

Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA

March 2005

Philippa Lawson¹
Executive Director
Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
Ottawa, ON, Canada

Abstract

To an extent unimaginable not too long ago, consumer profiling has become an accepted component of retail marketing. Most retailers have adopted some form of "Customer Relationship Management" ("CRM"), which involves collecting as much personal information about individual customers as possible in order to market to them more effectively. Such information is collected through a variety of means, ranging from straightforward surveys and registration forms to surreptitious electronic monitoring, using web bugs and spyware. In some cases, issues of misleading advertising and deceptive business practices arise. Even where these are not a factor, issues of consumer consent to the collection and use of their personal information for marketing purposes are central. How are different jurisdictions responding to these questions? What are the challenges facing those who seek to control the use of online data collection techniques such as cookies and spyware? This paper reviews techniques used by marketers to collect personal consumer information, and critically analyses approaches to their regulation in Canada and the USA.

Introduction

In the days before mass media, merchants tended to know their customers and marketing was a matter of one-to-one persuasion. With the advent of newspapers, followed by radio and television broadcasting, advertising to the masses became possible and grew into a business onto itself. Merchants soon realized, however, that they could get better returns on their advertising dollars if they targeted their marketing efforts to those consumers most likely to respond. Choosing to advertise in certain magazines or on certain television shows helped. But the classic lament of businesspeople remained: "Half of our advertising dollars are wasted; the problem is, we don't know which half." True targeting required knowing your customer, whether actual or prospective, and directing your advertising to that individual. And so marketers began to collect

¹ The author wishes to acknowledge the thorough research and analysis of consumer profiling provided by Gerardo Ludert, LL.M., during the summer of 2004. Also helpful for this paper was research conducted by Kathy Ann Chin Quee, Alison Gardner, David Lam, Dina Mashayekhi and Nelia Rodrigues.

information about individual consumers with a view to personalizing the pitch. They were limited, however, by what their filing cabinets could hold. The real revolution in marketing came with the development of computers and the massive scale of personalized marketing that computers facilitated.

Computerized databases have permitted marketers to collect, store, update, match, merge and trade information about individual consumers in ways never before possible. Retailers can now make use of massive amounts of consumer information through technologies that permit extensive "data mining" and the combining of characteristics into a consumer profile which can be called up at the click of a key.² "Customer relationship management" ("CRM") is the new mantra of marketing.³ Merchants now compete by finding out as much as possible about their customers and potential customers, and personalizing their marketing approaches based on that knowledge. Companies also use this information to categorize and discriminate among consumers, giving better service to more profitable customers.⁴ One term commonly used for this assembled personal information is "consumer profile"; another is "digital dossier".⁵

While some merchants do not share their customer profiles at all and others share only with their (often extensive) corporate affiliates, many companies sell to third parties the data they collect about consumers. Personal data has, in short, become a valuable commodity that is bought and sold like any other in the marketplace. And the database industry in North America appears to be growing, with annual sales in the billions of dollars.⁶ Large "information brokers" such as USA-based ChoicePoint, Axciom, Experian, and Lexis-Nexis and Canadian-based InfoCanada and Equifax specialize in the collection, enhancement and sale of personal information to marketers as well as governments, employers and

² See, for example, Constance Hays, "What Wal-Mart knows about Customers' Habits", *NYTimes* (Nov.14, 2004). According to a 2002 study on CRM conducted by the Canadian Marketing Association, 90% of companies collect name, address, purchase history, customer satisfaction information, and data on customer loyalty and retention, while 70% collect demographic information such as household income and age about their customers. 90% reported using technology to support their CRM efforts: cited in *Incorporating Privacy into Marketing and Customer Relationship Management*, a Joint Report by the Information and Privacy Commissioner of Ontario and the Canadian Marketing Association (May 2004), pp.7, 11.

³ For a detailed explanation of CRM, see Bligh and Turk, *CRM Unplugged: Releasing CRM's Strategic Value* (New Jersey: John Wiley & Sons Inc., 2004); or Fox and Stead, "Customer Relationship Management: Delivering the Benefits": A White Paper by CRM (UK) Ltd and SECOR Consulting Ltd, (UK, 2001); online at <http://crm.ittoolbox.com/browse.asp?c=CRMPeerPublishing&r=%2Fpub%2FSECOR031401%2Epdf>; or Jesus Mena, *Data Mining your Website* (Boston: Digital Press, 1999).

⁴ Joshua Freed, "The customer is always right? Not anymore", *AP/San Francisco Chronicle* (July 5, 2004); Lawrence Scanlan, "Someone to watch over me", *Queen's Alumni Review* (Fall 2004).

⁵ Daniel Solove explains his preference for this term in *The Digital Person: Technology and Privacy in the Information Age* (NY: New York University Press, 2004) at pp.1-2.

⁶ The annual sales of just one info-broker exceed US\$1.9 billion: Testimony of Laura DeSoto, Senior VP, Experian, before the USA Federal Trade Commission, in a workshop on the Costs and Benefits related to the Collection and Use of Consumer Information (18 June 2003) at p.20; online: <http://www.ftc.gov/bcp/workshops/infoflows/present/desoto.pdf>

insurance companies. They maintain databases with billions of personalized records about hundreds of millions of individuals, which records they collect from a variety of different sources in a variety of different ways.⁷

Techniques of consumer surveillance

Methods of collecting consumer information may be overt or covert. Typical overt methods include registration or application forms that consumers must fill out in order to purchase the good or service. Consumers also offer their personal information to merchants via warranty registration forms, surveys and contest forms. Often, the information requested in these forms goes far beyond what is necessary to engage the warranty or conduct the survey or contest. Sometimes, merchants are up-front about the purpose for which they are collecting the data, but more often than not, consumers are unaware that the data they are providing is being used to build personal profiles that are then used for secondary marketing purposes or sold in the marketplace.⁸

Collection of data may therefore be overt in the sense that the consumer knowingly provides it, but covert insofar as the consumer doesn't know for what purposes it will be used. Sometimes, notice as to the secondary uses of the consumer's information is provided in the company's privacy policy. Other times, it is hidden in detailed terms of service. Too often, no notice at all is provided.⁹

⁷ For an excellent overview of consumer profiling in the USA, see EPIC's webpage on Privacy and Consumer Profiling at <http://www.epic.org/privacy/profiling/>. The extent and implications of consumer profiling in the USA are also well catalogued in three excellent books: Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (USA: O'Reilly & Associates, 2000); Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (NY: New York University Press, 2004); and Robert O'Harrow, *No Place to Hide* (Free Press, 2005).

⁸ A 2001 survey of Canadian consumers found that while a slim majority expect that companies they purchase from will try to build an ongoing relationship with them, an almost equally large number do not. Similarly, a significant proportion of Canadian consumers surveyed did not expect companies to keep track of their purchases for further marketing purposes (20% to 55%, depending on the type of company): Ekos Research Associates Ltd., *Business Usage of Consumer Information for Direct Marketing: What the Public Thinks* (Ottawa, Canada: PIAC, August 2001) at pp.3-6; online at <http://www.piac.ca/Directmarketing%20survey%20E.pdf>.

⁹ The most egregious examples of semi-overt collection are intentionally deceptive: consumers are made to believe that the information they provide is being used for one purpose, when it is actually being collected for an entirely different, often fraudulent, purpose. "Phishing" is one of the fastest growing e-mail scams in recent years. "Phishers", posing as legitimate online businesses (typically banks or e-Bay), send unsolicited e-mail messages to consumers asking them to confirm their account details (name, address, account number, password, etc.). These messages are usually highly sophisticated spoofs of actual businesses, such that consumers are easily fooled. Unwary consumers then find themselves victims of financial fraud, perpetrated by the phishers using the data provided by the consumer. "Pharming" is the latest fraudulent technique used to steal consumers' personal data. It hijacks authentic domain names and surreptitiously redirects consumers to fraudulent websites, where consumers are asked to input their personal and account details.

Consumer transactions are increasingly conducted via payment cards or methods that keep track of every transaction. Loyalty cards offer consumers rewards in exchange for the consumer's use of the card. What is not always clear to the consumer is that her use of the card is being tracked, and that the resultant information about her purchases may be shared with affiliates of the loyalty card company for marketing purposes.¹⁰ Credit and debit cards also allow for automatic collection of consumer purchasing histories, which may then be used or sold for other purposes.¹¹ Online purchases offer merchants the opportunity to gather even more specific data about the consumer's preferences. While consumers can avoid leaving a data trail for marketers by using cash to purchase goods in-person, cashiers often demand a telephone number at checkout. The telephone number identifies the individual customer, whose purchases may then be tracked. As the title of a recent book on the topic of privacy states, there is, for US consumers at least, "no place to hide".¹²

Covert data collection occurs both online and offline. Offline, info brokers take advantage of publicly available databases (e.g., birth, death, and marriage records, court records, tax records, property ownership records, drivers licence records) to enhance their consumer profiles.¹³ They also collect aggregated demographic information from official census records, and add it to individual or household profiles based on physical addresses.¹⁴ Companies also buy and sell consumer information to each other privately. Almost all of this information collection and matching is done without the consumer's knowledge.

¹⁰ See, for example, the privacy policy of the Air Miles rewards/loyalty card popular in Canada: online at <https://www.airmiles.ca/servlet/ContentServer?pagename=Airmiles/Visitors/Privacy> . Over half of Canadians surveyed in 2001 reported being unaware that loyalty programs collect, use and disclose information about the customer's purchasing habits in order that companies can target commercial offers to them: Ekos Research Associates Ltd., *op cit* FN 5, at p.6.

¹¹ For example, the online application form for the American Express Rewards Green Card addresses this issue in the middle of its linked "terms, conditions and disclosures" as follows:

"I understand that I must provide all the information requested in this application and I certify that such information is accurate. I authorize you to verify the information on this application and to receive and exchange information about me, including requesting reports from consumer reporting agencies. If I ask whether or not a consumer report was requested, you will tell me and if you received a report, you will give me the name and address of the agency that furnished it. I authorize you and your affiliates and subsidiaries to contact these sources for information at any time, to use information about me, including information from this application and from consumer reports, for marketing and administrative purposes and shared with your affiliates and subsidiaries, unless I direct you not to share with your affiliates and subsidiaries certain credit information (other than transaction or experience information) about me or any Additional "Card" applicant(s) by writing to you at: American Express; P.O. Box 7852; Ft. Lauderdale, FL 33329."

¹² Robert O'Harrow, *op cit*, Note 7.

¹³ The ability and right to access such records varies by jurisdiction.

¹⁴ See, for example, MapInfo Canada's geodemographic market segmentation system, advertised online at <http://www.baselinegeo.com/segment.html> .

Online businesses use “cookies” and log files to track consumers’ online behaviour. More pernicious online surveillance tools include web bugs, spyware, and related tracking programs. Such technologies are used to gather consumer information from publicly available websites (e.g, the WHOIS directories of domain name registries) as well as from the consumer’s own computer or online interactions.

Cookies are data files automatically installed on the consumer’s computer by websites that the consumer visits, for the purpose of identifying the consumer the next time she visits the website. Cookies store information that the consumer has provided to the website (e.g., registration information) as well as information about the consumer’s navigation activities. Online merchants use this information to customize their website according to the customer’s perceived preferences and to call-up consumer address and payment information so that the consumer doesn’t need to re-enter it each time they visit the site. Cookies can also be used to develop and enhance consumer profiles.¹⁵ While some merchants explain their use of cookies up-front, many do not.

Log files, required for the functioning of the Internet, are also now used to understand how consumers interact with websites. Log files record the search engine and key words used by the consumer, the type and version of the consumer’s browser, the consumer’s internet address, and other transmission information. While the primary purpose of these files is to enable Internet surfing, the information that they contain can be used to construct consumer profiles, once combined with personally identifying information.¹⁶

Web bugs are graphics embedded in a web page or e-mail message in order to monitor who reads the web page or message. They are typically invisible so that the user is unaware of being monitored. While web bugs are often used to gather non-personal statistics such as the number of visitors to a website, they are also used to build consumer profiles by gathering information about the websites that the consumer visits. By linking internet addresses with e-mail addresses, web bugs (together with cookies) allow websites to identify individuals who visit their sites. This information may then be matched with other data to profile users of a particular website according to gender, age, postal code, and other demographic data.¹⁷

Amazon.com is considered a trailblazer in online tracking of consumer habits and preferences. It uses tracking and profiling technologies to make customized purchase recommendations and to direct search results toward products the consumer is most likely to want. "In general, we collect as much information as

¹⁵ See, for example, Junkbusters' webpage on "How web servers' cookies threaten your privacy": <http://www.junkbusters.com/ht/en/cookies.html> .

¹⁶ Jesus Mena, *Data Mining your Website*, *op cit*, Note 3.

¹⁷ For more on web bugs, see EFF's FAQ at http://www.eff.org/Privacy/Marketing/web_bug.html, and Spywareinfo's briefer at <http://www.spywareinfo.com/articles/webbugs/> .

possible such that we can provide you with the best feedback", said Werner Vogels, Amazon's Chief Technology Officer in a recent news article.¹⁸

Cookies, log files and web bugs collect information about internet users when the user engages in online communications or interacts with websites. Other technologies such as web bots (also known as spiders and crawlers) and spyware are more proactive in seeking out information on the web. While it is not clear to what extent web bots are used to collect consumer information for profiling purposes, such technologies are commonly used by spammers to harvest e-mail addresses from websites for marketing purposes.

Spyware refers to a range of computer programs that are installed on a user's computer without her knowledge (typically piggybacking on the installation of other programs) and that hide in the background while collecting information and/or making changes to the user's computer. Some spyware surreptitiously captures user information for malicious purposes. For example, keystroke logging programs are used by thieves to record the user's keystrokes and thereby steal passwords, credit card data and other information. In general, however, spyware is designed to monitor the user's online activity (including e-mail communications, web browsing, programs used, and screens viewed) and to transmit that information to a third party.¹⁹

Adware, the most common form of spyware, tracks the consumer's online activity in order to target (often endless) pop-up advertisements to the user. Advertising companies pay adware companies a fee (usually on the basis of the number of user clicks) to have their advertisements distributed to consumers. Browser hijackers reset the user's browser home page to display an advertisement every time the browser is opened. Other forms of spyware redirect web searches to sites that the user did not request. Adware companies may use these techniques to pad their web traffic statistics so as to increase the commissions they receive from the advertisers or website owners.²⁰

Tags and digital watermarks are increasingly being used by copyright owners to track use of their digital products by consumers. Such approaches to digital rights management ("DRM") are attracting the concern of privacy and consumer advocates, as tagging for DRM purposes is often used to profile and target advertisements to users.²¹ As stated by the International Working Group on Data Protection in Telecommunications,

¹⁸ <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/11231195.htm>.

¹⁹ For more on spyware, see <http://computer.howstuffworks.com/spyware.htm>. See also CDT's spyware webpage: <http://www.cdt.org/privacy/spyware/>.

²⁰ *Ibid.*

²¹ Article 29 Working Party (EU), *Working document on data protection issues related to intellectual property rights*, WP 104 (Jan.18, 2005); online at www.europa.eu.int/comm/privacy .

“Electronic Copyright Management Systems (ECMS) are being devised and offered which could lead to ubiquitous surveillance of users by digital works. Some ECMS are monitoring every single act of reading, listening and viewing on the Internet by individual users thereby collecting highly sensitive information about the data subject concerned.”²²

The automated tracking of consumer activity is now possible not only in the online world, but also in the real, physical world. While not yet in widespread use as tools of consumer profiling, radio frequency identification (“RFID”) tags are currently being deployed in the marketplace to track products from production to distribution and to thus reduce the costs of inventory and product theft. They are expected to replace the UPC or bar code now in common retail use. Unlike bar codes, RFID tags can store unique identifying information about a product and then transmit that information to a tag reader. It is thus expected that RFID tags will soon be used to track individual consumers without their knowledge. Privacy advocates are calling for legislation requiring labeling of products with RFID tags, as well as the deactivation of tags upon purchase.²³

The Problem with Consumer Profiling

Consumer profiling offers benefits to consumers in the form of offers that are more likely to match their interests, but it comes at a high price. Even if no single company's data collection or profiling activities is sufficiently invasive to attract public censure, the cumulative effect of all of this CRM activity is to strip individuals of privacy and control over their personal information. Consumers are exposed not only to endless direct marketing pitches, but also to identity theft and other informational abuses. Research suggests that the information in consumer profiles is often riddled with errors.²⁴ Yet important decisions are made on the basis of this information by employers, insurance companies, governments and others. Such decisions are made without the individual's knowledge and thus without any opportunity for them to explain, to correct inaccurate information, or to expose decision-making based on prejudice or misinterpretation.²⁵

²² “Common position on privacy and copyright management” adopted at the 27th meeting of the working group, 4-5 May 2000, quoted in Article 29 Working Party, *ibid*.

²³ See “RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, online at <http://www.privacyrights.org/ar/RFIDposition.htm>; see also EPIC's RFID webpage at <http://www.epic.org/privacy/rfid/>, and CASPIAN's proposed RFID legislation, online at <http://www.spychips.com/press-releases/right-to-know-bill.html>.

²⁴ See testimony of Marc Rotenberg, President, EPIC, before a committee of the USA House of Representatives, in a hearing on “Protecting Consumer's Data: Policy Issues raised by ChoicePoint” (March 15, 2005), pp.2-3; online at <http://www.epic.org/privacy/choicepoint/testimony3.15.05.pdf>.

²⁵ Examples of some such abuses are documented on the Privacy Rights Clearinghouse website at <http://www.privacyrights.org/cases/index.htm#3>, as well as in Robert Ellis Smith's *War Stories* (Rhode Island: Privacy Journal, 2004).

While many fear that the trend toward increased consumer profiling is leading us toward a dystopian “Big Brother” society foreshadowed by George Orwell, Daniel Solove argues that a more apt comparison is Kafka’s *The Trial*: there are a multitude of “digital dossiers” about us circulating in the marketplace, with no single control point but many opportunities for abuse by different actors.²⁶

And indeed, the actual and potential extent of such abuses is now coming to light, after a series of data leaks out of, and security break-ins into, United States data brokers made the news in early 2005. In February 2005, it was revealed that ChoicePoint had sold detailed personal records about over 145,000 Americans to criminals posing as legitimate businesses. As of early March, at least 750 cases of identity theft and over US\$1 million worth of fraud had been attributed to this leak.²⁷ Shortly after the ChoicePoint leak was disclosed, consumer data broker Seisint revealed that hackers had broken into its databases, gaining access to names, addresses, social security numbers and driver’s license information about an estimated 32,000 US citizens.²⁸ Around the same time, the Bank of America announced that it had lost backup tapes detailing the financial records of credit cards held by federal employees. Numerous other security breaches involving the exposure of personal information held by various institutions and commercial database operators have come to light in recent months, prompting US law-makers to consider greater regulation of the shadowy consumer profiling industry.²⁹

Challenges of Regulating Consumer Surveillance

The challenges of regulating data collection, use and disclosure are significant. Technology has always been ahead of the law. Vested interests have developed on the assumption that their practices were legal. Companies that have built up a business based on collecting, using and disclosing personal information without the individual’s knowledge or consent resist changes that put their business model in peril.

²⁶ As Solove states, “...the problem with databases and the practices currently associated with them is that they disempower people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare.”: *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, 2004), p.41.

²⁷ Interestingly, this data leak came to light only after ChoicePoint notified the 34,000 or so Californians whose data had been sold to the identity thieves. ChoicePoint was required, under Californian law, to disclose its security breach to affected individuals. As no other state required such disclosure, no other victims were notified until ChoicePoint bowed to public pressure after the breach was made public.

²⁸ See Matt Hines, “Lexis-Nexis break-in spurs more calls for reform”, CNet News, online at: http://news.com.com/LexisNexis+break-in+spurs+more+calls+for+reform/2100-1029_3-5606911.html .

²⁹ See news reports compiled by CNet at http://news.com.com/2002-1029_3-0.html?tag=ne.tab.hd

Many of these business models involve complex webs of affiliate relationships and actors, making it difficult for investigators to identify those responsible, and allowing each to point the finger at another.³⁰ Adding to the regulatory challenge is the borderless nature of the Internet, and the reality that much data collection and trading occurs across borders.

A further difficulty lies in the fact that privacy invasions are usually hidden. Consumers don't typically know when they are being spied on, when their personal information has been misused, or when it has been improperly shared with another entity. Someone receiving personally addressed junk mail or e-mail may realize that her personal information has been disclosed, but she won't usually know who disclosed it to the marketer. An individual may never know that his insurance application was rejected on the basis of inaccurate information about him in a profile relied upon by the insurer. Victims of identity theft typically only discover the theft months after it occurred, when they decide to seek credit or are pursued by creditors claiming that accounts are overdue. By the time a privacy invasion is discovered, it may be too late to catch the culprit.

The power imbalance created by this information asymmetry between consumers and the companies profiling them is compounded by the fact that individual consumers, even if aware of a privacy invasion, rarely have the time, energy, or resources to pursue it. Of the few that do, many are skeptical of their ability to make a difference, others may be concerned about the repercussions of complaining, and still others lack sufficient information about their rights to take action. Generally, only those who suffer significant loss as a result of a privacy breach have sufficient incentive to hold accountable the company responsible for the breach. Hence, complaint-based approaches to data protection are unlikely to be effective; proactive enforcement by well-resourced agencies, as well as the ability of consumers to take collective action against wrongdoers, is required.

Approaches to the regulation of consumer profiling: Canada and the USA

Unauthorized interception of or access to communications

Both Canada and the US prohibit the interception of electronic communications without the consent of at least one party to the communication.³¹ It is however questionable to what extent this provision would apply to the activities described above. In any case, because this is a criminal offence in Canada, requiring the resources of a law enforcement community with other priorities as well as a high

³⁰ Testimony of Ari Schwartz, Associate Director, Centre for Democracy and Technology, before the House Committee on Energy and Commerce, on "Combating Spyware: H.R. 29, the SPY Act" (January 26, 2005), online at <http://www.cdt.org/testimony/20050126schwartz.pdf>.

³¹ *Criminal Code of Canada*, R.S.C.1985 c.C-46, s.184; USA *Electronic Communications Privacy Act* 18 U.S.C. § 2511.

standard of proof (no reasonable doubt of guilt) in order to convict, it is unlikely to be used to prosecute consumer profilers.

In the United States, civil remedies are available for violations of a similar prohibition in the *Electronic Communications Privacy Act (ECPA)*. The ECPA also prohibits unauthorized access to stored communications. Nevertheless, a US court turned down a case brought against consumer profiler DoubleClick, ruling that the Act applies only to communications in "temporary, intermediate storage" and not to cookies permanently stored on user hard drives.³² The court also ruled that DoubleClick did not violate the ECPA because it had been authorized to access the cookies by the websites that the plaintiffs had visited. Thus, the ECPA does not appear to be effective in restraining private sector collection and use of personal consumer data.

Misleading Advertising and Deceptive Business Practices

Like most countries, both Canada and the USA have laws against misleading and deceptive business practices. In Canada, the *Competition Act* prohibits promoting the supply or use of a product, or any business interest, by making a representation to the public that is false or misleading in any respect.³³ Omission of information can constitute a misleading representation.³⁴ While Canadian authorities have used these provisions to pursue egregious cases of consumer fraud, they have not, publicly at least, held companies accountable for misleading statements regarding consumer privacy.

In contrast, the FTC has used its legislation banning unfair and deceptive trade practices³⁵ to prosecute companies that break promises they make in their privacy policies. Most of these (often high profile) cases have resulted in settlements, prompting USA privacy advocates to complain that the FTC's enforcement of privacy policies has been "weak and reactive".³⁶

Data Protection

But the fundamental problem underlying the collection and trade in personal information goes beyond fraud and deceptive business practices; it is about privacy and control – the inability for consumers to control the use of their personal information, and the consequent loss of privacy and related abuses that they suffer. Here, there is a sharp difference in approach between the USA and Canada.

³² *In re DoubleClick, Inc. Privacy Litigation*, 154 F.Supp 2nd 497 (S.D.N.Y. 2001).

³³ R.S.C. 1985, c. C-24, ss.52 and 74.01 (criminal and civil provisions).

³⁴ *Misleading Advertising Guidelines* (2001); online at <http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct01299e.html#g>; *Application of the Competition Act to Representations on the Internet*, Information Bulletin (Feb.18, 2003); online at <http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct02500e.html>

³⁵ Section 5, *Federal Trade Commission Act*.

³⁶ Solove, *op cit*, Note 7, p.72; Rotenberg, *op cit*, Note 24, p.7.

If there is one point on which all observers agree, it is the striking contrast between American law and policy in these matters and the approach prevailing in most other liberal democracies. Canada, the European Union, Australia, and other countries have adopted comprehensive legislation governing commercialization of personal data -- and sharply restricting commercial use of personal data, except where expressly approved by the individual. In the United States, by contrast, commercial appropriation of personal data in marketing, credit, insurance, and other industries is largely unrestrained.³⁷

Consumer data protection laws in the USA

Privacy protection in the USA is characterized by a patchwork of sector-specific and problem-specific laws at both the federal and state levels – a patchwork that many privacy experts have noted leaves open significant gaps.³⁸ In addition to the *Electronic Communications Privacy Act* and *FTC Act* mentioned above, the following privacy-related statutes have been passed by Congress in recent years:

The *Fair Credit Reporting Act* (FCRA) regulates the credit reporting industry in the USA, giving consumers the right to know the contents of their own credit records, and the right to challenge the accuracy of information and to have it re-verified, updated or removed.³⁹ Although recently amended to provide stronger protection against identity theft, the FCRA has been criticized as failing to adequately restrict secondary uses and disclosures of credit information.⁴⁰ It does not, for example, apply to data-brokers such as ChoicePoint and Seisint whose operate some of the largest databases of personal information in the world.⁴¹

Access to drivers licence information in the USA is now restricted under the *Drivers Privacy Protection Act*,⁴² after the highly publicized murder of actress Rebecca Schaeffer, whose killer found her address through drivers' licence records. The USA *Video Privacy Protection Act*⁴³ was passed in 1988 after a

³⁷ James B. Rule, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions", (2004) 54 Univ. of Toronto L.J. 183, at 184.

³⁸ See, for example, Testimony of Marc Rotenberg, *op cit*, Note 24; Testimony of Evan Hendricks to the Senate Banking Committee (March 15, 2005); Testimony of Chris Jay Hoofnagle before the California Senate Banking, Finance and Insurance Committee (March 16, 2004); all three online at <http://www.epic.org/privacy/choicepoint/majorasltr3.17.05.pdf>.

³⁹ 15 U.S.C. § 1681. Canadian provinces have similar legislation governing the credit reporting industry.

⁴⁰ Solove, *op cit*, p.67.

⁴¹ This could change as a result of Congressional hearings into the much-publicized data leaks and security breaches of these companies.

⁴² 18 U.S.C. § 2721(b)(12).

⁴³ 18 U.S.C. § 2710-2711.

newspaper published the video rental records of Supreme Court nominee Robert Bork. The *Cable Communications Policy Act* (CCPA)⁴⁴ requires cable TV operators to inform subscribers of any personal information collected, and prohibits disclosures that would reveal the subscriber's viewing habits. The *Children's Online Privacy Protection Act* (COPPA)⁴⁵ regulates the collection of children's personal information on the Internet.

Medical records are subject to special protections under the *Health Insurance Portability and Accountability Act* (HIPAA) regulations,⁴⁶ while financial records are subject to the *Gramm-Leach-Bliley Act*,⁴⁷ which permits financial institutions to share "non-public personal information" with affiliated companies and provides no protection for "public" information. Both statutes have been criticized by privacy advocates as being weak and ineffective.⁴⁸

The scourge of spyware is currently generating legislative attention at both state and federal levels in the USA. California⁴⁹ and Utah⁵⁰ have both enacted laws banning or restricting spyware, while bills are pending before state legislatures in at least Michigan,⁵¹ Pennsylvania,⁵² and New York.⁵³ Anti-spyware bills are also pending before both the Senate⁵⁴ and House of Representatives⁵⁵. The Senate "SPYBLOCK" bill would, among other things, prohibit the installation of software that collects and transmits to another person information about a user's Internet browsing or other computer use, without reasonable notification to the user. The House "SPY ACT" bill would, among other things, prohibit the collection and use or transmission of personally identifying information about users via computer software, without notice to and consent of the user.

While each of these initiatives is well-intentioned and has merit, they do not, taken together, provide consumers with control over their personal information in the marketplace. Perhaps reflecting a fear of government intervention in private activities, the American approach to regulating privacy is issue-specific and sector-specific. This reactive and fragmented approach leaves important gaps in privacy protection and fails to establish baseline rules addressing the fundamental issue of control over one's personal information. For example, USA

⁴⁴ 47 U.S.C. § 551.

⁴⁵ 15 U.S.C. § 6501-6506.

⁴⁶ 45 C.F.R. § 164.508(a).

⁴⁷ 15 U.S.C. § 6801-6809.

⁴⁸ Solove, *op cit*, Note 7, pp.69-70.

⁴⁹ *Consumer Protection Against Spyware Act*, California Business and Professions Code § 22947-22947.6 (2005).

⁵⁰ *Spyware Control Act*, Utah Code § 13-40 (2004); enforcement temporarily enjoined as a result of a successful constitutional challenge in June 2004. A new, revised anti-spyware bill has since been tabled: H.B. 104 (2005 GS).

⁵¹ S.B.1315 (2004) and S.B.1316 (2004).

⁵² H.B.2788 (2004).

⁵³ S.B.186 (2005).

⁵⁴ S. 687, the "SPYBLOCK Act"

⁵⁵ H.R.29, the "SPY ACT".

laws protect the online privacy of children under the age of thirteen, but provide no privacy protection for adults. While some types of merchants are subject to strict privacy regulations, many others are unregulated.

The problem with this approach, while obvious to many experts for some time,⁵⁶ is becoming widely apparent with the recent spate of high profile privacy breaches involving huge data-brokers in the USA. American legislators are finally appreciating the threat that unrestrained data collection, use and disclosure poses for individual citizens.⁵⁷

Consumer Data Protection laws in Canada

In contrast to the USA, Canada has comprehensive data protection legislation applicable to the private sector generally.⁵⁸ The federal *Personal Information Protection and Electronic Documents Act* ("PIPED Act"), which became law in January 2001, applies to the collection, use and disclosure of personal information by private sector organizations in the course of commercial

⁵⁶ For example, see "Privacy Advocates Again call for FTC to Halt Online Profiling", EPIC News Release (June 13, 2000), online at: www.epic.org; "Privacy Advocates call on Congress to reverse its anti-privacy attitude", News Release (July 12, 1999), online at <http://www.junkbusters.com/nr23.html>; "Junkbusters tells FTC: privacy laws shouldn't be restricted to Internet", Junkbusters News Release (June 4, 1997); see also Brian Bergstein, "In this data-mining society, privacy advocates shudder", *Seattle Post-Intelligencer* (Jan.2, 2004), at http://www.businessweek.com/bwdaily/dnflash/jan2002/nf20020124_0582.htm; and Jane Black, "Data Collectors need Surveillance, Too", *Business Week online* (Jan.24, 2002) at http://www.businessweek.com/bwdaily/dnflash/jan2002/nf20020124_0582.htm.

⁵⁷ Calling for tighter scrutiny of the consumer data industry, Senator Patrick Leahy stated at the first of a series of Congressional hearings into the data-broker industry:

"The susceptibility of our most personal data to relatively unsophisticated scams and logistical mishaps is greatly disturbing. And this is before we consider the dangers posed by insiders, hackers, organized crime and terrorists. In an era where personal information is a key commodity, the personal information of Americans has become a treasure trove, valuable and vulnerable.

Today, companies around the world routinely traffic in billions of personal records about consumers. The magnitude of these transactions has rendered the individuals behind the data faceless. But at the end of the day, when things go south, it is the consumer that bears the brunt of the harm. For consumers caught up in the endless cycle of watching their credit unravel, undoing the damage caused by such breaches becomes life-consuming and monumental." : March 10, 2005; online at: <http://leahy.senate.gov/press/200503/031005b.html>.

Senator Dianne Feinstein responded to the ChoicePoint debacle with a similar statement calling for greater regulation of data-brokers:

"This [Seisint's] new database breach clearly demonstrates that the effort to consolidate consumer information into huge databases and the lack of adequate protections for that information has made it possible for identity theft to be perpetrated on a massive scale.... The only way to fix the situation is with Federal legislation that would set a national standard for notification and privacy protection.": March 9, 2005; online at: <http://feinstein.senate.gov/05releases/r-seisint-breach.htm>

⁵⁸ Separate legislation, at both federal and provincial levels, applies to public sector collection, use and disclosure of personal data.

activities.⁵⁹ Under the PIPED Act, organizations are not permitted to collect, use or disclose personal information in the context of commercial activities without the individual's knowledge and consent, except as specified. "Personal information" is defined as any "information about an identifiable individual..." Exceptions to the knowledge and consent rule include, among other things, court orders, law enforcement, debt collection, and emergencies.

Under the Act, organizations are required to comply with the ten principles of the Canadian Standards Association Model Privacy Code, set out below. The CSA Code was developed by a multi-stakeholder group including representatives of major business interests, governments and consumer groups, and is based on internationally recognized fair information practices.⁶⁰ The ten principles include:

1. *Accountability*: Organizations must designate an individual to be accountable for their compliance with the principles. They must also ensure that third parties to whom they transfer data for processing provide a comparable level of protection.
2. *Identifying Purposes*: Organizations must identify the purposes for which they collect personal information at or before the time of collection.
3. *Consent*: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Consent to secondary marketing purposes may be obtained via negative option (also referred to as "opt-out") as long as the sensitivity of the information and the reasonable expectations of the individual do not suggest otherwise. But organizations cannot, as a condition of the supply of a good or service, require an individual to consent to information collection, use or disclosure "beyond that required to fulfil the explicitly specified and legitimate purposes."⁶¹

⁵⁹ S.C.2000, c.5; online at: <http://laws.justice.gc.ca/en/p-8.6/93196.html>. The PIPED Act came into effect on a staggered basis. Initially, it applied only to federally regulated industries such as banking, telecommunications, and airlines, as well as inter-provincial data transfers. As of January 1, 2004, it has applied to provincially regulated businesses as well, except in provinces that have substantially similar data protection legislation. As of March 2005, privacy legislation in the provinces of Quebec, Alberta and British Columbia applies to both commercial and non-commercial activities of non-federal organizations in those provinces.

⁶⁰ For example, as set out in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, online at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

⁶¹ Provincial data protection legislation has improved upon the wording of this clause, prohibiting refusals to deal where the information requested is not "necessary to provide the product or service": Alberta *Personal Information Protection Act*, s.7(2) and British Columbia *Personal Information Protection Act*, s.7(2).

4. *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.

5. *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 fulfilment of those purposes.

6. *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.

7. *Safeguards*: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

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

9. *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.

10. *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.

The PIPED Act adds a further principle, sometimes referred to as "*Limiting Purposes*", in subsection 5(3): Organizations "may collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances." This puts an absolute, albeit vague, limit on what organizations can do with personal information, regardless of consent.

Individuals may file complaints with the Privacy Commissioner of Canada against companies for contravening the legislation. The Commissioner has broad powers to investigate complaints and to audit the personal information management practices of organizations. However, she has no enforcement powers other than the right to publicize and thus affect the public reputation of an organization; her findings, which must be rendered within one year of the complaint, are not legally binding. If a complainant or the Commissioner wants to force an organization to change its practices or to obtain compensation for harm

suffered as a result of the privacy breach, she must apply to Federal Court for such an order.

Although strongly supportive of broad-based data protection legislation, privacy advocates in Canada are critical of the PIPED Act's weak oversight and enforcement provisions and of the failure of the Privacy Commissioner to use the full toolkit of enforcement powers that she has (especially audits and publicity).⁶² Some have also expressed concerns about Commissioner findings that are overly deferential to businesses.⁶³ In one of the few cases taken to Federal Court by a complainant, the Commissioner's finding in favour of a telephone company was ultimately reversed.⁶⁴ A detailed report published by the Public Interest Advocacy Centre in 2004 concludes that the PIPED Act "is a sheep in wolf's clothing", and that "the depth of the negative experience of consumers with PIPEDA suggests the need for major reforms to PIPEDA to make its process more practical and effective for consumers".⁶⁵ Such reforms are possible, given that the Act is scheduled for Parliamentary review in 2006.

While the PIPED Act clearly applies to the collection and use of consumer data by companies using the various techniques described above, it has not proven very effective in eliminating the non-consensual use of personal consumer data by companies for secondary marketing purposes.⁶⁶ This is likely due in part to the Act's vaguely-worded consent obligations, as well as the Commissioner's apparent reluctance to insist upon clear and strict consent requirements.⁶⁷ It is also no doubt due to lack of effective enforcement of the Act.

Whatever its weaknesses, however, Canada's data protection legislation is comprehensive. It covers key fair information principles and applies to all companies that deal with consumer data in the marketplace. This has the effect of infusing fair information practices into all sectors of the marketplace, and of

⁶² John Lawford, *Consumer Privacy under PIPEDA: How are we doing?* (PIAC, 2004); Christopher Berzins, "Three Years Under the PIPEDA: A Disappointing Beginning", *Canadian Journal of Law and Technology*, vol.3, no.3 (Nov.2004), pp.113-126; Michael Geist, "Privacy Law perversely protects those who break it" *Toronto Star* (Oct.18, 2004); "Revise Privacy law to expose offenders, block snoops" *Toronto Star* (Oct.25, 2004).

⁶³ Lawford, *ibid.*, pp.44-55. See also Michael Geist, "Weak enforcement undermines privacy laws" *Toronto Star* (April 19, 2004).

⁶⁴ *Englander v. TELUS Communications Inc.*, [2004] FCA 387, online at <http://decisions.fca-cf.gc.ca/fca/2004/2004fca387.shtm>; Commissioner finding "Use and disclosure of personal information in telephone directories", PIPED Act Case Summary #8, online at http://www.privcom.gc.ca/cf-dc/cf-dc_010814_01_e.asp. Note that the complainant succeeded on the issue of notice to subscribers regarding the various purposes for which their published information was collected, and regarding the availability of unlisted service. He did not however succeed on the issue of the \$2 fee for unlisted service.

⁶⁵ Lawford, *op cit*, p.3.

⁶⁶ *Ibid.*, pp.44-55. As well, CIPPIC's ongoing review of privacy policies and forms by which Canadian companies purportedly obtain consumer consent to secondary marketing indicates that the consent thereby obtained is often confusingly worded, under-informed, inadequately brought to the consumer's attention, and not easy to opt out of.

⁶⁷ *Ibid.*, pp.40-42.

focusing on the underlying principle of individual control over personal information, rather than on specific informational abuses. So, for example, the Canadian Marketing Association's *Code of Ethics and Standards of Practice* includes principles such as "Giving consumers control of how information about them is used".⁶⁸

Moreover, the Canadian approach gives Privacy Commissioners the authority to educate, encourage and effectively cajole organizations into compliance with the Act. Thus, in May 2004, the Information and Privacy Commissioner of Ontario and the Canadian Marketing Association published a joint report entitled "Incorporating Privacy into Marketing and Customer Relationship Management", which report concluded:

"Businesses should view privacy as a tool for ensuring that CRM initiatives succeed. This can be achieved by building fair information practices into CRM, with a particular focus on being open and transparent with customers. In short, privacy is good for CRM and can help companies to gain a competitive advantage in the marketplace by building strong customer relationships based on a foundation of trust."⁶⁹

A concrete example of how the Canadian approach can generate meaningful privacy protections for consumers involves postal addresses. In both Canada and the USA, national postal services offer a "change of address" service to customers, allowing them to have mail forwarded to a new address for a certain period of time after moving. In both countries, this change of address information is made available to marketers for the purpose of updating their mailing lists. There is a crucial difference, however, between the two regimes: in Canada, customers can opt not to have their change of address information shared with marketers; customers of the USA Postal Service have no such choice.⁷⁰ The Canadian approach was implemented as a result of negotiations between the Privacy Commissioner of Canada and Canada Post, based on the fair information principles enshrined in both public sector and private sector data protection legislation.

Finally, although there is a thriving business in the profiling of Canadian consumers using personal information gleaned from purchase/credit records, subscriber lists, market surveys, and telephone books as well as geographically aggregated information obtained from Statistics Canada,⁷¹ preliminary research by CIPPIC suggests that the market for Canadian consumer information is much less extensive than that for US consumer data, and that some USA-based data-

⁶⁸ Section J1, online at <http://www.the-cma.org/consumer/ethics.cfm>.

⁶⁹ http://www.the-cma.org/media/nr_crm2004.cfm

⁷⁰ See online change of address form at <https://moversguide.usps.com/?referral=USPS> .

⁷¹ See, for example, www.infocanada.ca, www.i-com.com, www.equifax.ca, www.tuc.ca, <http://www.cstonecanada.com/index.html>.

brokers are not collecting or selling information about Canadians, at least in part because of the PIPED Act.⁷²

Conclusion

New technologies, together with the relentless drive of private business to make innovative uses of such technologies in the pursuit of profit have created many new challenges, not least of which is for consumer privacy. It is now widely acknowledged that the potential harm to consumers from unrestrained collection, use and disclosure of their personal data by private companies outweighs any benefits that they may derive from such practices.

Yet legal protections inevitably lag behind the rapid development of technology and market practices, leaving consumers at the mercy of those testing the limits of social tolerance for an increasingly level of marketplace surveillance. And turning back the clock is difficult, if not impossible, once an industry has established itself as deeply as the consumer profiling industry has done in North America.

Moreover, the hidden nature of privacy invasions, together with the information asymmetry and power imbalance between consumers and the companies that are profiling them, makes effective protection of consumer privacy particularly challenging.

These challenges suggest not only that market forces are insufficient to protect consumer privacy, but also that effective data protection legislation cannot simply rely upon consumer complaints and lawsuits to discipline companies. Proactive enforcement by state authorities with expertise in data management is needed in order to expose, punish, and thus deter privacy invasions.⁷³

The approach to data privacy in the USA has so far been to rely on market forces and industry self-regulation, except where an actual crisis, such as the murder of a pop-star or the publication of a nominated judge's video sales records, highlights the need for legal rights and obligations. This approach has resulted in a complex and uneven legislative regime that is rife with gaps and loopholes. It leaves consumers powerless to control the uses of their personal information and vulnerable to abuses that they cannot challenge.

The Canadian approach to data protection attempts to remedy this situation by applying widely accepted fair information practices across the board, to all

⁷² For example R.L.Polk & Co., one of the major data-brokers in the USA, told a CIPPIC researcher that it has not collected or sold information about Canadians since 2001, as a result of "a change in Canada's laws". In response to our inquiries, ChoicePoint indicated that it could conduct criminal records and drivers' licence searches on named Canadians, but had no other information on Canadians for sale.

⁷³ International cooperation among data protection authorities is also needed in order to address the very serious, and increasingly relevant, challenges of cross-border data flows.

market sectors. However, it does so in a light-handed way, relying on substantive obligations drafted by a multi-stakeholder industry committee rather than by legal experts, and adopting an "ombuds" approach that focuses on complaint resolution and industry cooperation rather than proactive and meaningful enforcement. Businesses are able to take advantage of vaguely-worded provisions in the law, and need not worry much about enforcement under the current regime.

There is no question that broad-based data protection legislation similar to that in Canada is needed in the USA. But Canada's data protection regime is in need of more effective oversight and enforcement. If North American consumers are to gain any meaningful control over their personal information, data protection agencies must be given the tools, resources, and political will to investigate market practices swiftly and proactively (not just in response to complaints), to hold companies publicly accountable for non-compliance, and to apply meaningful penalties for privacy violations.

*** END OF DOCUMENT ***