RESEARCH PAPER

Internet Privacy in Canada: A Public Interest Perspective

Written By: Julie Gustavel

For: Professor Michael Burke

Joint Graduate Program in Communication & Culture
York University-Ryerson University
Toronto, Ontario, Canada

August 2002

Paper Abstract:

Issues about informational privacy have emerged in tandem with the escalating increase in information stored in electronic formats. Data protection is a pressing issue not only because files of personal information are being kept in greater detail and for longer periods of time, but also because the data can be retrieved and compared or matched without delay, regardless of geography. While defenders of information technology cite efficiency and safety among the countervailing benefits, concerns from an increasingly tech-savvy public have introduced a sense of urgency to demand tough legislation. Although many studies have provided evidence of online privacy concerns, few have explored the nature of the concern in detail, especially in terms of government policy for our new online environment. Bill C-6, Canada's recent legislative action, has provided a practical basis from which to appraise governments' role in privacy protection. With this in mind, the paper will be divided into two parts. Part one will be undertaken to: (A) evaluate the arguments of critics as well as defenders of contemporary record-keeping practices and the philosophical conceptions of privacy, which underlie them; and, using these themes (B) provide a comprehensive assessment of the effectiveness of Bill C-6, examining the ways in which policy makers have begun to treat privacy as both a commodity and a secondary adjunct to business activity. Part two of the paper, purposes a series of recommendations or, more specifically, a framework for Bill C-6 that would, more effectively, protect individual privacy from private entities, who collect online data.

Internet Privacy in Canada: A Public Interest Perspective

Without question, the Internet has revolutionized the computer and communications world like nothing before. Until recently, much of the interest in the Internet has focused on its impressive technological development and expansion ("FTC announces proposal," 1998, para. 2, 3). However, this essay grows out of recent attention, which has focused on its commercial potential and the phenomenon of electronic commerce (e-commerce).

During the 1999 Christmas season, the hype surrounding e-commerce was almost unavoidable. Hundreds of e-commerce Web sites poured millions of dollars into advertising, so that everywhere you looked, someone was throwing a dot com, a dot org, or a dot net at you. Every television commercial, every radio ad, and every billboard screamed, "Visit us on the World Wide Web at www.ourwebsite.com!" This flood of advertising pushed 1999 e-commerce sales to dizzying new heights. According to researchers at the Boston Consulting Group (1999), American and Canadian online shopping sites took in some $9 billion over the holiday, a 300 percent increase over the previous year's holiday season.

Yet, all is not so jolly in this tale for the 21st century. For the past couple of years, the big story in the high technology sector has been the painful bursting of the dot-com bubble and the inevitable fallout—layoffs, site closings, and the withering of available funding (Bounds & Silverman, 2000, para. 1,3). However, even as the most stable online companies survive this

drought, they are running headlong into another predicament. It seems that the Grinch who stole Christmas is now poised to steal the thunder of the e-commerce revolution. The Grinch is the issue of privacy on the Internet.

What is Privacy and Why is it Important?

If you are on a bus or plane and someone starts reading over your shoulder, you probably feel uneasy. What you are reading is not a secret. It is just that your privacy is being invaded. Yet, almost every day, in some new and creative way, that innate human need—the right to privacy—is being chipped away. Sometimes the reduction is subtle, sometimes it is a full frontal attack—but the process has begun and it is a challenge we must answer.

Privacy is not just an individual interest, but it is first and foremost a political value of the highest order. The term privacy often links together a number of interrelated concepts; it underpins human dignity and other key values such as freedom of association and freedom of speech ("Privacy and human rights," 1999, para. 1). Consequently, there are many definitions of privacy, and it is not possible to discuss each of them here. However, it is important to establish a clear, shared definition of privacy for the purposes of this research.

In the context of this paper, privacy will be defined in terms of informational privacy, relating to the protection of what is called personal information, which is any type of identifiable information associated with an individual through a name or identifying number ("An internet privacy primer," 2001, para.4). The most widely used definition of informational privacy was developed by privacy veteran Allan Westin. In his 1967 seminal work Privacy and Freedom, Westin called privacy, "The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967. p. 7). This research paper's definition will be guided by the same principles that Westin established and will be comprised of two elements: the right to be left alone, free from intrusion and interruption; and, the right to exercise control over one's personal information or, more specifically, the extent to which one's personal information is shared and how it can be used.

In 1980, Walter Cronkite said the following, "If computers are permitted to talk to one another, when they are interlinked, they can spew out a room full of data on each of us that will leave us naked before whoever gains access to that information. But we must be vigilant against

their misuse, either accidentally or intentionally" (Berton, 2000, para. 22). Twenty years ago Cronkite recognized the threats to privacy associated with the vast amounts of information being compiled on all of us, then stored and interlinked.

Since that time, our privacy has been protected pretty much by default. As long as information about us, in paper records, is scattered over a whole variety of locations, someone would have had to go to a great deal of trouble to systematically violate the privacy of any of us. However, new information technologies have increased exponentially, sweeping away barriers of time, distance and cost. Now someone sitting at a computer terminal can compile a detailed dossier on any of us quite literally in minutes, if not seconds. These capabilities have created an intense consumer backlash from an increasingly tech-savvy public, who are worried about potential breaches of personal privacy and security with the advent of increasingly powerful computer technologies.

Are Consumers Worried About Online Privacy?

You hear a lot about Big Brother, in the context of government surveillance. Many Canadians today are just as worried about what Corporate Brother is going to do with their personal information. The salience of consumer Internet privacy concerns has been shown in numerous public opinion polls. In 1992, Ekos Research Associates Inc. released a survey of 3,000 Canadian households called, "Privacy Revealed: The Canadian Privacy Survey". The survey results showed that 92 percent of all Canadians felt at least "moderate" levels of concern about personal privacy, while 52 percent expressed "extreme" concern ("Privacy and Canadian Information", 1994, para. 12). Furthermore, in the 1994 TELUS Longwoods survey 39 percent of respondents felt that they would be so concerned about privacy invasions that they probably would refrain from using the Internet ("Privacy and Canadian Information", 1994, para. 12).

More recently, a study commissioned in 2000 by Derivion, a Canadian e-billing technology provider, revealed that eight out of ten Canadian consumers are concerned about protecting their privacy when participating in online activities (Zronik, 2001, para. 5). The survey also found that 40 percent of Canadians, who use the World Wide Web, would be more inclined to participate in online transactions if they had greater assurances that their privacy would not be compromised (Zronik, 2001, para. 5).

On the whole, these findings reinforce and renew the fact that knowing what is done with our online information once it has been collected, and having reasonable control over those uses is important. Privacy is built on reciprocity and transparency. To date, online collectors of personal information have not been transparent about their collection and usage, and this has led to the emergence of consumers who are more aware of how their personal information is used by businesses, more informed about their rights and more intent on preserving their privacy.

The primary reason for the public's uproar over Internet privacy is the tremendous amount of transactionally generated, personally identifiable information, which Web sites routinely collect, often in a completely invisible manner through a technique known as online profiling. Most online profiling is generated in three ways; through simple Web surfing, the use of server set cookies, and through Web bugs.

The Technologies of Privacy Invasion

If you point your Web browser to http://www.junkbusters.com/cgi-bin/privacy, the Junkbusters Web site will display all of the information that its server has acquired about you by simply requesting a page from its site. First, Junkbusters will be able to identify your Internet Protocol (IP) address and your remote host. While IP address and remote host information are not necessarily personally identifiable information (because several users can use a single IP address, and because many Internet Service Providers (ISP) dynamically assign IP addresses), Web sites can infer the organization or ISP you belong to, as well as the general geographic location of your host server.

Next, if you followed a link from another Web site to the Junkbusters page, Junkbusters can record that location, and if you discovered the Junkbusters site by using a search engine, they will even know the term you used to find them. Also passed along in the transaction is your Internet browser type and version, what type of computer and operating system you are on (Windows, Macintosh, Unix), your screen resolution, and the date and time of your visit. Web sites record all of this information in huge log files, which allow them to identify the "click trails" of people surfing through their site (Nelson, 2000, p. 20).

A more efficient method for Web sites to identify individual Web surfers and their browsing habits is through the use of cookies. Cookies are small bits of text that Web sites may place on your hard drive. Not only are most Web browsers preconfigured to automatically accept cookies,

but if you have a Web browser on your computer, you also have a cookie file (Anderson, 2000, p. 37). As you view a Web page, HTML code—the standard language of the Web—directs the browser on your computer to write a cookie in your cookie file, recording whatever data the server specifies (Anderson, 2000, p. 37). Subsequently, the Web server can read your browser's cookie file and can create cookies that contain a unique identifying number that can be used to call up whatever information they have previously collected from you and stored in their databases (such as which pages you visit within a site, how long you spend on a particular page, and information supplied via forms such as email addresses, passwords, and credit card numbers) (Anderson, 2000, p. 37). Each Web site, however, can read only its own cookies; in other words, one site cannot read a cookie created by another site (Anderson, 2000, p. 38).

The primary use of cookies is for Web site "personalization"—the point is to make the Web site more appealing to you, so you come back again (Anderson, 2000, p. 38). A prominent example of cookies can be found at Amazon.com. For instance, when Jane Doe visits Amazon.com and purchases a book, the Web server sets a cookie, which gives her a unique identifying number. Jane's unique ID can then be correlated with the information she supplied to Amazon.com via a purchasing form. The next time she visits Amazon.com, the site reads her cookie, instantly recognizes her unique ID and customizes the Amazon Web page to say "Hello Jane, welcome back". While site personalization may seem benign, the trouble with cookies is that Web sites can share user profiles with other companies, often without a user's knowledge or permission, by exchanging unique cookie identifying numbers (Anderson, 2000, p. 38).

Web bugs, which are similar to Internet cookies, are perhaps the best example of the ways in which consumers are not aware that they are being profiled. Like cookies, Web bugs are electronic tags that help Web sites and advertisers track visitors' whereabouts in cyberspace. However, whereas cookies can be turned off or controlled through a Web browser, there are no such management features for Web bugs, because they are embedded within the HTML code on a Web page (Bradley, 2000, p. 41). Despite its insidious moniker, a Web bug is simply a 1-pixel GIF—a graphic image so tiny that it is essentially the smallest dot possible on your computer screen. The Internet advertising community prefers to identify them by more palatable names like "1-by-1 GIF's" and "invisible GIF's" (Bradley, 2000, p. 40). Whatever name, Web bugs track surfers in areas online where banner ads are not present, or on sites where people may not expect to be trailed. Essentially, they behave like beacons, so that every time you hit a Web page

it sends a "ping" or a callback to the server saying, "Hi, this is who I am and this is where I am" (Bradley, 2000, p. 41).

As I have set out to illustrate, the level of tracking facilitated by transactionally generated information on the Web is truly incredible and quite unique. Jerry Kang (1998) points this out by noting the difference between shopping in a real world mall, and surfing through a Web site. In the real world mall we are generally anonymous as we window shop, flip through magazines in the bookstore, and walk from shop to shop. The only time that we are personally identified is if we use a credit card to purchase something.

> "By contrast, in cyberspace, the exception becomes the norm: Every interaction is like a credit card purchase. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home. There are entities called "road" providers, who provide the streets and ground you walk on, who track precisely where, when, and how fast you traverse the lands, in order to charge you for your wear on the infrastructure. As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you peer into, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyber-bookstore notes which magazines you flipped through, recording which pages you have seen, for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John's Wort, read for seven minutes a news weekly detailing a politician's sex scandal, and flipped every-so-quickly through a tabloid claiming that Elvis lives. Of course, whenever any item is actually purchased, the store as well as the credit, debit, or virtual cash company that provides payment through cyberspace take careful notes of what you bought" (Kang, 1998, p. 1198-1199).

Developments in information technology are claimed to be revolutionary innovations that will propel societies and nations toward renewed economic growth, new modes of political participation, and a rejuvenated sense of community. Nonetheless, Kang's example vividly illustrates why the public is concerned about online profiling and its relationship to privacy. However, depending on your conceptualization of the importance of privacy and its role in promoting the common good, you may draw quite separate implications from this situation. This is the case with how industry and privacy groups have responded.

With this in mind, the overall goal of this major research paper is to examine two competing views about whether all of this data collection is a bad idea, and if so, what should be done about it. To this end, I am proposing to undertake an investigation of online privacy from two different perspectives:

1. **Privacy as a human right, essential to self determination, autonomy, and democracy; and**
2. **Privacy as a market efficiency maximizing commodity**

The aim of this discussion paper is to more fully outline the philosophical underpinnings of these two competing views of privacy, and how they have evolved to take account of the vast data collection capabilities facilitated by computers and the Internet. Understanding the values inherent in market and rights based conceptions of privacy, I want to examine the ways in which various government bodies, civil liberties groups, business and newly emerging industry groups, in the United States and Canada have proposed solutions to the perceived problems on the Internet, with differing results.

Within this context, it is my contention that the greatest threats to privacy seldom come from those who want to do something corrupt. They come from those who argue, with the very best intentions, that privacy needs to be sacrificed on the altar of some greater good—efficiency, better customer service, improved delivery of government programs, enhanced security. This has resulted in a situation where "private industry," not personal privacy, is seen as the more valuable social good. As I will illustrate, technological changes and the growing specialization and widening scope of government has made it increasingly difficult for the Canadian government to formulate policies adequate to the complex tasks they undertake. This trend contains core elements of a strategy that is complemented by the fact that industry and government privacy policy has consistently failed to address these issues, opting instead to focus on the narrow needs of the information economy. With this in mind, Canada's Bill C-6—The Personal Information Protection and Electronic Documents Act—will be the cornerstone of this paper. While the legislation shows leadership, I argue that it does not fundamentally recode the architecture of cyberspace privacy in a way that adequately addresses and reduces privacy concerns.

In order to make what follows intelligible, it is important to describe the historical background of the development of privacy law and current state of conflicting priorities that have become the defining issues in this "e-com" decade. It is only by articulating the various positions and identifying and evaluating the dominant themes that it is possible to move towards the consideration and analysis of specific policies that have been implemented in the area of online personal privacy. Data protection legislation is not a new phenomenon, so it is not hard to identify principles upon which to base the legislation. The real difficulty lies not in agreeing on what those principles should be, but in determining how they should be implemented. There is a

greater need for uniformity in legislation applying to the private sector, and the analysis, which follows focuses on this area in particular.

Privacy: A Brief Historical Background

Absolute privacy, except for the individual living alone on an island, has never existed. In small towns and villages, where most people lived before the industrial revolution, there was little or no privacy (Rifkin, 1992, p. 154). The details of one's wealth or health could not be hidden for long from other community members. Indeed, someone seeking privacy from others might have been looked at with suspicion.

The industrial revolution and the large cities it created changed all of that. With the industrial age came individualism, anonymity and privacy (Nizer, 1941, p. 526). More people became mobile, moving where they could find work, and the telephone and radio communications made the limits of time and space less relevant (Nizer, 1941, p. 526). Gradually, the small communities where everyone knew everyone began to disappear. The State had not yet attained size, and it did not have the resources or the will, to collect much personal information about its citizens, and what little information there was had not yet acquired a high enough value to trigger the interest of the burgeoning large corporations (Nizer, 1941, p. 528). As a result, individuals came to enjoy, and expect, an unprecedented level of privacy. The same industrial age that allowed privacy to flourish, however, also created the means to intrude upon it and eventually threaten to take it away.

Progressively, with the introduction of income tax and with the creation of social programs, the State began to collect more personal information. The creation of the computer to process all this new information made information useful for new purposes, and it quickly gained economic value (Nizer, 1941, p. 529). As workers have begun to be replaced by computer-controlled machines and as new communications technologies link together not only the great financial capitals of the world, but also the most remote places on earth, information and knowledge have gained a new importance in our economies. With computer technology, information can now be compiled, processed, stored, retrieved and communicated at speeds and in quantities unimaginable not long ago.

Widespread concern about privacy and the computerization of personal information first arose in the United States in the 1960's (Rifkin, 1992, p. 154). Over that decade, the public and private

sectors made new demands for personal information and tried to establish large computerized data banks. In addition, there were proposals to establish a national data centre that would bring together different types of personal information held by the U.S. government in a central data bank (Rifkin, 1992, p. 154).

Throughout the 1960's, and into the early 1970's, congressional hearings, government studies, academic publications, and popular books considered the new threats to privacy. The issue of privacy in an information-based economy first attracted attention in Canada in the early 1970's when the former Department of Communications and the Department of Justice put together a joint Task Force on Privacy and Computers. The study produced by the Task Force warned that computers "may magnify, or at least highlight the problems" all information systems pose to privacy (Rifkin, 1992, p. 154).

As we move increasingly into the electronic economy not only have solitary mainframe computers been replaced by powerful networks, but the concern that the government holds a great deal of information does not reflect the reality that the private sector is now a major collector and user of personal information. As Anne Wells Branscomb, a highly respected privacy scholar stated, "Historically, our concern about computers was Big Brother—the government invading our lives and having too much knowledge about and control over what we're doing. Now we're discovering that big business is the real Big Brother" (Branscomb, 1996, par. 2). Clearly, the spotlight has now turned to cast a light on the role of private sector companies, and the previously benign view of the private sector's handling of personal information, in turn, sparking two competing views about whether all of this data collection is a bad idea.

Transactional Information and the Internet: Two Views of Privacy

(i) Privacy As a Market Efficiency Maximizing Commodity

On one side of the Internet privacy debate are online marketers and advertisers, who still in their infancy, are struggling to figure out how to get the right advertising message out to the appropriate individuals. Within this economic framework, personal information is seen as a commodity, which retailers value highly. As a result, Internet and data marketing industries (which are infinitely intertwined because most Internet revenue is generated through targeted advertising) insist that they need to glean information that will help target sales. This is simply

because Internet users are unlike television viewers or newspaper readers, who usually pay attention to the medium for a sustained period of time (Farwell, 2000, p. 24). Instead, statistics show that Web surfers tend to roam online—checking stocks, paying bills, sending e-mails, and making travel plans. According to media research firm Neilson Net Ratings, Internet users visit an average of six unique sites during a 30-minute online surfing session and afford a meager 57 seconds to each page that they view (Farwell, 2000, 24).

With all this competition for surfers' attention, advertisers decided they either had to abandon Internet advertising or find a better way to target consumers. Since Internet users tend to feature some of the most lucrative demographics (high income, college and university educated, etc.), abandoning the audience was not a viable option (Farwell, 2000, 24).

When advertisers began casting about for ways to target prospective buyers, online advertising network companies stepped up with the concept of online profiling through mechanisms like Web surfing, the use of server set cookies, and Web bugs. They did this under the premise that it is in the best interests of e-commerce if information is collected, because this information allows companies to (i) determine the interests of consumers (ii) determine the effectiveness of advertising, and (iii) tailor marketing campaigns to individual interests (Farwell, 2000, 25). Whether this kind of targeted marketing is better is, in my eyes, as subjective a decision as whether a restaurant specializing in steaks is better than one with a wide variety of items and no specialty.

Better or not, Internet and data marketing companies insist that the benefits of online profiling have a tangible effect on increasing revenue, and it is precisely this situation that has evoked a strong disincentive for the private sector to develop and implement privacy policies (Farwell, 2000, p. 25). This is not to say that within the past year and, more specifically, in the past couple of months, that the industry has not been concerned about online privacy. Heightened concerns surrounding privacy may, in fact, be evidence of a whole new dynamic in the marketplace, should consumers refuse to purchase products online due to privacy concerns. Unquestionably, Internet and data marketing companies are worried that they will not be able to maximize profits due to consumer groups who have understandably asked some loud and pointed questions, which have thrust privacy issues into the spotlight (Hatlestad, 2001, para. 2). These concerns, however, have been transformed into a "broccoli" issue. What I mean is that Internet and data marketing companies know it would be good for them to pay greater attention to what is happening and the

implications for their relationship with their customers. Yet somehow, privacy issues are usually only considered, and then only reluctantly, when they are plopped on the plate in front of them and cannot be avoided.

For instance, many companies in both Canada and the United States have yet to adopt a concerted policy on privacy (Geist, 2000, para. 4). As a result, consumer groups are inviting intrusive government regulation, aggressively pushing the development of a legal framework of predictable, uniform, rules that would enforce the principle of accountability through law (Geist, 2000, para. 5). However, most, if not all, high-tech companies claim increased privacy demands place an undue burden on their businesses, when government prematurely forces markets towards regulation. They argue that laws, which make it more difficult and expensive to compile databases, have a disproportionate impact on small and new businesses that cannot afford other means of growing (Singleton, 1999, para. 4). This situation, they insist, will ultimately hurt consumers because competition will be decreased, and, in turn, fewer goods and services will be offered (Singleton, 1999, para. 4). Therefore, companies maintain that for the retail industry to grow its share of the market online, the private sector must remove the privacy barrier. In other words, instead of trying to turn privacy into a consumer protection issue that invites intrusive government regulation, it should be treated as a market issue, which will channel privacy into a proactive approach (Hatlestad, 2001, para. 2, 3). It is argued that such an approach would offer consumers the protection they want without subtracting from sales numbers and, thus, win over more potential customers than the "hard line" would (Hatlestad, 2001, para. 2, 3).

In the United States, many of these principles are enshrined in a self-regulatory framework, which, in theory, is supposed to inform customers of data collection techniques and uses through the posting of accessible privacy policies (Singleton, 1999, para. 8). Supporters of a self-regulatory approach to privacy protection point out that it is clearly in the self-interest of industry to protect the personal information of its customers (Hatlestad, 2001, para. 3). Simply put, they argue that it is good business to maintain a reputation for respecting consumer rights. In actual practice, however, the performance of the industry leaves much to be desired.

The United States Federal Trade Commission (FTC) has, in place, a four-point program for privacy protection: notice, choice, access, and security. The idea is that you have rights: 1) to be notified that your information is being shared; 2) to choose if you want that to happen; 3) to have access to the information to ensure its accuracy; 4) to have the security of knowing it will not fall

into the wrong hands (Noak, 2000, para. 5, 6). However correct the program might sound, the FTC has no effective power to enforce it. In the absence of regulatory authority, the agency has been forced to negotiate with an industry that profits from violating those very rights on what are, in effect, voluntary standards (Dodd, 2000, 10). The result is an agreement that was described as a great advance in privacy protection but is nothing of the kind.

Although the initiative contains useful items, such as a contractually binding commitment to allow individuals to correct information a company may be distributing about them, it is not binding on businesses that refuse to subscribe to it (Dodd, 2000, 10). It also does not give consumers the right to control the use of their personal data, as outlined in the FTC's own program (Dodd, 2000, 10).

In lieu of these problems, many American Internet and data marketing industries have established their own voluntary enforcement mechanism, the use of privacy seals. Seals, alternatively referred to as "trustmarks," are currently provided by TRUSTe and the Better Business Bureau Online (BBB Online), and are meant to certify that a Web site displaying a seal dutifully follows its posted privacy policy. Web sites interested in receiving a seal pay an annual licensing fee and agree to have their privacy practices evaluated by the seal granting authority. TRUSTe evaluates member sites through periodic reviews. The BBB Online also requires its members to conduct an annual "self assessment" test, which entails answering a series of questions relating to specific privacy practices (TRUSTe, 2001, License fees, para.1). Both seal granting authorities also have a dispute resolution system, which allows consumers to seek redress against a site for violating its privacy policy. If an agreement is not reached a site's seal may be revoked, and the complaint may be referred to American government prosecutors as a possible fraud case (TRUSTe, 2001, Resolution process, para. 8, 9).

Just as the FTC's four-point program for privacy protection has its problems, so do seal programs, which the industry proudly claims guarantee a Web site's compliance with posted privacy policies. First, it is procedurally difficult for consumers to bring a complaint against a Web site, and have that complaint swiftly resolved. TRUSTe, for example, requires users to first complain to the site committing the claimed violation (TRUSTe, Resolution process, 2001, para. 13). If a site does not respond promptly (TRUSTe does not specify how long this should take), or if a consumer feels that a response is unsatisfactory, then TRUSTe will step in. At this point, TRUSTe will decide whether a customer's complaint is legitimate. If it is, it will seek to

negotiate a settlement with the violating Web site. If a satisfactory solution is still not reached, TRUSTe insists it will pursue the issue further by enlisting outside auditors (TRUSTe, Resolution process, 2001, para.13). Finally, and according to TRUSTe, only in "extreme cases" will a complaint be forwarded to the "appropriate government agency" (TRUSTe, Resolution process, 2001, para.13). TRUSTe offers no guidelines about how long this whole process should take.

Even more troubling than the burdensome resolution process is the fact that TRUSTe has never removed a member site's seal in roughly six years of operation, and it consistently rules against online consumers (McCullagh, 1999, para. 4). It does this simply because independent privacy groups like itself and BBB Online earn their money in sign up fees they receive from e-commerce organizations, becoming more of a privacy advocate for the industry rather than for consumers (McCullagh, 1999, para. 4).

Unquestionably, the numerous and cogent criticisms presented above are not unlike those made by privacy rights and civil liberties groups, who maintain that the Internet data marketing industry's self-regulatory framework is deeply flawed and does not live up to high promises of privacy protection and user empowerment. Even if all of the problems with privacy policies and seal enforcement were somehow ironed out, the current system in the United States would still contain one fatal flaw; data marketers know they will not be punished for violating their own privacy policies and, as a result, they have little incentive to act in a responsible manner.

(ii) Privacy As a Human Right, Essential to Autonomy and Democracy

Consumers want the convenience of secure e-commerce without worrying about having their identities stolen, being spammed, or having the aggregators of personal data knowing—and profiting from—every detail of their lives. They argue that privacy is an intangible good that is compromised by the largely invisible and intrusive collection of browsing habits.

By all means, people must be willing to divulge some of their personal data to participate in modern life. As strongly as I believe in the fundamental privacy rights of the individual, I equally strongly reject the view that considers access to information as an "administrative right," or that it is merely desirable but not essential in our society. I reject the view that privacy "trumps" access. That view is, I suggest, patently simplistic and ignores the balance foreseen by the framers of our privacy legislation. It is, however, important to underscore the way in which the

issue of privacy has taken on a distinctly more sensitive note since the tragic events of September 11, which put access to information—both personal and general government records—and privacy, squarely in the targets of security experts.

Watchdog organizations, public advocacy organizations and the media have been vigorous in their denunciation that security appears to be trumping privacy rights (Fitzpatrick, 2002, para. 1). The events of September 11 have given governments the apparent justification to lessen the privacy protections afforded individuals—under the guise of security. This leads to a higher likelihood that a variety of enforcement mechanisms, in place, to minimize violations of fair information practices will fall short of their intended purpose(s).

Indeed, going back to the argument surrounding privacy, as a market efficiency maximizing commodity, when privacy rights are diminished and public good gets corrupted by the desire for private gain and when aggregate data are broken down so they can be traced to individuals, the question is how to curtail abuse. Valerie Steeves (2001) provides some real-life examples to ponder:

- Earlier this year, a company obtained a list of people who had signed up for a weight loss program, and sent them chocolate bar samples by direct mail at Easter, reasoning that Easter was when they were most vulnerable to food pressures.

- During hearings to confirm his appointment to the United States Supreme Court, Judge Robert Bork was personally embarrassed when a reporter published the names of all the videos he had rented from his local video store.

- Donnelly & Sons, the largest American data firm, consistently argued that its databases did not pose a threat to children – until Los Angeles journalist Kyra Phillips reported that, for $277, she was able to buy a list of the names and addresses of over 5,000 children in the Los Angeles area, even though she used the name of a notorious child killer (Steeves, Privacy: A right or a commodity? para.10).

The scenarios that Steeves describes sound menacing. However, they clearly illustrate that online profiling has social consequences. The most obvious are the ones, which affect the individual, who suddenly faces embarrassment or loss of a service, because a corporation or government has invaded his or her privacy and seized their personal information. However, there is also a larger issue at stake.

While, on a theoretical level, self-regulation assumes that all privacy values can and should be resolved by the marketplace, a marketplace approach to privacy ignores the fact that privacy has other values, such as its role in promoting identity formation, free speech, and democracy (Diffie

& Landau, 1998, p. 55). It is my contention that the pervasive loss of privacy on the Internet poses a much greater threat to individual identity, free speech and democracy, than any threat to an efficient marketplace. However, nobody talks about the loss of democratic rights, because we enjoy them on a daily basis; they are invisible until they are taken away. That is very similar to privacy.

Ideas about the importance of autonomy, a space (both psychological and physical) for individuals to develop free from impositions by the state (and increasingly commercial interests), were first put forward during the Enlightenment by John Locke. Locke argued that the very essence of a person's being is tied to property, which helps express that person's feelings and future plans (Radin, 1993, p. 43). The paramount property right is therefore in a person's own body, and by extension a person's thoughts. Thus, when an agent such as a government or commercial entity "takes" a person's property without cause, this is a violation of individual autonomy and privacy (Radin, 1993, p. 43).

Locke's foundational arguments have been extended by many scholars who have helped articulate the connection between privacy and democracy, and the specific harms that occur when it is taken away. Here, privacy provides a space for individuals to develop their own identity and ideas, free from political or commercial control. Echoing this view, Susan Diffie and Whitfield Landau (1998) note, "Without the opportunity to discuss politics in private, the finished positions that appear in public might never be formulated." Jeffery Reiman (1995) shares this view, commenting that in the absence of privacy, individuals will not feel free to engage in perfectly legal, but unpopular activities—apply for welfare, join a demonstration—for fear of "going on the record".

Oscar Gandy (1993) shows how the loss of individual autonomy, which results from the act of being watched, is socially problematic. In the Panoptic Sort, Gandy explains by way of illustration how computer matching is now becoming a routine feature of bureaucratic surveillance. It has also been shown that by a process known as cross-system enforcement it is possible to make an individual's relationship with one organization dependent on the performance in another. In New York, suggestions have been made, introducing the idea that issuing marriage licenses should be dependent upon the payment of outstanding parking fines (Gandy, 1993, p.32).

Apparently some administrations hope that by letting people know that cross-system computer matching can occur, it will act as a symbolic deterrent against "deviant" behavior. However, these activities classify people into abstract, impersonal categories, which claim to identify not only "good" customers, but also "risky" ones who should be avoided and possibly punished (Gandy, 1993, p. 34). These models are based on faulty assumptions about categories of people, and result in a form of market discrimination that is akin to racism. While these categories may be acceptable according to Internet and data marketing companies, for an outside entity to take a snapshot of your private self, or worse, to codify and exploit that version of you, represents a profound threat to your freedom.

The fundamental problem with these practices is that they deny individuals (and groups) the right to determine which categories they wish to be placed in, narrowing the range of societal options open to the individual (or group) (Gandy, 1993, p. 35). In Lockean terms, the individual no longer "owns" himself or herself (Radin, 1993, p. 46). In a world where people are not free to define themselves, and do not speak out for fear they are under the gaze of some unidentified authority (be it government or a corporation), conformity will become the norm and democracy will surely suffer (Gandy, 1993, p. 38). This kind of atmosphere is not only problematic, as it always acts to normalize by discouraging the different but sameness is not what makes our culture so vibrant; it is our uniqueness that makes it possible for many new ideas to flourish.

The identification of this loss of autonomy brought about by database marketing has led many scholars and policy makers to call for mechanisms to protect personal information online. No one should be surprised in the wake of this altered privacy landscape, the articulation of privacy issues and their resolution has shifted. Sectoral codes, self-regulation, an ad hoc or patchwork set of laws and industry watchdogs are no longer sufficient, as they leave the individual without any effective tools to assert his or her privacy rights. To remedy this troubling situation, privacy and civil liberties groups are pushing for the passage of tougher legislation that will ensure a baseline of enforceable privacy rights.

What Protection Exists: The Canadian Experience?

In terms of online privacy, the Canadian government's original assumption was that our regulations took precedence and Internet users would just have to adapt. Over time it has become apparent that the confidence with which we began regulation has begun to evaporate.

This is because it has become increasingly clear that the Internet is not a mere variation on existing means of expression but a radically new form.

Recently, the Canadian government has decided to get involved in the growing chorus of legislators responding to public demand for statutory recognition of the right to control one's personal information. Until now, businesses have enjoyed freedom in collecting and using customers' private data—they could compile mailing lists, create customer profiles and even sell the information to others. However, the Canadian government has claimed it wants, ostensibly, to protect the privacy of personal information in the private sector, and to ensure that data is treated with respect and not left open for all to read or resell. In 1998, after years of consultations with business professionals, consumer advocates, and public policy experts, this legislative desire coalesced into legislation known as Bill C-54. However, Bill C-54 was short-lived, and after it "died" (when Parliament prorogued), the government reintroduced it as Bill C-6—The Personal Information Protection and Electronic Documents Act—in October 1999. On January 1, 2001, Bill C-6 became law.

At the federal level, it is important to note that in Canada there is little protection of privacy by formal regulations, especially few attempts to respond to growing public concern about personal privacy on the Internet.

For its part, the Canadian Radio-Television and Telecommunications Commission (CRTC), under the provisions of the Telecommunications Act, sets out to protect the privacy of individuals from telemarketing, including time of day restrictions, identification and disclosure requirements, and consumer's rights to have themselves removed from marketing lists. However, these are merely band-aid measures in relation to the underlying problem, since protection is principally restricted to the use of automatic dialing-announcing devices (ADADs) for commercial solicitation purposes (Ayed, 1998, para. 3). What is interesting here is that ADADs were considered a privacy invasion, even before taking into account the unauthorized collection and disclosure of personal data that made the call possible. At the time, consumer complaints focused on the physical privacy invasion, without fully appreciating that such invasions were based on a growing trade in personal information.

It is in this sense that the federal telecommunications regulator has not purported to limit the unauthorized collection, trading and use of personal information. Instead, it has opted to take a "laissez-faire" approach to the Internet, citing that the goals of the Telecommunications Act are

not only being achieved, but they are vibrant, highly competitive and successful, without regulation (Ayed, 1998, para. 3). This decision, which arrived in the spring of 1999, after a 10 month review of Canada's new media industry, not only leaves the powerful new technology facing far less oversight than any other Canadian medium, but it has left privacy advocates angry, since online privacy was not one of the issues raised during the hearings. This is evident in the CRTC media release, whereby it was noted that there are already adequate Criminal Code provisions and occurrences of self-regulation to handle on-line crimes (CRTC News Release, 1999, para. 2). These crimes, however, were defined in nature as the production of hate literature, child pornography and the distribution of bulk e-mail ads (CRTC News Release, 1999, para. 3).

Before this year, only Quebec had adopted comprehensive privacy legislation applicable to the private sector. Quebec's Act, Respecting the Protection of Personal Information in the Private Sector, provides a detailed framework for the collection, use and disclosure of personal information ("Privacy Protection," 2000, para. 2). The legislation came into force in January 1994, and while it may still be too early to fully assess its results, it is fair to say that it has not created havoc for Quebec businesses. In the rest of Canada, the right to be let alone is reflected in our laws.

First, at the constitutional level, is the Canadian Charter of Rights and Freedoms. While it does not contain an express right to privacy, it does guard against unreasonable invasions of privacy. As the Supreme Court of Canada recognized in a 1990 decision, the primary value served by section 8 of the Charter (the right to be secure from unreasonable search or seizure) is privacy, although exclusively in the criminal law context (Steeves, Humanizing cyberspace, para. 12). In terms of the electronic surveillance of individuals, the Court interprets section 8 in a more relaxed fashion, making the level of constitutional protection given to personal information very limited. In any case, the Charter is essentially an instrument for checking the powers of governments over the individual, so this constitutional right to privacy would apply only to state action and not to private conduct.

In Canada, the federal Privacy Act, enacted in 1982, governs the collection, use, disclosure, retention and disposal of personal information by federal government institutions, which includes all federal departments, most federal agencies and some federal Crown Corporations. However, it was written in the information-technology "dark ages" of the early 1980's and it has, for instance, no specific rules for online profiling ("Privacy Protection," 2000, para. 2). The federal

Privacy Act, was very good in its time, and has stood up very well, but to leave unattended and—I will avoid the use of the word "unregulated"—unwatched, the activities of the largest accumulators, users, manipulators, and marketers of personal information, the commercial world, has, in my opinion, been an unfortunate oversight, which should have been dealt with much earlier. In this context, the implementation of The Personal Information Protection and Electronic Documents Act has been long over due.

According to former Industry Minister John Manley, who spearheaded Bill C-6, The Personal Information Protection and Electronic Documents Act is a big piece of legislation that heralds a major structural change within the online e-business world. Aside from gun control, Manley insists that it is probably the biggest piece of regulation that the Canadian government has enacted (Thompson, 2000, p. 12). That is not to suggest that the use of personal information by the private sector outside Quebec is completely unregulated. However, privacy protection in the Canadian private sector consists of a patchwork of laws, regulations, and codes that create different standards applying to few industries.

The origins of Bill C-6 are found in an early approach to establishing privacy standards known as the Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, issued by the Organization for Economic Cooperation and Development (OECD) in 1980, for its member states. These guidelines set an internationally recognized minimum standard for the treatment of personal information and incorporated what have become known as principles of fair information practice. In 1984, Canada became a signatory to the OECD guidelines.

To follow up on the commitment it made when it subscribed to the OECD guidelines, the federal government encouraged private sector corporations to develop and implement voluntary privacy protection codes. Since there is already privacy legislation embodying the OECD guidelines in the public sector at the federal level, and in most provinces, the area where there is the most need for privacy legislation guidelines is in the private sector. That is why the federal government worked closely with the Canadian Standards association (now known as CSA International), releasing, in 1996, the CSA Model Code for the Protection of Personal Information, which substantially embodies the principles contained in the OECD Guidelines.

The Code, a national standard, was developed following a lengthy consultation involving representatives of business, government and consumer groups and sets out to balance trade interests and business needs with the consumer's inherent right to privacy. It provides ten

consumer privacy principles that have been adopted by various industries and organizations. These principles include addressing accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access and challenging compliance, with respect to personal information (Refer to Appendix 1). Bill C-6 essentially incorporates the CSA Model Code, transforming it into law ("Connecting Canadians," 1999, para. 4).

Bill C-6 applies to all federally regulated industries, including transportation, financial services, telecommunications, and to any interprovincial transfer of personal information—even something as simple as the electronic transmission of a name and address across a provincial boarder for use on a mailing list (Lawson, 2000, para. 4, 5). The provinces have three years to enact their own privacy laws. If they fail to do so, Ottawa will apply its rules to all businesses within that province (Lawson, 2000, para. 4, 5).

There are three parts to the Bill. However, for the purposes of this discussion I will only be focusing on Part 1, which aims to protect the privacy of personal information collected, used or disclosed in the private sector ("Connecting Canadians," 1999, para. 27). Unfortunately, rather than being a comprehensive privacy Bill that protects Canadian citizens, the legislation suffers from a narrow commercial focus. It is the contention of this paper to illustrate how subsuming privacy rights within legislation designed "to support and promote electronic commerce" is the crux of the problem with Bill C-6. Buried deep in the Bill is a highly unusual constitutional time bomb that speaks to the relative dominance of the market model and does not provide clarity in certain key areas.

The Bill creates an uncertain grey zone between obligatory portions of the CSA Model Code, which are expressed as "shall", and recommended portions, which are expressed as "should". This is illustrated in Division 1, Paragraph 5 (2), which states, "The word 'should', when used in Schedule 1, indicates a recommendation and does not impose or ensure an obligation" ("Bill C-6," 2000).

By my count, the word "should" appears eleven times in Schedule 1, and while many of the occurrences in which it emerges sets out to define reasonable modes of operation to ensure that businesses comply with the principles of the Act, this is not the case in all situations. For example, Clause 4 (3)(6) reads in part, "An organization should generally seek express consent when the information is likely to be considered sensitive" ("Bill C-6," 2000). I would argue that

this statement is too weak in an age when vast amounts of information are collected, sold, and resold.

While the principles set out in the CSA Code provide an excellent basis for the development of legislative standards, word-for-word adoption of the Code creates confusion. The CSA Code was drafted in language suited not to legislation but rather to voluntary self-regulation. In other words, it was never meant to be used in this manner. A preferable approach would be to refine, adapt and expand the CSA principles as appropriate, so that all vague language is removed from the legislative standards. In this context, the word "should" must be replaced by "shall" if online consumers are to be properly protected, otherwise much of the intended protection is illusionary.

What constitutes "sensitive" information is going to vary from case to case and person to person. Most people would probably deem their personal, medical, or financial histories as "sensitive". More importantly, someone fleeing an abusive spouse might put their name and address into the same category. Clearly the language embedded in the clause is sufficiently vague and open to so much interpretation, that it will be difficult to determine what should be classified as "sensitive" information. Surely, in such cases, the consumer can only be protected if organizations are required to seek informed consent, in the full meaning of the term. This is interpreted to mean that a person grants his or her permission to collect personal information with a clear understanding of the reasons for the collection of the information and the uses to which it will be put (Geist, 2000, para. 4). However, this notion of informed consent will be an extremely daunting task, as the standard for consent is particularly troubling.

Consent may be the most contentious question of the entire privacy issue. Division 1, Clause 7(2)(A), reads, "...an organization may collect personal information without the knowledge or consent of the individual only if the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way" ("Bill C-6," 2000). If, indeed, companies are to be allowed to collect information on citizens, the Bill makes no effort to outline what kind of data collection can be constituted as being "in the interests of the individual". More importantly, in lieu of the recent public outcry over online profiling, which gave rise to the Bill, I think it is reasonable to infer that many Canadian citizens would not want data collected about them "for their own good".

Canadians have the right to know if data is being collected about them, and if they cannot be convinced that the collection is clearly in their best interests, then they must have the right to

deny permission for such information to be collected. A clause added to the Bill last fall, however, does not necessarily ensure that this will happen.

The introduction of the Bill, as it was originally written, described its intent 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" ("Bill C-54," 1997-98, purpose section, para. 1). The new clause added these words: "...for purposes that a reasonable person would consider appropriate in the circumstances," however, no guidance is provided as to how this requirement will be interpreted ("Bill C-6," 2000, purpose section, para. 1).

Essentially, the Bill fails to separate the requirements of knowledge and consent in situations where the requirement for consent is waived. In this sense, Bill C-6, like the CSA Model Code, treats knowledge and consent as one and the same thing. In other words, wherever the requirement for consent is waived, so is the requirement for notification. The fact that a consumer is unaware that information is being collected, and no consent at all needs to be obtained, leads to a situation that is a serious failing in implementing the intent of the Bill and I would argue that it must be rectified. Nonetheless, it is precisely when different levels of consent come into play that the meaning of the term is far from a black and white issue.

Consider the law's exceptions. Division 1, clause 7(1)(C), reads in part, "An organization may collect personal information without the knowledge or consent of the individual only if the collection is solely for journalistic, artistic or literary purposes" ("Bill C-6," 2000). Why are journalistic, artistic, statistical, or literary purposes exempted from privacy protection? It would seem clear that, under the protection of this clause, an individual's privacy can be violated by a journalist, artist, or scholar. Besides, the terms "journalistic", "artistic", "statistical", "scholarly" and "literary" are so vague that there is no limit to the types of organizations and activities, which can qualify under these exceptions and practically anyone could use them as a shield from prosecution. The term statistical purpose(s) is subject to abuse, as Canadian consumers well know, from the endless clever marketing solicitations they receive. If these exceptions were meant to apply only in cases where the research or study is conducted under the purview of an academic institution with rigorous standards and oversight, then the legislation should so specify.

Furthermore, Clause 4 (3)(7)(B) is a clear example of the wrong default condition, which is at odds with the arguments presented here. It reads, in part, "a check-off box may be used to allow

individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties" ("Bill C-6," 2000). In other words, do nothing and you have automatically agreed. While a more appropriate approach would be to ask users to opt in for the use of their personal data, marketers have suggested that mandatory positive requests for consent would irreparably harm Canada's fledging e-commerce and Internet marketing industries (Geist, 2000, para. 4). Despite this argument not only should positive consent be the guiding principle in the legislation, it should be a mandatory requirement that no information be collected unless permission has been granted.

Recall that online profiling through simple Web surfing, Cookies, Web Bugs—the ubiquitous means by which Web behavior is captured—is a prime example of concerns regarding how data can be collected without one's permission. Bill C-6, as written, assumes that businesses will operate in an "open manner" ("Bill C-6," 2000, Clause 9(2.2)). However, it should be noted that in browsers such as Netscape's Communicator or Navigator and Microsoft's Internet Explorer, no notification is given to the user that cookies or Web bugs are being deposited. Even if notification is given, it is often co-opted by vaguely worded, technical, and legalistic privacy policies that are extremely difficult for users to understand. After all, why should we expect the average Internet user to have any idea about what cookies, Web bugs, IP addresses, and remote hosts are? As Sherwin and Avila (1999) maintain, when faced with the legal mumbo-jumbo of long-winded privacy policies, of course consumers will just agree to everything rather than torture themselves.

In terms of cookies, it is possible to be informed by the browser that a request is being made for a cookie to be deposited. In order for this to take place an informed user must select the Preferences option under the Edit tab of the Netscape menu, and then select the Advanced option and click on the appropriate cookies option (Anderson, 2000, p. 38). However, this feature is not generally advertised, and unless one is a dedicated and well-informed Internet user, it is difficult to acquire the necessary knowledge.

More importantly, while we may be able to select the option to be informed about cookies, it becomes extremely inconvenient to carry on browser activities because of the frequency with which requests are made. Furthermore, it may be virtually impossible to visit some sites if

permission to deposit a cookie is not given (Anderson, 2000, p. 38). Thus, even many informed users may reluctantly turn off the request condition, in order to facilitate ease of use.

Clearly, there needs to be policies in place that would oblige businesses to review how they currently obtain consent to ensure that the method is appropriate with respect to the type of data being collected. However, even if these problems are resolved, it is important to note that if an individual does give explicit consent to a business or organization, it cannot be assumed that permitting an organization to collect and use personal information implies the right of that organization to sell or transfer such information to third parties. To assume this would be a clear violation of the Act, namely the idea that there must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent" ("A Private Sector Privacy Law," 2001). In other words, the default condition should not be that, once collected, transactional information is the property of the company that provides the product or service. The information should not be considered a cost-free bonus.

If the company wishes to use it beyond the immediate purposes of the transaction it must obtain the unambiguous approval of the customer. This principle may, however, prove to be a difficult task to implement. First, the protections offered by the Bill apply to interprovincial transactions and to those between Canada and other countries. However, in the latter case, Canada has little control over how other countries deal with the personal information of Canadians. In other words, so much personal information on Canadians flows to the U.S. where it is stored, processed, transferred and generally used beyond the jurisdiction of the Canadian government (Bennett, 1996, para. 4). With this being the case, it will be necessary, at the very least, for Canada to obtain the agreement of U.S. companies that do business in Canada, that personal information of Canadians that is transferred to the U.S. receive protection equivalent to that which is in force in Canada. It is plausible that Canada will be in a similar situation to the European Community.

Canada is certainly not alone in its commitment to effective regulation of privacy. In 1995, the European Union enacted a Data Protection Directive that restricts trans-boarder flows of personal information to countries that do not have adequate privacy protection in place. Late last year, Europe's Privacy Directive came to a compromise with the United States, exempting companies from European sanctions that ban the transfer of personal information about its

citizens to third-party countries that do not have adequate privacy protections, if they agree to join a "safe harbor" self-regulatory program (De Bony, 2000, para. 4, 5). The program promises European consumers basic information about and control over how their personal data is used and exemplifies the ways in which Europe was developing ground rules for transborder data flows.

In Canada, the primary reason for the change of direction from voluntary compliance to legislation was not simply the government responding to Canadians, who have expressed, in clear terms, the need for their personal data to be protected. This may well be what the government wants the public to assume, however, one of the main reasons that the government enacted C-6 was because of the persuasive power of the directive and the way in which the European Union puts pressure on non-European countries, like the United States and Canada, to pass private sector privacy laws in order to freely receive and process information provided by European companies or affiliates.

Although the rules have never been legally tested, the safe harbor system may put pressure on the United States to develop a policy initiative with Europe and Canada, which respects transborder data flows, since failure to develop regulations could act as a potential non-tariff trade barrier (Thompson, 2000, p. 13). Whether Bill C-6 should be amended to reflect these concerns, I do not know, but it is important for the Privacy Commissioner of Canada to be able to track data flows and transfers in order to determine whether the act is being complied with. This concern should not be ignored, if the aim of the legislation is to offer Canadians meaningful and workable privacy protection.

It must be remembered that in a fishbowl society, continuing protection against the threats of an ongoing stream of new and powerful technology will be difficult to achieve. Privacy policies are site specific and allow major Web portals to wiggle their way out of their contractual obligations and, thus, claim no responsibility over the privacy policies of advertising networks, such as DoubleClick, which serve their ads. Thus, even though Yahoo! Canada contracts with DoubleClick to deliver its ads, Yahoo! claims that it is not responsible for DoubleClick's privacy practices. This is a particularly audacious position considering that Yahoo! essentially invites DoubleClick onto its site, and because most Yahoo! users have no idea who DoubleClick is, or what it does.

Furthermore, most privacy policies only tell users about personally identifiable information that is collected online. No notice is given if a particular site is trying to merge its online profiles with information it has purchased from another company. This can be illustrated by the most recent controversy in the United States over the plans to "synchronize" online profiles with off-line direct marketing databases. On June 14, 1999, DoubleClick announced it was merging with Abacus Direct, an off-line direct marketing company, which collects individual credit card numbers, mailing addresses, phone numbers, and household income (Macavinta, 2000, para. 1, 2).

Another recent development facing online consumers is the growing number of Internet companies that are auctioning off personal information when they go bankrupt. Toysmart.com, a U.S. online toy retailer, filed bankruptcy protection in 1999. Majority-owned by Walt Disney Co., the company had posted guarantees on its Web site promising that personal data "Would never be shared with a third party," and that "Your information is safe with us!" (Farmer, 2000, para. 8). However, in an effort to recoup some cash, the company put its customer lists up for auction. Those lists included all sorts of personal information—birth dates, children's names and shopping preferences—that consumers had provided willingly in light of the privacy guarantees (Farmer, 2000, para. 8). In the end, Toysmart did not sell its customer lists because the bids were not high enough.

According to Andrew Shen of the Electronic Privacy Information Center (EPIC), these two examples illustrate how the possible merging of online and offline information databases can create the ability to not only obtain personally identifiable information, but a way in which to know the online behavior of real individuals (Electronic Privacy Information Center, 1998, para. 2).

Unquestionably, these large databases of information are a marketer's dream come true. It is precisely because of this situation that many companies argue that Bill C-6 and its new kind of "permission marketing", which requires an organization using existing repositories of information to return to individuals to gain their consent, may impede business from carrying on standard business activities and transactions (Thompson, 2000, p. 13). By way of illustration, not only are there limits on trading or bartering customers lists but if you gather data from a customer and send them a catalogue, you cannot use it later to send them a book of coupons. You must have their permission again. Aligned with permission is the idea that organizations must

identify their purposes internally, and must make reasonable efforts to ensure that the individual is advised of those purposes.

Clause 4 (2)(3) of the Bill reads in part, "The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected..." ("Bill C-6," 2000). While there is nothing to stop organizations from collecting or using personal information for objectionable purposes, as long as they have identified such purposes, many Internet and data marketing companies argue that this clause is a not simply an inconvenience rather it is a hindrance, especially when the rapid growth of the Internet continues to reduce traditional customer loyalties and intensifies competition (Farwell, 2000, p. 25). They argue that they are constantly looking for new ways to package and use information, and they insist there is, not necessarily, a unitary purpose for the information that is collected (Farwell, 2000, p. 25). In other words, the online profiler does not know what personal data will be of value or what relationships will emerge. Therefore, identifying a primary purpose at the beginning of the process, and then restricting one's use of the data to that purpose is, according to many businesses and companies, the antithesis of the entire data collection exercise.

While organizations' hands may be tied in the sense that they will not be able to go on great "fishing expeditions" for personal information unless they spell out exactly why and what data is to be used for this still may not be enough. Why? Because the vast majority of commercial Web sites do not post privacy policies at all. While the industry has been quick to indicate that many of the most heavily trafficked Web sites have posted privacy policies, such sites represent an infinitely small proportion of the universe of roughly seven million ".com" Web sites (DomainStats.com, 1999).

A study conducted by Law Professor Michael Geist between May and September 2000 at the University of Ottawa, examined 259 leading Web sites based in or targeting Canada. His findings paint a troubling snapshot of the state of Canadian privacy and e-business practices. A disappointing 41 percent of the sites failed to disclose their privacy policies and 26 percent of sites use cookies but do not reveal that to users (Geist, 2000, para. 4). Over half the sites do not provide contact information, and more than 6 out of 10 do not allow users to access information they already submitted (Geist, 2000, para. 4). More importantly, for companies that do post privacy policies, there are no restrictions on how often a Web site can change its posted policy. Most sites reserve the right to change their policies at any time, and suggest that users check

back from time to time (Geist, 2000, para. 5). For example, Federal Express' privacy policy states, "FedEx reserves the right to amend the privacy policy at any time with or without notice. Please check back frequently in the event of changes" (Federal Express, 2001). This violates the essence of disclosure, because it fails to provide adequate notice of potentially serious retroactive changes.

How difficult is it to have clear and straightforward procedures, including restrictions on the use of cookies and similar devices, consent boxes to tick off, and contact information for more details, presented on a Web page linked in an obvious fashion to the organization's home page? None of the requirements in the Bill seem burdensome. In fact, this is one case where a certain degree of organizational inconvenience, in the defense of the right to privacy, is necessary in order to provide effective privacy protection. Even more necessary, however, is a tougher Bill that forces businesses to act in a responsible manner.

Under the architecture of Bill C-6, individuals often do not have the means to determine whether their privacy has been violated, and, even if they had the means, it could be costly and time consuming to launch and pursue such a complaint. For instance, the extensive oversight powers afforded to the federal Privacy Commissioner do not necessarily ensure that all complaints will be resolved justly. Under the Act, the Office of the Privacy Commissioner is required to investigate complaints referred to it and report its findings. Instead of being authorized to award restitution directly, a complainant or the Privacy Commissioner must apply to the federal Court for a hearing ("Bill C-6," 2000, Clause 14 (1)). However, the federal Court is not accessible to the ordinary citizen. It requires the assistance of a lawyer, and a significant financial investment, allowing only the most determined and financially able complainants to pursue their wrongdoers under this regime.

To make matters worse, the Bill limits punitive damages to a maximum of $10,000 (indictable offences, which are rarely reprimanded in Court can be subject to a fine not exceeding $100,000) (Bill C-6," 2000, Clause 28). Consequently, this amount is sufficiently small so as to render the protection essentially ineffective and, in many cases, it is merely pocket change for some corporations. In other words, there may well be cases in which such a penalty constitutes nothing more than a cost of doing business from the perspective of the wrongdoer and, as a result, I would argue that the maximum compensation the Court can award should be

unlimited. However, despite the implementation of harsher fines, the real threat under the Act is public embarrassment, and Bill C-6 allows many companies to escape it.

In the event of a dispute, most corporations negotiate a settlement with the Privacy Commissioner, because it is better to settle than endure the negative publicity of being cited in a public report or having to defend one's self in court (Thompson, 2000, p. 13). A more reasonable scenario to the present situation would be one in which the Privacy Commissioner allows the process to be truly complaint-driven. This situation would entail that the Commissioner reacts to complaints and automatically initiates publication or legal proceedings when there has been a history of violations and the organization involved is unwilling to offer serious remedial measures. This is not to say that the auditing powers of the Privacy Commissioner should be limited to cases in which the Commissioner "has reasonable grounds to believe that the organization is contravening [the Act]" ("Bill C-6," 2000, Clause 18(1)). Given the invisible nature of privacy violations, audits are an important tool for obtaining compliance, and should be conducted even when no complaints have been received. These measures must be fulfilled, not ignored, if the aim of the legislation is to offer Canadians meaningful and workable privacy protection.

A Troubling Shot of E-Privacy: the Government's Failure to Address the Problem

As I have illustrated, Bill C-6 is arguably over-reaching in its application and does not go far enough in extending privacy protection outside the domain of commercial activity. It was not designed to punish or cripple the business community. This is precisely because when government action is perceived by businesses to be harmful to their interests, they react by cutting back production and deferring or canceling investments. The reaction is automatic, triggered by a change in the environment in which business operates, and to the extent that it means unemployment and economic slowdown, the reaction sets out to punish a government, which trespasses beyond the line of business tolerance (Brooks, 1989, 49). As a result of this situation, not only are incentives and disincentives used to persuade the business community to behave in ways desired by the government but there is also a special sensitivity of public officials to business interests.

The discussion paper, which preceded the legislation, exemplifies the government's sensitivity towards the conditions necessary to ensure business performance. The discussion paper states:

> Legislation that strikes the right balance between the business' need to gather, store, and use personal information and the consumer need to be informed about how that information will be used ... is an important element of building the consumer trust and the market certainty needed to make Canada a world leader in electronic commerce (Industry Canada, 1998, para. 1).

It is also worth noting that the discussion paper uses the words "consumer," "business" and "industry" seventy-eight times, as opposed to a total of ten occurrences of the word "citizen". However, the focus on economic stability in Bill C-6 does not exist in isolation. I would argue that the government and private businesses have a fundamental interest in economic stability, which is now part of a larger shift in governance.

Traditionally, we view government as a vehicle to advance the public good. From this point of view, privacy is an essential part of what Professor Ursula Franklin calls the indivisible benefits of governance: justice, dignity, freedom, clean air and equality (Franklin, 1996, para. 5). However, some private institutions, such as large-scale corporations, exert such a heavy influence on the public that policy makers increasingly see government less as a vehicle for the preservation of meaningful data protection and more as a vehicle to divvy up divisible benefits; things that benefit one set of private interests at the expense of another. In my mind, e-commerce is a good example of this dynamic.

Canada's economy is based on the principle of the primary markets. In this context the government can be seen as a supplier of services, whereby "good" government is perceived as efficient, cost-effective, and, most importantly, competitive in the global information economy (Doern and Phidd, 1983, 54). These principles are part of the need for larger efficient entities, a theme in Canada's overall policy framework, which places a high value on the realization of a goal at the least cost (Doern and Phidd, 1983, 54). From this perspective, the government has extolled the need to promote unfettered access to, and the manipulation of, a wide range of personal information, in order to achieve its goal to promote economic growth, producing optimum returns and strengthening its domestic and international market opportunities for Canada, as e-commerce becomes widespread. The conceptualization of privacy as a good in

itself, a fundamental human right, or indeed a right that is the foundation for many other fundamental human rights, is not part of the equation.

Our privacy, once an integral part of our human dignity and autonomy, is a barrier to efficiency and competitiveness and has led to a situation where personal information has simply become a commodity that can be bought, sold or bartered. By framing privacy in the context of e-commerce, Bill C-6 begs the privacy question. The drafters intended to create a regulatory scheme, which will ensure that companies will continue to be able to collect and use personal information to generate profits and remove inefficiencies. The power that comes with information can be abused, especially if efficiency and cost reduction is valued more than the human beings the information describes (Thompson, 2000, p. 13).

Democratic societies are notoriously inefficient. Nonetheless, we accept those inefficiencies because democracy is the best way to maintain some degree of individual freedom. However, the fact that business interests occupy a privileged position within the policy-making system, leads many to question whether policy making can still be controlled democratically.

The primary consideration is that in a democracy, legitimacy lies with the citizenry. Canadian citizens have a right, by statute, to decide what information they want and need in order to most effectively exercise their responsibilities of citizenship. As a result, the overarching purpose of access to information legislation is to ensure that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry (Mitchinson, 2000, para. 4). However, parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on, nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view (Mitchinson, 2000, para. 4). Access laws operate on the premise that politically relevant information should be distributed as widely as possible. Although the values underlying the laws are laudable and embraced proudly and enthusiastically by governments that introduce them, commitment to these values is hard to sustain over time (Mitchinson, 2000, para. 5).

Recommendations: Finding the Right Balance

After reviewing Bill C-6 and its framework, can legislation adequately protect an individual's privacy? The short answer is no. The long answer is that while a legislative approach to the protection of privacy is fraught with enough uncertainties and obstacles, it is crucial that the Canadian government does not throw what is meant to be broad privacy protection under the narrow legislative umbrella of e-commerce promotion, because it misleads the public and industry about the nature of the legislation, and it risks narrowing the rights and obligations in question well beyond what was originally intended.

It is unclear why two completely separate and distinct legislative inniatives have been combined, and what benefits may be derived from them. This gap may have been acceptable in the context of a self-regulatory code, but it is not acceptable in government legislation. In order to achieve the goal of privacy protection, it is not enough to design and implement a system, simply because no single approach to the resolution of the problems is viable. Formulating rules in this area is necessarily a risky process that should be conducted with considerable caution.

As I have set out to illustrate, much of the dialogue about information privacy is a balancing act, and a new legal framework awarding the entitlement of information to the individual, rather than the current system, which awards the entitlement to the business community, is necessary.

The framework for discussing privacy issues now encompasses a private sector commercial perspective, in addition to the traditional human rights approach. A shared responsibility for the management of personal information will be essential, involving government, business community and consumers. Only through shared responsibility, sustained by the business community through a culture of privacy, and strengthened by the voice of consumers, can personal information become a protected, managed and valued resource. This series of recommendations sets out to strike that balance in favor of the individual, by employing a combination of approaches that are most likely to succeed because they are inter-related, mutually supportive, and set the default rule at privacy for users. They are based on a framework that will give all three parties — consumers, businesses, and government — incentives for action towards protecting personal information in the marketplace.

OBLIGATIONS

RECOMMENDATION 1:

RE-DEFINING CONSENT

An essential element of privacy is the question of consent. Careful consideration must be given to the definition of consent in order to ensure that the privileges, which flow from it, are granted by fully informed and free individuals.

Consent, however, has different interpretations. Generally, the consumer, privacy advocates and the Privacy Commissioner see consent in terms of "informed consent". This is interpreted to mean a clear understanding of the reasons for the collection of information and the uses to which it will be put, being free from any form of "coercion" (Geist, 2000, para. 4). Many in the business sector also appear to subscribe to the concept of "informed consent," however they tend to interpret it as being given by an entry into a transaction (Geist, 2000, para. 4). In other words, purchase a product, for example, and you have automatically agreed to have your personal data used for profit in ways you might never have imagined.

A clear definition of fully informed consent must be expressed within the legislation and require that online vendors take reasonable steps to ensure that agreement to contract is fully informed and intentional, by making sure that their customers are:

- Aware that permission to collect, store, and use personal information is being requested; and
- Fully cognizant of the manner in which the information will be collected; and
- Informed of the manner in which the information will be used.

Consent should be obtained in writing, wherever feasible, and it should not exist in perpetuity but be given a clear limitation period, appropriate for the type of information collected (Geist, 2000, para. 4). Businesses should be required to obtain consent for selling or sharing information with its own departments and affiliates, as well as non-affiliated organizations. Moreover, certain types of personal information deserve special protection, such as children's and health information (Steeves, Privacy: A right or a commodity? para. 10). For example, there should be specific provisions to ensure that parents and guardians have control over the process of giving consent to the collection and use of their children's information.

In addition, there must be an "opt-in" mechanism, as opposed to giving individuals the right to request that the organization refrain from collecting or using their personal information. The legislation should include a provision whereby individuals who do not consent to release their personal information should not be denied goods or services or penalized in any way, unless the information is necessary for the provision of those goods or services (Geist, 2000, para. 4).

Unless the entire process is fully open and transparent, consent given will be less than fully informed and accordingly not a meaningful method of protecting the individual's right to control his or her personal information.

RECOMMENDATION 2:

PURPOSE OF COLLECTION AND NOTIFICATION

In keeping with the desire to give individuals as much control as possible over their personal information, the definition of purpose of collection must be carefully drafted to ensure that the need of organizations to collect and use information is balanced against the right of the individual to enjoy information privacy. In particular, the legislation should require that organizations not only be limited to only the collection of personal information, which is necessary to support the current or planned activities, but they must also set out the specific purposes for which they will use the information they collect (Cavoukian,1998, para. 5). It is in this sense that drafters must guard against meaningless and vague definitions of purpose, such as "to manage our relationships with our customers" (Cavoukian,1998, para. 5). If the organization is collecting the information to use it for micro targeting, or to sell it to third parties, then that must be clearly stated at the time consent is requested.

In addition, the individual should have the right to challenge the appropriateness of the purpose stated. The legislation should clearly state that the individual must be free to refuse to consent to the collection and use of his or her personal information for inappropriate purposes, without losing access to goods or services (Cavoukian,1998, para. 6).

Furthermore, whenever personal information is collected, the individual should be informed of the following:

- What information is being collected and why;
- The legal authority for the collection, if relevant;
- How the information will be used and disclosed;

- Whether the provision of information is voluntary or mandatory;
- The consequences of providing or withholding the requested information; and
- Who to contact with questions about the collection, use or disclosure of the information.

If personal information is collected indirectly form another source, the individual should still be informed about the collection, where possible. Notification must include a description of the sources of the information and the reason for using indirect sources (Cavoukian,1998, para. 7).

RECOMMENDATION 3:

INFORMATION PRIVACY AS A RIGHT

The value of privacy as a human right must be made explicit, and the legislation should incorporate and adopt the definitions of 'privacy' and 'information privacy' set out in this major research paper.

The response of the Canadian government to the changing nature of privacy invasion has been disappointing. The government has steadfastly refused to recognize privacy as a human right or to create the overarching privacy legislation, which would address emerging invasive practices in a cohesive manner. Instead, under the banner of a competitive a global information economy, the government has made clear policy choices supporting the re-definition of the right to privacy, so that it is valued in so far as it is facilitated by commercial activity, and, thus, given only minimal protection in non-commercial circumstances.

Advances in new information technology should not be implemented at the expense of diminished privacy (Steeves, Privacy: A right or a commodity? para. 14). By no means should individuals have to spend money to maintain basic and existing levels of privacy. The government as well as those who plan to introduce new information technologies and services should bear the responsibility for ensuring that Canadians are provided with the means for maintaining privacy at no extra cost.

The conflict, which has resulted over the appropriate roles of the State and the market has led to a situation where mediation between individual citizens and the State is essential in the face of a rising rights consciousness. With this in mind, a definition of privacy that protects our most fundamental social and political values must be articulated within the scope of the law, and to do this, we must move beyond the limiting language of the marketplace and embrace a human rights

perspective (Steeves, Privacy: A right or a commodity? para. 11). This means that privacy rights should be legally recognized on their own merit, not as enablers of electronic commerce. Placing privacy in a rights context is important, especially because there is a need to balance individual control against other, competing interests (Steeves, Privacy: A right or a commodity? para. 11). The language of rights and responsibilities reinforces the individual's personal responsibility to become informed about the use of his or her personal information.

The government's success in creating an appropriate regulatory mechanism will be tested against the strong desire for control expressed by the public. When it comes to the protection of personal information, the majority of the public requests a legal response, which will shift control from the organization to the individual as much as possible.

POWERS

RECOMMENDATION 4:

REGISTRATION OF INFORMATION PRACTICES

Some privacy analysts have suggested that the government turn to a technological solution to the Internet privacy problem, something similar to what is known as the Platform for Privacy Preferences technology (P3P). P3P is a protocol that was developed by the World Wide Web Consortium (W3C), with funding from many private sector organizations. It is said by some analysts that if constructed, P3P can create a cyberspace architecture, which will grant people true control over their information in the sense that users would configure their privacy preferences to protect privacy according to the value that they attach to it (World Wide Web Consortium, 2002, para.1).

Those in favour of P3P say that this will be accomplished by creating a language in which Web sites describe their privacy policies in a machine-readable format that allows users to describe their privacy preferences and match them against the machine-readable policies of various Web sites (World Wide Web Consortium, 2002, para.1). However, while it may sound like this technology is balanced in favour of the consumer, P3P has a number of shortcomings.

For each and every data type that P3P defines, end users have to decide whether or not to automatically grant access to their information (World Wide Web Consortium, 2002, para.2). In

many cases, the end users may have different preferences from the ones that the P3P technology defines, in which case new terms would have to be specified out into a seemingly endless universe of preferences (World Wide Web Consortium, 2002, para.3). Individuals should not be required to negotiate or choose among Fair Information Practices. This complexity makes it extremely difficult to develop a comprehensible graphical user interface.

A more significant shortcoming with P3P technology is that it has been criticized for falling short of accepted Fair Information Practices. It presumes no cohesive set of privacy standards, such as the OECD Privacy Guidelines, which would provide a simple, predictable, uniform environment for online transactions. Instead, it is really only focused on the collection limitation, use limitation, and openness principles (World Wide Web Consortium, 2002, para.5). It has almost nothing to say about the other five principles. This is due to the fact that P3P merely describes the terms of data exchange, but once the exchange has taken place, P3P's role is basically over. As a result, P3P cannot ensure data quality, data security, if data will be shared with third parties, or if access to a user's information will be granted. While P3P does allow sites to make general statements about third party use limitations, and user access to information, it cannot (and this is the crux of the problem with P3P) enforce these statements. In other words, P3P has nothing to do with the accountability principle, which holds data collectors to their stated policies.

As outlined, P3P has too many shortcomings that it would be inappropriate to build this technology into the framework of the legislation and, thus, a workable definition of privacy protection for Canadians. Consequently, there is still no effective means of enforcement for Bill C-6. No real effort has been undertaken to begin auditing or conducting oversight to ensure that the privacy policies posted are being followed.

Part of the problem with online privacy is that most companies do not have a plan to institute a process for identifying, analyzing and resolving privacy issues both at a reactive level and at a strategic level within their respective organizations. Take Mike Gurski's example of Guess.com, the distributors of fashion wear like Guess jeans. Their privacy policy is above average, clear and less than two pages. Despite this, Gurski points out that the company had a Web site security flaw that exposed 200,000 credit card numbers, pointing out some chronic and fundamental problems.

Gurski's interest in Guess did not stem from the fact that a 19-year-old computer geek found a way through the Web to access more than 200,000 credit card numbers, with names and expiry dates. What he did find interesting was the difficulty that this young man had in informing Guess of its problems. After getting bumped to voice mails, the 19-year-old sent a number of emails to the only email contact address that was listed on the privacy policy page, only to find that the address was not active (Gurski, 2002, para. 11). According to Gurski, he had to go to Security Focus Online, a security company, which in turn contacted Guess and then had to provide a demonstration of the leak before the company would respond. A few weeks passed before the problem was finally solved.

Guess disputes the young man's account of trying to contact it regarding the security breach (Gurski, 2002, para. 12). In my mind, there seems to be a lack of accountability and internal processes that can handle a privacy complaint such as a security breach. Like Gurski, I think that this apparent lack of accountability for privacy and security that is contributing to the e-privacy chill.

I give you these examples to sketch out the e-commerce privacy landscape in which it is surprisingly easy to show gap breakdown in privacy leadership. Online vendors and intermediaries must respect the privacy principles set out in the CSA International's Model Code for the Protection of Personal Information (now law). With this in mind, the legislation should look for alternative solutions that would provide a more central direction to the information policies of companies, who use the Web to conduct business.

It seems that the Information and Privacy Commissioner (IPC) of Ontario, with the help of Price waterhouse Coopers and Guardent, is searching for these alternative solutions. It has developed a tool, known as the privacy diagnostic tool (PDT), which is designed to help you take a company's privacy pulse. It is based on each of the fair information practices and, accordingly, is divided into sections, one on each of these practices (Mitchinson, 2002, para. 24). Each section provides a definition of the term, and identifies potential risks in not following the practice. Then, there are two sets of questions in each section. One set relates to what every company needs to do in order to implement the principle in question; the second set of questions relates to best practices—policies for ideal privacy protection (Mitchinson, 2002, para. 32). Once you get to the end of the series of questions, the PDT will generate a printed report to let

you know what privacy areas your business is strong in, and where it still needs work (Mitchinson, 2002, para. 33).

Ultimately, the value of the PDT is that it helps senior executives to make fully informed policy and system design decisions based on an understanding of privacy risks and of the options available for mitigating them (Mitchinson, 2002, para. 33). Once in place, one way to make certain that these policy decisions are adhered to is by appointing a chief privacy officer, with dedicated responsibilities to ensure that personal information management processes are soundly designed and effectively managed.

In my opinion, the legislation must also make it mandatory for organizations to register their information policies with a government oversight agency, which works in partnership with the office of the Privacy Commissioner. Registration is an important component of any data protection regime. It is especially important for the enforcement authority to be aware of those companies whose activities bring them within the scope of the legislation (Cavoukian,1998, para. 5). It is also important in terms of assisting such companies in developing and administering data protection processes which meet the requirements of the Act, thereby maximizing compliance with the legislation. Through registration, "high risk" businesses can be identified and monitored more closely than low risk users and inappropriate or inadequate practices can be identified and corrected.

There has never been a time of greater need for independent oversight bodies and privacy commissions, because never before have the operations of government been so complex, so much a part of the fabric of society. As a result, the government agency should take on the role of an ombudsman, ensuring that Web sites make available a privacy policy that is easy to find and that clearly states how and when personal information is collected. The process should not be overly burdensome for businesses, but it should involve filing a statement, which includes detailed information as to the nature of the information being handled, and how it is collected, stored, processed, transported, traded or otherwise disclosed, and the purposes of these activities (Geist, 2000, para. 4). The oversight agency must have sufficient resources to review these filings, and to follow-up with businesses where the filing indicates a potential for non-compliance. Such a follow-up could range from a telephone call to a full-scale audit.

Assuming that the registry is open to the public, it can serve as a resource centre for interested parties to learn about data protection practices in the private sector, and to assist in the

enforcement of the Act. The goal of registration should be to establish a privacy agency with the expertise, competence and resources to provide individuals with easy access to information on organizational practices and policies, in turn, acting as a voice for privacy within the administration (Geist, 2000, para. 4). At the end of the day, the real measure of the legislation's success will be the extent to which businesses have been able to move beyond simply complying with the rules, and have embraced a culture of privacy within their organization. The proper management of personal information must become second nature in order to be truly and consistently effective.

RECOMMENDATION 5

CONSUMER-FRIENDLY COMPLAINTS PROCESS

As currently drafted, the legislation provides no easy way for complainants to achieve justice and/or obtain redress, should the Privacy Commissioner's recommendations go unheeded and should the Commissioner be unwilling to take a complainants case to Court. Organizations wishing to push the limits of the legislative regime can do so in the comfortable knowledge that only the most determined and financially able individuals will pursue them in Court (Thompson, 2000, p. 13).

If a small expert tribunal were established with the power to provide rulings, upon request, as to the application of the legislation in specific circumstances (e.g. what constitutes reasonable efforts to inform?) then organizations would be more certain of their obligations and citizens would be more certain of their rights. Leaving the resolution of such issues to the federal Court means that many will go unresolved, while significant resources will be spent on those that are taken to Court. This is neither an efficient nor an effective way to proceed. For these reasons, it would be more beneficial to implement a regime in which enforcement and redress can be pursued through an expert tribunal, which is more accessible and less costly than the federal Court.

In brief, the tribunal should ensure that the complaints procedure is easy and straightforward. The process should be understandable, accessible/affordable, fair and not unduly lengthy (Thompson, 2000, p. 13). The expert tribunal should also be allowed to tailor punitive damages to the circumstances before it, so as to effectively punish wrongdoers and deter organizations from such privacy violations.

The legislation should also include specific protection for corporate "whistle blowers" to ensure that employees, who reveal that their employers are misusing personal information, do not lose their jobs or be punished in any way (Thompson, 2000, p. 13). Given the hidden nature of privacy violations, it is especially important that employees and others be protected from retribution in the event that they disclose non-compliant practices to the Privacy Commissioner.

RECOMMENDATION 6:

POWERS OF ENFORCEMENT BODY

While there is no way to restore privacy once personal information has been improperly used, a means is essential to ensure that the improper collection, retention, use and disclosure of personal information must not occur without consequence.

It should be mandatory that results of all investigations/audits (including all consent agreements of voluntary compliance, statistics on the number of such agreements, a summary of their contents, the names of the parties involved, and whether compliance has occurred) be publicly available (Mitchinson, 2000, para. 5). More importantly, to ensure the complaints process functions effectively, the Privacy Commissioner must be obligated to:

- Publish the name of all organizations that break the rules
- Order an organization that does not obey the rules to compensate persons who are harmed because the organization did not obey the rules
- Order an organization that does not obey the rules to pay a fine

Legislators should also consider giving the Privacy Commissioner the power to:

- Require an audit to make sure organizations are obeying the rules
- Require organizations to have an independent third party—an oversight agency—review their information policies

The legislation should introduce a system to compensate those who suffer harm as a result of the improper collection, retention, use and disclosure of personal information (Mitchinson, 2000, para. 5). It should make it clear that nothing in the law prohibits individuals from using other remedies for information privacy violations, including:

- Criminal charges
- Civil remedies

In order to be effective, criminal offences must carry penalties that are of a magnitude sufficient to deter those engaged in this profitable industry, and these penalties must apply to both companies and responsible individuals within those companies. The application of criminal sanctions should be rare, in turn, allowing their mere existence to give the legislation the clout it needs in order to obtain compliance with the law.

DISTRIBUTION OF POWERS AND RESPONSIBILITIES

RECOMMENDATION 7:

PRIVACY IMPACT ASSESSMENTS

The legislation should include a provision requiring companies developing new information technologies to conduct a privacy impact assessment before the new technologies are made available to the public. The assessment should be filed with an oversight agency by companies developing and/or selling the technologies and where necessary by companies purchasing the new information technologies (McHardie, 2001, para. 5). The oversight agency should be empowered to receive, review, and evaluate these assessments. It should also be empowered to demand further assessment where it considers appropriate, as well as determine the form of the assessment, the questions to be answered, and the issues to be addressed.

Privacy impact assessments should be completed as early as possible in the process of developing the technology and in any case prior to marketing. More importantly, the assessment procedure should be developed through broad-based public consultation, making it available to the public for review and comment, in order to strengthen a partnership approach between government, industry and the consumer sector (Thompson, 2000, p. 13).

The process of completing and filing a privacy impact assessment should be minimally burdensome. However, the rules governing personal information should be clear and able to protect the individual's right to information privacy as new technologies emerge.

Ultimately, the negative impact of various technologies on privacy can only be averted by instilling a culture of privacy within the business community. "Instilling a culture of privacy" means that it is essential to attempt to identify these implications and address the public's growing concern about privacy protection as early in the process as possible, through

consultation and analysis of the public's concerns (Cavoukian, 1998, para. 10). If privacy concerns can be identified up-front, it will be possible to incorporate technical and policy solutions into the design and implementation of new information technologies and services. It is far more difficult and expensive to address problems, which arise once a system is fully operational.

RECOMMENDATION 8:

EDUCATION

The legislation should state that public education on privacy is a priority, as effective protection requires that Canadians are aware of their privacy rights and know how to protect themselves.

There is wide recognition of a lack of awareness and confusion among the public with regards to the benefits and services that are and will be available on the Web. This is coupled with an equal lack of awareness concerning their privacy rights, how to obtain those rights, the consequences of providing personal information, and the protective measures which are available. This leads to vague but real concerns, which could prejudice the success of our online world. Therefore, there is widespread agreement that education of the public on these matters is both essential and urgent in order to reduce concerns and because of the rapid growth of the Web. This point cannot be overstated—if citizens are unaware of their rights or how to exercise and enforce them, then the rights lose effectiveness.

In addition, it must be recognized that both employees and businesses need to be educated on their responsibilities in regards to privacy protection. We need to make loss of privacy the exception, not the new way of doing business, and we need to have an attitudinal change that both recognizes the threats and places limits upon them.

Businesses have major responsibilities in this area (McHardie, 2001, para. 5). Many private sector organizations are already engaged in education programs, not only for their customers but also for their employees. Moreover, the media is also seen as having a significant role to play. Massive advertising campaigns are not recommended, although periodic public awareness campaigns, which could take many forms, are recommended. The use of information centres, including public and academic libraries, for the distribution of materials and brochures should be

considered as another avenue. Brochures and publications can be directed at different audiences, including the public at large, schools and universities, and customers of businesses. Other suggestions include a publicly funded national toll-free privacy "hotline" for consumers.

It is also recognized that consumers, themselves, must take the initiative to absorb educational materials provided to them, to shop around for the best balance of services and privacy protection, and to understand their own responsibilities with regards to privacy matters (McHardie, 2001, para. 5). Equally, businesses must also take the initiative to inform customers of potential privacy problems related to their products and services and not hold back until a crisis occurs.

The legislation should state that responsibility to fund privacy education is a responsibility, which is shared by the government, private companies and organizations, and industry associations. The Privacy Commissioner should accordingly be authorized to enter into strategic partnerships in order to fulfil his or her educational mandate.

The importance of privacy education cannot be overstated. Individuals will only be able to take personal responsibility for becoming informed if they have easy access to high quality informational and educational materials. At present, the technological capabilities for profiling are unfamiliar to many people. However, if consumers are adequately informed about profiling, as well as other practices that raise privacy concerns, they can pressure the government and politicians to be aware of these issues and act accordingly (McHardie, 2001, para. 5).

RECOMMENDATION 9:

WHAT CAN CONSUMERS DO?

For those consumers who wish to have greater control over the use and circulation of their personal information, I would like to suggest the following initiatives:

Ask to see a business's privacy or confidentiality policy. Assess it against your expectations of how you want your personal information handled. If the policy does not meet your expectations, contact the business and inform it of your expectations. If no policy exists, inform the business that you expect respectful and fair handling of your personal information. Give only the minimum amount of personal information needed to complete a transaction. If you are in doubt about the relevance of any information that is requested, ask questions about why it is needed, and ask that all of the uses of the requested information be identified.

A Final Word

Anyone today who thinks the online privacy issue has peaked is greatly mistaken. We are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope.

The challenge of any privacy-protection initiative, it seems to me, is to separate the uses of surveillance technologies from their abuses. In the end, that is why government participation in privacy protection is vital: even if privacy laws are not entirely effective they are the foundation for a society that remains mindful of privacy issues.

The years ahead are going to be challenging as governments attempt to implement online policies and at the same time grapple with the implications of these initiatives. These recommendations are the first step in the process to make legislation more effective—it is intended to function as a redefinition of what information is private. This is a context-sensitive redefinition, which extends beyond the Web—we are living in an age where vast stores of data about every person in this country are freely available. The above recommendations lay the groundwork for this new understanding of "public" and "private" depending on who has access to the information, how it is used, and how much control the individual has over it, but there is still much to be done. We must alter our understanding of "public" and "private" from how these terms were meant, to what those terms mean now, when our technological architecture has reached a place that no one could have envisioned when the rules were created. Unquestionably, Canada needs a privacy Bill, since privacy is not just an individual interest, but is first and foremost a political value of the highest order. All Canadians deserve the same legislated rights and protections with respect to their personal information, and the federal government has acted where provinces (with the exception of Quebec) fail to do so (Lawson, 2000, para. 4, 5).

Privacy, as a subject of legislation, is not exclusively either a federal or provincial concern. It is an area of shared responsibility, like human rights legislation, and legislation in this area should preferably be, if not identical throughout the country, at least based on the same underlying principles, especially with respect to the private sector (Lawson, 2000, para. 4, 5). Given the ease with which information crosses boundaries, cooperation between the federal and provincial governments on this issue is essential if we are to meet the concerns that Canadians

have expressed over privacy. Citizens do not want to be deprived of protection simply because their provincial government failed to act (Lawson, 2000, para. 4, 5). Moreover, they do not want a patchwork of different standards and regimes across the country, especially when the problem of data flows so often crosses borders (McHardie, 2001, para. 6). This problem is not a local issue: it transcends provincial, even national boundaries. Its solution must similarly transcend provincial and national boundaries.

The tension between technology and privacy can be minimized if privacy safeguards are a key consideration upfront, rather than as an afterthought. As the Web and use of computers continues to grow, the importance of this process cannot be underestimated—and it requires more direction from our government than a simple hope that ultimately, everything will work itself out (McHardie, 2001, para. 7).

Individuals have a dangerously naïve sense of privacy when they use these communication technologies, perhaps because access is conducted in the relatively anonymous environment of interaction between an individual's own personal computer and an unseen, faceless communications server (McHardie, 2001, para. 3). Whether privacy will survive in our society as a human right will significantly depend on public recognition and activism. What we do not have in Ontario, and this is a common problem in many other jurisdictions as well, are internal champions for freedom of information. People in a position of influence and power who are prepared to commit themselves to the values inherent in the law and to do so publicly and proudly.

This paper has identified the structural elements of a comprehensive privacy architecture, one which could provide appropriate levels of control and choice for individuals, depending on the context in which they entered into different institutional relationships with government or private sector organizations. It also has the courage to take a stand and suggest ways in which the government, consumers, and businesses can help protect personal privacy. The ball is now squarely in the court of informed consumers, non-profits, and legislators to question the framework at hand. The only question now is will the public and, more significantly, will Canada's policy-makers have the courage to follow such recommendations, ensuring that privacy rights, not market excess, become the default in cyberspace?

Bibliography

An internet privacy primer: Assume nothing. (2001, August). A collaborative paper by the Information and Privacy Commissioner of Ontario and Microsoft Canada Co. Retrieved October 5, 2001, from http://www.ipc.on.ca/english/pubpres/papers/primer-e.htm

Anderson, Heidi. (2000, April). Cookie crumb trails: How sites know your identity & can track your Web travels. Smart Computing, 8(4), 37-39.

Ayed, Nahlah. (1998, November 23). CRTC begins hearings on new media. Retrieved October 5, 2001, from Canoe Web site: http://www.canoe.ca/TechArchive/981123_crtc.html

Bennett, Colin J. (1996). Regulating privacy in Canada: An analysis of oversight and enforcement in the private sector. Retrieved October 5, 2001, from http://sitka.dcf.uvic.ca/poli/bennett/research/regpap.htm

Berton, Paul. (2000, January 29). The surveillance society. Retrieved October 5, 2001, from CNEWS Web site: http://www.canoe.ca/CNEWSFeatures0001/29_camera.html

Bill C-54 [Electronic version]. (1997-1998). Retrieved October 5, 2001, from Canada, Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/90052bE.html#5

Bill C-6 [Electronic version]. (2000, April 13). Retrieved October 5, 2001, from Canada, Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II, http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_coverE.html

Boston Consulting Group (BCG) Media Releases. (1999, April 22). E-commerce statistics. Retrieved October 5, 2001, from http://www.bcg.com/media_center/media_press_releases.asp

Bounds, Wendy & Silverman, Rachel. (2000, November 15). Crisis of confidence. Retrieved October 5, 2001, from ZdNet Web site: http://www.zdnet.com/ecommerce/stories/main/0,10475,2654115-2,00.html

Bradley, Helen. (2000, April). Beware of Web bugs and clear GIFs. Smart Computing, 8(4), 40-42.

Branscomb, Anne. (1996, February 15). Interviewed in CIO magazine. Retrieved October 2001, from http://www.cio.com/archive/cio_021596_qa.html

Brooks, Stephen. (1989). Public policy in Canada: An introduction. Toronto: McClelland & Stewart Inc.

Canada Gazette. (2000). Canadian Privacy. Retrieved October 5, 2001, from 7 http://canada.gc.ca/gazette/gazette_e.html

Cavoukian, Ann. (1998, January). Data mining: Staking a claim on your privacy. Retrieved February 9, 2002, from http://www.ipc.on.ca/english/pubpres/sum_pap/papers/datamine.htm

CRTC News Release. (1999, May 17). CRTC won't regulate the internet. Retrieved October 5, 2001, from http://www.crtc.gc.ca/ENG/NEWS/RELEASES/1999/R990517e.html

De Bony, Elizabeth. (2000, July 27). EU gives final OK to U.S. safe harbor privacy plan. Retrieved October 5, 2001, from http://www.idg.net/crd_privacy_205543.html

Diffie, Whitfield & Landau, Susan. (1998). Privacy On the Line: The Politics of Wiretapping and Encryption. Cambridge, MA: MIT Press.

Dodd, Jeff. (2000, April). Us VS. Them: How U.S. privacy concerns compare with rest of world. Smart Computing, 8(4), 10-12.

Domain Stats. (1999, November 29). Number of .com domains. Retrieved October 5, 2001, from http://www.DomainStats.com

Doern, Bruce and Phidd, Richard. (1983). Canadian public policy: Ideas, structure, process. Toronto: Methuen publications.

E-commerce and privacy leadership from a policy and legislative perspective. (2002, March). A speech by Mike Gurski Senior Policy/Technology Advisor, Audit and Information Systems Workshop in Toronto. Retrieved July 5, 2002, from http://www.ipc.on.ca/english/pubpres/speeches/0302mg.htm

Electronic Privacy Information Center. (1998, June). Surfer beware II: Notice is not enough. Retrieved October 5, 2001, from http://www.epic.org/reports/surfer-beware2.html

Farmer, Melanie. (2000, July 27). Toysmart suspends auction of customer list. Retrieved October 5, 2001, from CNET news Web site: http://news.cnet.com/news/0-1007-200-2359462.html

Farwell, Jennifer. (2000, April). Online profiling: Smart marketing tool or menace to privacy. Smart Computing, 8(4), 24-26.

Federal Express. (2001, January). Privacy Policy. Retrieved October 5, 2001, from http://www.fedex.com/us/privacypolicy.html

Fitzpatrick, Chris. (2002, April 24). Paranoia over Privacy. Retrieved July 6, 2002, from, http://www.alternet.org/story.html?StoryID=12949

Franklin, Ursula. (1996, September 19). Stormy weather: Conflicting forces in the information society, closing address at the 18th international privacy and data protection conference in Ottawa. Retrieved October 5, 2001, from http://www.privcom.gc.ca/english/02_05_a_960918_05_e.htm

FTC announces proposal to clarify how the law will apply to advertising and commercial transactions on the internet.(1998). Retrieved October 5, 2001, from Federal Trade Commission Web site: http://www.ftc.gov/opa/1998/9805/interbus.htm

Gandy, Oscar. (1993). The Panoptic Sort: A Political Economy of Personal Information. Boulder, CO: Westview Press.

Geist, Michael. (2000, November 10). Privacy compliance is the new priority. Retrieved October 5, 2001, from Globe and Mail Web site: http://www.globetechnology.com/archive/gam/News/20001110/ECGEIS.html

Government of Canada: Senate Committee Studying Bill C-6. (1999, December). Connecting Canadians. Retrieved October 5, 2001, from http://www.connect.gc.ca/en/sp/1328-e.htm

Hatlestad, Luc. (2001, January 16). Online Privacy Matters. Retrieved October 5, 2001, from Red Herring Web site: http://www.herring.com/index.asp?layout=story&channel=50000005&doc_id=17 60015576

Industry Canada. (1998). Building Canada's information economy and society: The protection of personal information. Retrieved October 5, 2001, from http://ecom.ic.gc.ca/english/privacy/632d1.html

Junkbusters. (2000). How Web servers' cookies threaten your privacy. Retrieved October 5, 2001, from http://www.junkbusters.com/cookies.html

Kang, Jerry. (1998). Information privacy in cyberspace transactions. Stanford Law Review, 50(4), 1193-1294.

Macavinta, Courtney. (2000, January 25). Privacy fears raised by DoubleClick. Retrieved October 5, 2001, from CNET Web site: http://news.cnet.com/news/0-1005-200-1531929.html

McCullagh, Declan. (1999, November 5). Is TRUSTe trustworthy? Retrieved October 5, 2001, from Wirednews Web site: http://www.wired.com/news/politics/0,1283,32329,00.html

McHardie, Daniel. (2001, January 2). Internet privacy law now online. Retrieved October 5, 2001, from Globe and Mail Web site: http://news.globetechnology.com/servlet/GAMArticle.html

Mitchinson, Tom. Privacy in Ontario: The future of business. (2002, March). A presentation to the Greater Barrie Chamber of Commerce. Retrieved July 5, 2002, from http://www.ipc.on.ca/english/pubpres/speeches/052602tm.htm

Mitchinson, Tom. Balancing public access and accountability with the right of privacy. (2000, March). New Directions in Professional Regulations Conference. Retrieved October 5, 2001, from http://www.ipc.on.ca/english/pubpres/speeches/pubacc00.htm

Nelson, Michelle. (2000, April). Web tracking is watching you: Log files & cookies record your actions & anticipate your interests. Smart Computing, 8(4), 20-23.

Nizer, Louis. (1941, February). The right of privacy, a half century's developments. Michigan Law Review, 39, 526-560.

Noack, David. (2000, May 23). Feds want to regulate internet privacy. Retrieved October 5, 2001, from APB News Web site: http://www.apbnews.com/newscenter/internetcrime/2000/05/23/privacy0523_01.html

Privacy Commissioner of Canada. (2001). A private sector privacy law. Retrieved October 5, 2001, from http://www.privcom.gc.ca/english/02_06_e.htm

Privacy and human rights: An international survey of privacy laws and developments. (1999). Retrieved October 5, 2001, from Privacy International Web site: http://www.privacyinternational.org/survey/Overview.html

Privacy and the Canadian information highway. (1994). Retrieved October 5, 2001, from http://www.privacy.org/pi/countries/canada/report.html#A1

Privacy protection on the way: Bill C-6 finally passes! (2001). Retrieved October 5, 2001, from http://www.piac.ca/april00.html

Radin, Margaret. (1993). Reinterpreting Property. Chicago: University of Chicago Press.

Reiman, Jeffrey. (1995) Driving to the Panopticon. Santa Clara Computer and High Tech Law Journal, 27, 37-38.

Rifkin, Jeremy. (1992). Biosphere Politic. New York: Harper Collins.

Sherwin, Greg & Avila, Emily. (1999, November 26). Privacy or piracy? Retrieved October 5, 2001, from ClickZ Network Web site: http://gt.clickz.com/cgibin/gt/cz/cz.print.me.html?article=1001

Singleton, Solveig. (1999). Privacy vs. innovation: Self-regulation: Regulatory fad or market forces? Retrieved October 5, 2001, from http://www.cato.org/pubs/wtpapers/990507report.html

Steeves, Valerie. (2001). Humanizing cyberspace: Privacy, freedom of speech, and the information highway. Retrieved October 5, 2001, from the Human rights research and education centre: http://www.uottawa.ca/hrrec/publicat/cyber95e.html

Steeves, Valerie. (2001). Privacy: A right or a commodity? Protection of privacy is endangered by new technologies. Retrieved October 5, 2001, from Canadian Centre for Policy Alternatives Web site: http://www.policyalternatives.ca/publications/articles/article270.html

Thompson, Robert. (2000). Industry vs. privacy. E-Business Journal: Strategies and Solutions for the Digital Economy, 2(1), 12-14.

TRUSTe. (1999). Resolution process. Retrieved October 5, 2001, from http://www.truste.org/consumers/users_how.html

U.S. Department of Commerce. (1999). Safe harbor: Safe harbor overview. Retrieved October 5, 2001, from http://www.export.gov/safeharbor/SafeHarborInfo.htm

Westin, Alan F. (1967). Privacy and Freedom. Atheneum, New York: 1967.

World Wide Web Consortium. (2002, March). Platform for privacy preferences (P3P) project. Retrieved March 1, 2002, from http://www.w3.org/P3P/

Zronik, John. (2001, January 16). Consumers worried about online privacy, poll shows. Retrieved October 5, 2001, from http://www.canoe.ca/CNEWSTechNews0101/16_consumer-can.html

APPENDIX
(1.)

Accountability - An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Identifying Purposes - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Consent - The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information except where inappropriate.

Limiting Collection - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention - Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Accuracy - Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness - An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Individual Access - Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.