra* text accompanying note 199.

[217] *See* Cha, *supra* note 113.

attain consent (as set out in Principle 4). For instance, it is not clear if stating that "we are collecting information so that we may market products that *may* be of interest to you" is sufficient, or if a more specific "we are collecting information so that we may market products of interest to you that you have specifically indicated the categories for" is required. If the former were adequate, retailers could determine through statistical and correlational analyses of one's demographics and previous purchases what one may also like, whereas if the latter were true, then vendors could only market items that consumers have specifically selected, e.g., for household items and mystery books.

Further, certain practices such as data mining will face particular difficulties in meeting the identified purposes requirement. The very nature of data mining is premised upon the discovery of unknown relationships and associations. Thus, the data miner will not know from the outset just what personal information will be of value and thereby used, or even what type of relationships will emerge.[218] This process of knowledge discovery cannot ensure that personal information will be used for limited, defined purposes as it lacks transparency, and does not provide consumers with the opportunity to access or request corrections to the personal information created through data mining.[219]

Hence, since data mining would constitute a secondary use, explicit consent would probably be required from the consumer. Furthermore, Ann Cavoukian, Ontario's Privacy Commissioner, suggests that simply adding the words "data mining" as the primary purpose at the time of data collection would not be sufficient to constitute meaningful data protection since it would be challenging to identify an unknown secondary use as a primary purpose.[220] This is especially true since it would not be reasonable to expect the average consumer to

---

[218] Cavoukian, *Data Mining,: Staking A Claim on Your Privacy*, Information and Privacy Commissioner/Ontario (Jan. 1998) *available at* http://www.ipc.on.ca/English/pubpres/papers/datamine.htm (last visited Mar. 28, 2002).

[219] Franklin, *supra* note 122.

[220] Cavoukian, *supra* note 211.

understand or fully appreciate the nature and the results of data mining. The problem raised by data mining lends further credence to the earlier assertion that fully informed consent is not easily obtained.

2. Principle 3 – Consent

Subject to certain specific exceptions, organizations must ensure the prior knowledge and obtain the consent of individuals. It is noted that organizations that do not have a direct relationship with the consumer are not expected to receive their consent, given the practical difficulties. Instead, it would be up to the initial collector to receive consent regarding further disclosure of the data to other organizations. However, this principle does not address the use of aggregate information since one single aggregator could be receiving information from three different sources. Although all of these sources could provide anonymous data, as illustrated earlier in this paper, mining techniques could easily enable the profiling of identifiable individuals. It may be possible to capture the aggregation of data under the term "collection," but as has been stated in the consent provision, these organizations would still not have a direct relationship with the individuals, thereby not requiring their consent. This would also not cover situations like the merger between DoubleClick and Abacus where anonymous data is linked to identifiable information. Such mergers present real danger in an industry increasingly dominated by a small number of players who will ultimately possess greater, merged databases.

(a) Informed consent

The consent principle stipulates that consent must be informed in that organizations are required to make "reasonable efforts" to identify the purposes for which personal information is acquired at the time of collection.[221] Moreover, in order for consent to be meaningful, the purposes must be stated in a manner in which a person can "reasonably

[221] PIPEDA , Schedule 1, Principles 4.3.1 and 4.3.2.

understand how the information will be used or disclosed". The phrase in quotations is problematic in an era where there are disparate levels of technological awareness in society, especially between generations and educational classes. For instance, one study found that 69% of Internet users have unknowingly signed up for e-mail distribution lists and more than 40% of users do not know or understand what cookies are or how they work.[222] Given this finding, how much knowledge should we assume consumers have? Should users be aware and understand that if they give one piece of information out, e.g., their e-mail address, it could be linked to public information from the phone book, motor vehicle sale registrations, driver's license, consumer warranties or subscription information? Should companies write up policies in a manner that a reasonable Generation X'er or a reasonable 65-year-old can understand?

Under the federal Privacy Act, the organization should assume no knowledge. It has been suggested that the PIPEDA be interpreted in the same way,[223] with organizations required to set out detailed explanations and seek explicit consent from the consumer for everything they propose to do with the data. While this would best protect the privacy interests of the consumer, the actual practice of administrating such a detailed document would be quite burdensome.

Similarly, how explicit do consent explanations have to be, given the disparities in technological aptitudes among different age and social groups? Further, the level of detail required to constitute "informed consent" is unclear. For instance, would it be sufficient to inform the consumer that her personal information may be disclosed to a third party who performs data mining or would the name of the third party be required? Whether consent for multiple purposes would be allowed is another uncertainty of the consent principle.

---

[222] Michael Pastore, *Privacy Issues Dividing Internet Customers*, CYBERATLAS (Apr. 24, 2000), *available at* http://cyberatlas.internet.com/markets/advertising/print/0,5941_346371,00.html (last visited Mar. 27, 2002).

[223] BEARDWOOD, *supra* note 217.

There is also the additional issue of changing privacy policies, such as those of DoubleClick's and Amazon's. DoubleClick suggests that its users review the privacy policy periodically as it "may update it from time to time." Would this constitute sufficient notification to its customers? Does that automatically mean that the customers, having accepted these possibilities of future changes, have consented to any, even possibly contentious, processes that DoubleClick may later choose to undertake? Surely, this would not constitute informed or legitimate consent since one would not know from the outset, at the time of consent, to what one is consenting.

(b) Sensitivity of information and reasonable expectations

This principle also notes that the nature of the consent required depends on the sensitivity of information and on the reasonable expectations of the individual, not the organization.[224] It states that any information can be sensitive, depending on context, and provides an excellent example of magazine subscription information that, while not ordinarily considered sensitive, it would be if it belonged to a special-interest magazine with stigma attached to it.[225]

It should be noted that the "reasonable expectations" of the individual would be influenced by the "identified purposes" and how they are explained to her. If the organization did not provide detailed explanations of the purposes, the understanding and expectations of the individuals would be more limited.. The words "reasonable expectation" create the presumption of an objective standard in the face of uncertainty in the application of the consent principle.[226]

(c) Limitations of consent

There are also limits attached to this principle; namely, an organization cannot require an individual to consent to the

[224] PIPEDA, Schedule 1, Principle 4.3.5.

[225] PIPEDA, Schedule 1, Principle 4.3.4.

[226] Robert Alilovic, *Express, Implied and Negative Option Consent: An Analysis of the Personal Information Protection and Electronic Documents Act*. (Nov. 20, 2000) (unpublished manuscript, on file with author).

collection, use or disclosure of information as a condition of supplying a product or service beyond what is required to fulfill explicitly specified and legitimate purposes.[227] It is unclear how this provision will be interpreted. As discussed in Part IV(C), I provided my personal information to a site whose registration page specifically claims that registration is required in exchange for free access to the content on the site.[228] The stated purpose of the collection of "unique identifiers", which "verify the user's identity", is to "expedite future login operations and for content reporting purposes."[229]

(d) Withdrawing consent[230]

Individuals may withdraw consent at any time and be subject to the resulting contractual and legal restrictions. This is a crucial provision of the Act, however, it may not always be possible to remove a particular individual's data. The data may have already been aggregated into a non-identifiable form or sold to a multitude of retailers who may have also disseminated it to multiple other companies, leading to a ripple effect where one piece of information may have conceivably been shared with an infinite number of organizations. It may be overly onerous to mandate this, as it would be an administrative nightmare for the first company to retract the individual's personal data. Moreover, it would be expensive for organizations to continuously update and maintain accurate lists of customer consents. On the other hand, if there are loopholes permitting the withdrawal of consent, companies will undoubtedly provide excuses to justify why the individual cannot withdraw his consent.

In addition, under the Act, individuals will be able to withdraw their consent completely, or withdraw their consent for use or disclosure for only *some* or particular purposes. For

---

[227] PIPEDA, Schedule 1, Principle 4.3.3.

[228] *Privacy Statement for www.MohanSawhney.com*, *available at* http://www.mohansawhney.com http://www.mohansawhney.com/privacy.asp (last visited May 6, 2002).

[229] *Id.*

[230] PIPEDA, Schedule 1, Principle 4.3.8.

example, a customer may change her mind and withdraw her consent to three of five purposes to which she had previously consented. While this is a necessary component of affording the consumer full protection of her privacy rights, it will undoubtedly be administratively complex and difficult for the organizations to keep track of the customer's continuously changing consent.[231]

(e) Opt-in vs. Opt-out approaches

The consent principle states that in some cases, consent may be implied, which may take the form of a "negative option" (e.g., "check this box if you do *not* want us to give information to other organizations"). In other contexts, an express "yes" may be required. It is not an easy task to determine when an activity requires express or implied consent. As a general rule, express consent is not required if the information provided is required for the broader transaction, such as subscription services requesting address information.[232] The only clear stipulation for express consent is for sensitive information, although the 'sensitive' information is not defined.[233]

The nature of implicit consent is subject to two varying interpretations. The first would treat *not* opting out as explicitly opting in. This is based on the premise that if an individual is fully informed of the purposes for which her personal information would be used, and she does not opt-out or provides the information, this indicates express consent.[234] The second interpretation views the negative option method only as implicit consent, where the person implies his consent through a lack of action in checking off the box. There is some support

---

[231] John P. Beardwood, *Personal Information As An Asset: Consent Issues in the Corporate Context under the Personal Information Protection and Electronic Documents Act*, (Nov. 16, 2000) (unpublished manuscript, CBA-O Privacy Law Section Seminar #2, Privacy: Balancing Private Rights and Business Interests, on file with author).

[232] YOUNG, *supra* note 188.

[233] *Id.*

[234] *See, e.g.,* McCormick, *supra* note 149.

for the latter construction in the CSA Workbook, which provides guidelines for interpreting the principles.[235]

The problem with implicit consent is that it may not afford a broad enough protection to consumers, since the opt-out box or clause may be buried so deep that people do not even see it at all. It would thus be questionable whether implicit consent would constitute informed consent. BLACK'S LAW DICTIONARY defines informed consent as "a person's agreement to allow something to happen, made with full knowledge of the risks involved and the alternatives."[236] If an Internet user fails to notice the opt-out box, there would certainly not be any knowledge of the existence of the organization's intention to collect information, let alone any knowledge of the risks involved or the alternatives. Thus, the opt-out approach would clearly not meet the informed consent threshold.

Implicit consent would be less problematic if the legislation required the opt-out option and a full explanation of the repercussions of not opting out to be placed at the front or top of the page, as suggested by Ontario Privacy Commissioner Ann Cavoukian.[237] With notice, users would have greater opportunity to be made aware about the site's data collection practices, more closely resembling informed consent.

Further, as Paul Schwartz points out, people do not even read privacy statements. He maintains that some Web sites:

> contain consent boilerplates in their privacy statements that seek to create the legal fiction…. [and is] likely to turn into a hollow ritual. Individuals may not bother to read a given "informed consent" screen or know where to look for a "privacy statement" before they click through or "surf" deeper into a Web site. In addition, the language on a consent screen or "privacy statement" may approve any and all use

---

[235] YOUNG, *supra* note 188.

[236] BLACK'S LAW DICTIONARY 300 (7th ed. 1999)

[237] Ann Kerr, *Still grey areas in new privacy law*, GLOBE AND MAIL. Jun. 9, 2000, at E12.

> of an individual's personal information. Self-reliant consent cannot fulfill its assigned role if individuals are guided into making uninformed, non-voluntary exchanges.[238]

As a matter of policy, should the legislature be concerned about people clicking through their consent even though it is likely that they have not read or comprehended the policy? Or would this just be akin to a regular contract where parties sign without reading the entire contract?

In *Rudder v. Microsoft Corp.,*[239] the Ontario Superior Court held that a click-wrap online contract (a contract by which terms are assented to through clicking an "I Agree" button) was valid and not akin to "fine print," even if the plaintiffs could only read portions of the Agreement on the screen at a time. In *Rudder*, the court analogized this to a multi-page paper contract. Further, neither the form of this contract nor its manner of presentation was so aberrant so as to lead to an anomalous result and therefore, the click-wrap should be afforded the sanctity given to any agreement in writing. This judgment substantiates Part 2, § 20(1) of the Uniform Electronic Commerce Act (UECA) which provides that online consent is valid unless the parties agree otherwise, since an offer or acceptance thereof can be expressed in electronic form by clicking on an appropriate icon.[240] In essence, the UECA provides statutory acceptance of the principle that electronic documents are functionally equivalent to traditional written documents.[241]

---

[238] *Supra* note 2.

[239] [1999] O.J. No.3778 (Ont. Sup. Ct.), *in* Michael Geist, INTERNET LAW IN CANADA 558-60 (2000).

[240] Uniform Law Conference of Canada, *Uniform Electronic Commerce Act* (Jun. 1999), available at http://www.law.ualberta.ca (last visited Mar. 27, 2002).

[241] In order to ensure greater likelihood of the enforcement of webwrap and clickwrap contracts, it is recommended that there be: a prominent display/notice of its provisions, delivery of the agreement by e-mail or regular mail, use of a dialogue box to confirm that the purchaser first scrolls through the terms and conditions before agreeing, reference to the agreement in other related documentation, and providing the purchaser with the ability to reject the conditions and to terminate the transaction at any time. D.A. Dietrich, *Legal Issues Affecting Canadian Based Electronic Commerce Undertakings*

Rudder is consistent with other click-wrap cases in the United States which have also deemed such contracts to be valid and enforceable. The court in *In re RealNetworks, Inc.*,[242] dismissed the argument that electronic writings were not included in the plain and ordinary meaning of "writing" and maintained that the License Agreement was printable even if "print" and "save" buttons did not appear on the screen. Further, the allegation of procedural unconscionability was discounted because the provision at issue was not "buried" in the license agreement nor were the pop-up window and scroll-down contents so small as to be deemed unconscionable. Likewise, although it did not deal directly with the validity of clickwrap agreements, *Hotmail Corp. v. Van$ Money Pie, Inc.*[243] implied that the clickwrap agreement was an enforceable contract as there was no discussion as to the ineffectiveness of Hotmail's Service Agreement by virtue of it being of the clickwrap variety.

However, not all types of online contracts have been found to be valid. In *Specht v. Netscape Communications Corp.*,[244] website visitors could download SmartDownload software by clicking on a box on the introductory screen. The sole reference on the page to the license agreement appears in a text visible only if the user scrolls down through the page to the next screen. Visitors were not required to affirmatively assent to the license agreement or even to view the agreement before downloading the software, although if the license agreement link is clicked, there is a stipulation that the user read and agree to its terms before downloading the software.[245] The court held that downloading the software did not amount to the mutual assent required for contract formation. It was not an unambiguous

---

(1998) (unpublished manuscript, presented at the IT Industry Series on Intellectual Property Centre for Property Studies), *in* John P. Beardwood, *Issues in Electronic Contracting*, NET INCOME: HELPING CLIENTS DO BUSINESS ON THE INTERNET, CANADIAN BAR ASSOCIATION – ONTARIO 2000, INSTITUTE OF CONTINUING LEGAL EDUCATION, (2000).

[242] 2000 U.S. Dist. Lexis 6584 (N.D.III. May 11, 2000).

[243] 47 U.S.P.Q.2d 1020 (N.D.Cal.1998).

[244] 150 F.Supp. 2d 585 (S.D.N.Y. 2001).

[245] *Id.*

indication of assent as the "purpose of downloading is to obtain a product, not to assent to an agreement," especially one whose provisions and contractual nature are not obvious.[246] Further, the court found that the user downloading the software was not aware that she was entering into a contract since the software was available for free.

The court likened the SmartDownload license agreement to a 'browse-wrap' license,[247] such as that in *Pollstar v. Gigmania, Ltd*,[248] in contrast to the contentious 'shrink-wrap' license cases discussed below. In *Pollstar*, the plaintiff placed a notice in small gray text on a gray background with the full text of the license agreement on its web page. The user was not required to click on an icon or to view its terms to assent explicitly, as merely clicking on the notice links allegedly bound the user. The court noted that many web site visitors might not have been aware of the license agreement, although it did not explicitly declare whether such browse-wrap licenses were valid or enforceable.

The *Specht* court distinguished its case from the *ProCD, Inc. v. Zeidenberg*[249] shrink-wrap case because the latter required unambiguous affirmative actions to be performed in order to indicate assent. The court in *ProCD* found that the absence of contract terms was not material since there was a written notice on the boxes that the software came with restrictions in the enclosed license and because consumers were free to prevent the formation of the contract by returning the software. Moreover, computer shrink-wrap licenses were held to be enforceable and binding on their customers unless their terms were objectionable on contractual grounds, such as unconscionability.[250]

This line of reasoning was extended in *Hill v. Gateway 2000, Inc.*[251] in which the plaintiff customer purchased a computer by telephone. The court found that retention of the product for

---

[246] *Id*. at 595.
[247] *Id.* at 587-89.
[248] 170 F. Supp. 2d 974 (E.D. Cal. 2000).
[249] 86 F.3d 1447 (7th Cir. 1996).
[250] *Id.* at 1452-53.
[251] 105 F.3d 1147 (7th Cir.1997).

more than 30 days amounted to sufficient acceptance by conduct. The court in *M.A. Mortensen Co., Inc. v. Timberline Software Corp*[252] also followed suit.

In contrast, *Klocek v. Gateway, Inc.*[253] came to a different conclusion, viewing the consumer as the offeror and the vendor as the offeree who accepted the purchaser's offer by shipping the computer in response to the offer.[254] The court held that the vendor did not accept the license agreement as a condition of the purchaser's acceptance of the computer. Moreover, although the computer had been shipped with the terms attached, there had been no communication to the plaintiff any willingness to proceed without the plaintiff's agreement to the license terms.[255]

As is evident from the above summary of American case law, the validity of unconventional contracts remains somewhat contentious, although if *Rudder* sets a precedent for Canada, any opt-in click-wrap contract would likely be enforced. Would the absence of opt-out be treated the same way? Would the failure to opt out of website policies be as binding as a click-wrap contract, even if the policies are obscure or hidden and people do not see them? In other words, if a Net surfer does not check off the opt-out box, is he bound by his inaction? If so, PIPEDA in its current form would be inadequate since the lack of action (of opting out) may not have necessarily indicated consent and especially not informed consent, but only a lack of awareness, especially if it was placed in a clandestine location or in miniscule font.

Jerry Kang argues that a mandatory opt-in policy as a default rule would not only provide greater privacy protection,

---

[252] 140 Wash. 2d 568, (Wash. 2000).

[253] 104 F.Supp. 2d 1332, (D. Kan. 2000).

[254] *See also* Step-Saver Data Sys., Inc. v. Wyse Technology, Inc., 939 F.2d 91 (3d Cir. 1991) (holding that printed terms on the computer software package was not part of the agreement); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F.Supp.759 (D. Ariz.1993) (holding the license agreement shipped with the computer software was not part of the agreement); U.S. Surgical Corp. v. Orris, Inc., 5 F.Supp. 2d 1201 (D.Kan.1998) (holding that the single use restriction on a product package was held not to be a binding agreement).

[255] Klocek, 104 F.Supp. 2d 1332.

but would also make more economic sense.[256] Kang suggests that there are large transaction costs of negotiating explicit agreements between Internet users and Web site operators and as a result, individuals and information collectors do not generally negotiate but conclude privacy contracts before transacting in cyberspace.[257] Conventional law and economics scholars assert that society should pick the default rule that most parties would have agreed to had there been a costless opportunity to do so.[258] Naturally, this would be problematic given that businesses would prefer the opt-out rule while consumers would rather have the opt-in approach.

In evaluating both options, Kang concludes that the opt-out default rule would be overly onerous for the individual consumer to contract out of, since she would face substantial research costs to determine what information is collected and how it is being used.[259] She would also run into a collective action problem in which the retailer would likely not comply with her idiosyncratic request to purchase back her personal information, due to the high costs of administering an individually tailored program.[260] On the other hand, if the vendor values the individual's personal information more than she does, it will purchase her consent in the opt-in default rule situation. Contracting around this opt-in default would be easier since the information collector knows what is currently being done with the data. Further, there would be no collective action problem, since each individual would likely consider an individualized offer from the merchant to purchase personal information. There would also be no 'hold out problem' since one individual's refusal to sell personal information to the organization would not destroy the value of the data altogether.[261]

---

[256] Kang, *supra* note 37.
[257] *Id*.
[258] *Id.* at 1250-51.
[259] *Id*.
[260] *Id.*
[261] *Id.*

According to Kang's argument, from the economic and the consumer perspective, the opt-in approach would be the most advantageous. However, it could be argued that the opt-in approach is overly onerous for companies. PIPEDA seeks to simultaneously balance the interests of both businesses and private individuals. The U.S. Tenth Circuit Court of Appeals held that opt-out default rules do not provide sufficient protection.[262] Thus, this decision may suggest that opt-in is more extensive than required since the opt-out approach would be a less restrictive means, yet sufficient, for advancing the desired goals of the legislation.

The court further held that the regulation in question would have restricted commercial speech.[263] Commercial speech "does no more than propose a commercial transaction; is an expression related solely to the economic interest of the speaker and audience; and advertises a product or service for profit or a business purpose."[264] Commercial speech in advertising has been recognized as being protected in section 2(b) of the Charter of Rights and Freedoms (Charter) under freedom of expression in several key Canadian cases.[265] Therefore, the contention that opt-in measures are not appropriate since they are overly onerous and could infringe upon the corporations' freedom of expression may be a potential line of argument pursued by such organizations.

3. Collection without knowledge or consent

Section 7.1(a) of the Act maintains that the collection of personal information is allowed only if "the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way." The word "clearly" is subject to interpretation and it is uncertain whether a civil standard of 'more likely than

---

[262] U.S. West, Inc. v. Fed. Communications Comm., 182 F.3d 1224 at 1239 (10th Cir. 1999).

[263] *Id.* at 1233.

[264] R.v.Smith, 44 C.C.C. (3d) 385 at 424 (Ont. H.C. 1988).

[265] *See e.g.,*Rocket v. Royal College of Dental Surgeons of Ontario, [1990] 2 S.C.R. 232.

not' or a criminal standard of 'beyond reasonable doubt' would be employed. This section could also cover third party consent. For example, if a man sends his sister a gift from an e-retail site, providing the merchant with all her personal information, the sister would not have had the opportunity to consent to this dissemination of her data. Most reasonable people would agree that receiving the gift would be "clearly in [her] interest." The only way permission could be obtained would be if her brother asked for her consent before ordering her gift, which may ruin the element of surprise. This example illustrates that the validity of third party consent and the acceptable forms thereof may lead to a rather undesirable path of endless possibilities for debate.

It is also unclear if the retailer would now be able to contact the sister in its marketing efforts or if it would need to seek consent from her or her brother first (since by contacting her directly, it would already be violating the consent principle). If one subscribes to the consequential approach of statutory interpretation, one would not want to ascribe to the legislature these administratively difficult and irrational consequences[266] which would mandate that the merchant contact the brother and have him send a consent form to his sister in order to forward her advertising brochures.

4. Implementation

An additional difficulty PIPEDA faces is the implementation of the ten CSA principles. Canada's Privacy Commissioner, George Radwanski, has decided to maintain a non-disclosure policy, except for those interpretations that may be highlighted in his annual report.[267] The reason articulated by Mr. Radwanski for his policy is that limited use of adverse publicity serves as his weapon to sanction non-complying organizations.

---

[266] DAVID DUFF, CANADIAN INCOME TAX LAW: CASES, TEXT AND MATERIALS, VOLUME I. (2000). (unpublished – on file with the author).

[267] Michael Geist, *Privacy law needs open disclosure*, THE GLOBE AND MAIL, May 31, 2001, at T3

This non-disclosure policy is problematic for several reasons. As there are no guidelines in the Act regarding what constitutes sensitive data or what acceptable implied consent would be, organizations would naturally turn to the Privacy Commissioner for guidance on these interpretations. Furthermore, both individuals and organizations will lack sufficient information to either take advantage of their rights or to meet their obligations, respectively.

At this point in time, there have been a number of issues and questions raised concerning the way the Act has been drafted. As has been asserted, there is ambiguous language employed, which is arguably necessary to prevent the unnecessary limitation of unlisted issues that may later surface. There is much speculation as to how the courts will interpret PIPEDA. For instance, they may "read in" an opt-in approach in their decisions. However, in the interest of clarity and in order to fully protect the rights of consumers, more comprehensive, express language should be employed in the Act and the opt-in approach should be employed.

VII. A PRIVACY MENU?

As the preceding analysis of the potential issues and shortcomings of PIPEDA demonstrates, it is indeed difficult to draft legislation that would adequately address the interests of both individual consumers and businesses. Moreover, the comfort level of online surveillance varies greatly with each individual, rendering it difficult to properly protect the concerns of those who prefer greater privacy, while also enabling those who are less privacy sensitive to reap the benefits offered by vendors as incentives to analyze their surfing activities.

Such divergence in consumer preferences may be addressed by the privacy menu suggested by Forrester Research.[268] It has proposed a four-tier privacy model that employs the basic premise of the Platform for Privacy Preferences (P3P)[269] in

[268] Michael Pastore, *Consumers Fear for their Online Privacy*, CYBERATLAS, Nov. 1, 1999, *at* http://cyberatlast.internet.com/markets/retainling/print/0,,6061_228341,00.html

[269] *Supra* note 155.

helping consumers identify sites that meet their personal level of privacy requirements:

Level 1: "where visitors choose anonymity, deliberately forgoing additional benefits offered by personalization and premium content. Retailers build trust by promising not to collect data or to use cookies."

Level 2: is a "one-way communication relationship whereby retailers promise not to initiate contact with the shopper or to disseminate personal information to third parties."

Level 3: "where consumers agree to two-way communication with retailers in which they share more personally identifying information in exchange for proactive notifications of specials."

Level 4: "is considered a trusting relationship whereby shoppers seek advice and active solicitations from retailers, including deals offered by established partners." [270]

This type of ranking technique exhibits the principles of both informed consent and choice since consumers will be made aware of the possible uses of their information while being presented with various alternatives. It would allow consumers to choose privacy policies that meet their personal standards of privacy while enabling companies to build trust with their clients, thereby foreclosing some of the concerns addressed in what would constitute a reasonable expectation or informed consent.[271] Retailers can also provide greater or fewer rewards according to the level of privacy selected.

CONCLUSION

This Note has addressed the tension that arises in the attempt to balance the interests of individuals in protecting their privacy rights while simultaneously recognizing the legitimate business requirement of data collection. It is generally agreed that individuals have a valid interest in protecting their privacy., Tthe Internet has drastically transformed the capabilities that organizations and even private individuals

[270] Pastore, *supra* note 271.
[271] *Id*.

have in discerning personal information. It is unquestionable that data mining and cookies, even with their potential for nefarious consequences, can and are put to legitimate and incredibly beneficial purposes.

The key to leveraging the advantages the Internet provides, while eradicating, or at least minimizing, the potential for deleterious results lies in an amalgamation of the proposed solutions. Many of the mechanisms proposed to address privacy concerns are wholly insufficient, as demonstrated by the problems that currently prevail in cyberspace. Government legislation is certainly a step in the right direction. It is very difficult, however, to draft legislation that adequately addresses the interests of both consumer and vendor parties. There is a constant tension between drafting regulations too restrictively, thereby excluding potentially important issues and defining clauses too broadly, creating ambiguity and uncertainty for the businesses that are required to abide by it as well as the consumers who may not be protected under overly general laws.

Countries and states seeking to implement similar privacy legislation ought to recognize the need to explicitly define certain terms such as "identifiable" and "purposes"[272] to avoid confusion. One useful way of doing this is to provide a non-exhaustive list of examples. Similarly, such legislation should not merely apply to 'commercial activity' but to any online browsing activity, since a commercial requirement excludes a great amount of Internet use such as research or surfing. The legislation should mandate fully informed, opt-in consent and should require that information be provided to consumers regarding the collection, use and disclosure of data, and in language that the non-technically oriented person can comprehend.

However, legislation is not enough. Consumer education and a basic level of technological safeguards may be required to radically reduce the dissatisfying number of privacy violations

[272] Such as in 'personal or domestic purposes', 'artistic, journalistic or literary purposes', and 'Principle 2's Identifying Purposes'.

that currently exist. Netizens need to be more aware of the potentials that exist for their personal browsing activities and information to be divulged to organizations as well as learning how to turn off the default 'accept cookie' options. Furthermore, those who are more sensitive to privacy concerns may find it prudent to invest in some technological tools such as Anonymizer.com which would enable them to browse anonymously, that is, until another company finds new ways to circumvent such products. In addition, an additional layer of consumer protection may be attained by adopting a privacy menu akin to what Forrester Research[273] recommends.

There needs to be a mechanism in play to educate Internet users of the possible privacy violations that technology can create, while providing them with the tools to make informed choices through a Forrester-like "privacy menu". Similarly, online businesses should not be burdened with overly onerous legislation insofar as they meet equitable regulatory requirements that should at least mandate informed consent and consumer choice. Treating information as a commodity which individuals can choose to use in informed bargaining transactions may be the most viable means to properly address the issue of legislating privacy in a manner that best employs the plentiful benefits the Internet provides, while simultaneously respecting the interests of both parties.

[273] Pastore, *supra* note 271.

RIDER TO STUDENT NOTE

PRIVACY WARS IN CYBERSPACE: AN EXAMINATION OF THE LEGAL AND BUSINESS TENSIONS IN INFORMATION PRIVACY

JEANETTE TEH†

RIDER 1

Page 64 first paragraph, third line, after the word broad, add the following footnote (which would be footnote number 193):

> Since the initial writing of this paper, the Privacy Commissioner has released a number of findings regarding PIPEDA's application. In his September 21, 2001 decision entitled "Selling of Information on physicians' prescribing patterns", the Commissioner held that personal information would not be interpreted so broadly as to include physicians' prescriptions or prescribing patterns. He further stated that other work products such as legal opinions or documents written in the course of employment would not be protected as "personal information". www.privcom.gc.ca/cf-dc_010921_e.asp (last accessed Nov. 21, 2002).

RIDER 2

Page 65, after the first full paragraph beginning with "This vague definition...", add the following footnote in the last line after the last word "traceability":

> This challenged has already arisen in the early findings of the Privacy Commissioner. In one decision, "Musician objects to collection of salary information by

---

† University of Toronto, JD/MBA Candidate 2002. Special thanks to the University of Toronto Centre for Innovation Law and Policy for providing me with a publication grant, Professor Lisa Austin (University of Toronto, Faculty of Law) and John Beardwood (Fasken Martineau LLP) for their assistance and guidance, as well as my family and friends for their support.

professional organization" issued July 23, 2000, *at* www.privcom.gc.ca/cf-dc/cf-dc_010723_04_e.asp (last accessed Nov. 21, 2002), the Commissioner held that as the professional organization which had the legal authority to collect the salary allotment of a company's entertainment budget, the information was not identifiable even though the musician complainant was the only entertainer in that establishment. In contrast, in a later decision issued November 20, 2001 decision entitled "A broadcaster accused of collecting personal information via Web site", *at* www.privcom.gc.ca/cf-dc/cf-dc_011220_e.asp (last accessed Nov. 21, 2002), the potential of a computer's NETBIOS (a "friendly" name related to its Internet Protocol) to identify an individual was deemed to be identifiable, and thus, personal information contrary to the Act. For a more detailed discussion of these decisions, see Beardwood, John, *Tea Leaves and Goat Entrails: A Review of the Privacy Commissioner's Significant Findings under New Canadian Privacy Legislation*, COMPUTER UND RECHT INTERNATIONAL JOURNAL, June 2002.

RIDER 3

Page 81, after the first paragraph, add in the following paragraph:

This principle was confirmed in the decision "Telephone company demands identification from new subscribers"[1]. In this decision, the Commissioner held that although a reasonable person would consider it appropriate for the telephone company to collect personal identification in order to run a credit check, the company did not state this purpose explicitly to prospective customers, thus, contravening the Act.

---

1 Issued November 8, 2001. *See* www.privcom.gc.ca/cf-dc/cf-dc_011108_e.asp (last accessed Nov. 21, 2002).

RIDER 4

Page 81, after the first paragraph under subheading (c), add in the following paragraph:

> A further limitation of consent was articulated in the Commissioner's April 26, 2002 decision[2], where he asserted that future legal requirements that are not yet enacted do not constitute a necessary purpose for the collection of personal information. This was due to the fact that there was no current legal necessity for such collection nor would a reasonable person consider such collection appropriate.

RIDER 5

Page 89, before heading 3, add in the following paragraph:

> The Privacy Commissioner has recently taken a very strong stance against the use of opt-out consent in his recent decisions. In a finding against Air Canada on March 11, 2002, he found that information for the use and disclosure of information customized according to the individual plan members' purchasing habits and preferences was sufficiently sensitive to warrant obtaining positive opt-in consent[3]. While the practice of using plan members' information to of advertise products, services and special promotions is unobjectionable, a reasonable person would not expect that this practice be extended to the "tailoring" of information to the individual's potentially sensitive personal or professional interests, uses of or preferences for certain products and services, and financial status without the individual's positive consent.
>
> The Commissioner concludes by stating that he has a "very low opinion of opt-out consent" and intends to ensure that any circumstances where opt-out consent is

---

2 "Bank accused of inappropriately demanding birthdates from account applicants". www.privcom.gc.ca/cf-dc/cf-dc_020426_e.asp (last accessed Nov. 21, 2002).

3 "Air Canada allows 1% of Aeroplan membership to "opt out" of information sharing practices". http://www.privcom.gc.ca/cf-dc/cf-dc_020320_e.asp (last accessed Nov. 21, 2002).

> permitted "remain limited, with due regard both to the sensitivity of the information at issue and to the reasonable expectation of the individuals"[4].

RIDER 6

Page 90, at the end of the first paragraph under heading 4, add in the following sentence:

> Even the Commissioner's decisions are sparsely written and the names of the organizations or companies omitted in his findings.

---

4 *Id.*