PROTECTING ONLINE PRIVACY IN THE PRIVATE SECTOR: IS THERE A '*BETTER*' MODEL?

Par David Dubrovsky[*]

"No human reads your mail to target ads or other information without your consent." This is an excerpt included in Google's Gmail Privacy Policy that explains the methodology underlying the interactive advertisement process incorporated into Google's web-based e-mail service. Google's inclusion of this assurance reveals a number of complex privacy concerns. As information technology continues to influence privacy on the Internet, the latter's viability as a legally protected right comes into question.The theme of this essay competition is the relation between law and cyberspace. In addressing the struggle faced by governments and industry experts to identify effective approaches for regulating emerging technologies, the author compares the effectiveness of legislation and industry self regulation aimed at protecting online privacy. Three central issues are considered: consent, burden of protection and enforcement. The analysis suggests that neither course is mutually exclusive and that a consolidated approach provides a more effective level of protection and a more malleable framework to meet future needs.

"No human reads your mail to target ads or other information without your consent." Cet extrait de la politique de vie privée de Gmail illustre la méthodologie qui sous-tend le procédé de publicité interactive incorporé au service de messagerie en ligne de Google. L'inclusion par Google de cette représentation soulève plusieurs préoccupations complexes relatives à la vie privée. À mesure que les technologies de l'information continuent d'influencer la vie privée sur Internet, sa viabilité en tant que droit protégé par la loi est remise en question. Le thème de ce concours de dissertation est la relation entre le droit et le cyberspace. Considérant les obstacles rencontrés par les gouvernements et les experts de l'industrie dans l'identification d'approches efficaces pour réglementer les nouvelles technologies, l'auteur compare l'efficacité de la législation et de l'autorégulation de l'industrie visant à protéger la vie privée en ligne. Trois aspects centraux sont considérés : le consentement, le fardeau de protection et la mise en œuvre. L'analyse suggère que les méthodes ne sont pas mutuellement exclusives et qu'une approche conjuguée fournit une protection plus efficace et un cadre plus malléable pour rencontrer les besoins futurs.

[*] Student-at-law at the firm McMillan Binch Mendelsohn LLP (Toronto). David Dubrovsky holds a B.COM. with major in Finance 2003 (John Molson School of Business) and a LL.B./B.C.L. 2006 (McGill University). This paper was written as a second year law student and was selected as the co-winner of the 2005 Matthieu-Bernard Essay Competition on the question of: "L'espace cybernétique est-il sans loi?".

Introduction

"No human reads your mail to target ads or other information without your consent."[1] This is an excerpt included in Google's Gmail Privacy Policy that explains the methodology underlying the interactive advertisement process incorporated into Google's web-based e-mail service. Google's inclusion of this assurance reveals a number of complex privacy concerns, which are discussed in this paper. As information technology continues to influence privacy on the Internet, the latter's viability as a legally protected right comes into question. Industry leaders such as Sun Microsystems Chief Executive Officer Scott McNealy contend that "[y]ou have no privacy anymore. Get over it."[2] This paper, however, maintains that while the Internet continues to widen the scope of privacy concerns, the right to privacy as a fundamental legal right continues to need protection.

The theme of this 2005 edition of the Mathieu-Bernard essay competition is the relation between law and cyberspace. In addressing this topic, this paper discusses the struggle faced by governments and industry experts around the world in identifying effective approaches for regulating emerging technologies. Specifically, this paper will ask whether the government has a duty to enact legislation aimed at protecting online privacy or whether the industry should self regulate. This paper will conduct a comparative analysis of both approaches, focusing on three central considerations that are fundamental to the effectiveness of such a privacy protection scheme: consent, burden of protection and enforcement. The analysis will reveal that neither course is mutually exclusive. Rather, a consolidated approach provides a more effective level of protection and a more malleable framework to meet future needs.

I. Have we Googled our Privacy Away?

The rise of e-commerce and Internet technology presents an abundance of novel privacy concerns. In an era where Internet users can work remotely, manage their personal affairs and access a vast amount of information within a couple of clicks on a mouse, privacy is not what it used to be. The ability to be tracked in a digital society has the effect of "[c]onsumers becom[ing] the consumed as information about everyday activities is suctioned into a file for later perusal."[3]

The major difficulty facing Internet users today is the inability to know when they are being watched. "In cyberspace, surveillance is not self-authenticating. Nothing reveals whether you are being watched, so there is no real basis upon which

---

1 Google Inc., "Gmail Privacy Policy" (12 November 2004), online: Google <http://gmail.google.com/gmail/help/privacy.html>.

2 Michael W. Lynch, "Privacy at Stake" *The Chief Executive* (November 2000), online: Find Articles <http://www.findarticles.com>.

3 John MacDonnell, "Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?" (2001) 39 Alberta L. Rev. 346 at 349 [MacDonell].

to consent."[4] Professor Jerry Kang characterizes this situation as one where you are being invisibly stamped with a bar code.[5] The following section will discuss several methods, of the many available, which enable organizations to collect personal information on the Internet.

A. Cookies, Java Applets, Spyware and Data Mining

The use of cookies is prevalent in almost every type of Internet activity. Also known as persistent client-side hypertext transfer protocol files,[6] cookies are "small bits of text stored on a user's computer that enable the recognition of repeat visits from a single computer, allowing settings particular to that user to be maintained."[7] These data files may include various bits of information, including the date and time of the last visit to the website, usernames, passwords and more.

The conventional use of cookies is to identify users of a website in order to customize the delivery of the requested page or pages. However, an alternative use of cookies allows for the acquisition of data that reveals the user's online activities, such as which links are selected and which web pages are viewed. This type of data, known as "clickstream data", involves a third party who collects information about a user's patterns across multiple websites. In many instances, such third parties are Internet direct marketing companies that place advertisements in the form of banner ads on websites.[8]

When a user visits a website that contains a banner ad, which is part of an advertising network, cookies are inadvertently stored on the user's computer and enable the third party to monitor the user's online activities. As the user clicks from web page to web page, the information is continuously tracked by the cookies common to the advertisement banners across the websites. Once collected, the data is compiled and synthesized to create complete user profiles, a process otherwise known as "data mining".

Spyware and Adware are applications that enable organizations to collect large amounts of data without the user's permission.[9] Such applications may be installed without the user's consent as part of a separate application or by way of a

---

4 Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv L. Rev. 501 at 505.

5 Jerry Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan. L. Rev. 1193 at 1198.

6 Ian R. Kerr, "The Legal Relationship between Online Service Providers and Users" (2001) 35 Can. Bus. L.J. 419 at 421.

7 MacDonell, *supra* note 3 at 353.

8 Rachel K. Zimmerman, "The Way the 'Cookies' Crumble: Internet Privacy and Data Protection in the Twenty-First Century" (2001) 4 N.Y.U.J. Legis. & Pub. Pol'y 439 at 444.

9 Paul M. Schwartz, "Property, Privacy, and Personal Data" (2004) 117 Harv. L. Rev. 2055 at 2065 [Schwartz].

Trojan horse virus.[10] Those applications have the ability to monitor and capture information about the user's computer activities while the user is online.[11]

B. Implications of Data Collection

From an e-commerce perspective, the ability to collect and compile large amounts of Internet user data is extremely valuable. An increased flow of information provides organizations with an advanced ability to examine online behaviour, presenting competitive advantages in increasingly aggressive markets.[12] These benefits, arguably, pass on to consumers in the form of cost savings and more targeted advertising. Also, data collection provides users with the convenience of customized web surfing such as personalized web pages.

However, online data collection provides organizations with powerful means to violate an Internet user's right to privacy. In many instances, users are not provided with notice of the website's data collection practices and do not have the ability to conduct their online activities in a private manner. Information technology has effectively taken target marketing up a notch by allowing companies to synthesize data in a manner that provides more detailed profiles of users. It is the ability to integrate the data that has the effect of changing its propriety. As Professor Solove puts it:

> [w]e are accustomed to information on the web quickly flickering in and out of existence, presenting the illusion that it is ephemeral. But little on the Internet disappears or is forgotten, even when we delete or change the information. The amount of personal information archived will only escalate as our lives are increasingly digitized into the electric world of cyberspace.[13]

To illustrate this phenomenon, it is useful to recount events surrounding DoubleClick Inc. (DoubleClick). DoubleClick is one of the largest Internet direct marketing companies, with banner ads placed on more than 11,000 websites and databases with information on over 88 million American households. In 1999, DoubleClick purchased Abacus Direct Corporation (Abacus), a direct marketing company that held, at the time, identifiable information on approximately 90 percent of all American households. Following the merger, DoubleClick amended its online privacy policy by removing the assurance that information collected online would not be linked with personally identifiable data. Public outcry and legal challenges

---

10 A Trojan horse is an application that overtly carries out one function while covertly doing something else.

11 This includes any type of activity, from monitoring the user's individual keyboard strokes, reading a user's emails or recording credit card numbers entered.

12 Svetlana Milina, "Let the Market Do its Job: Advocating an Integrated Laissez-Faire Approach to Online Profiling Regulation" (2003) 21 Cardozo Arts & Ent. L.J. 257 at 261 [Milina].

13 Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. Rev. 1393 at 1412-13.

followed the move, as it became clear that DoubleClick was planning to merge the non-personal data that it had collected online with its newly acquired database of identifiable data collected by Abacus. The merge would enable identification of names, addresses and complete profiles of millions of Internet users. Following a class action challenge,[14] DoubleClick quickly announced that it would halt any plans to merge their databases until further notice.

Although the public outcry impacted DoubleClick's attempt to merge their databases, the potential for data mining is a reality that Internet users must face. Technological developments are making it increasingly difficult to prevent the synthesising of large amounts of data. "The holy grail is to find a way to link online clickstream data with offline data captured in the warehouse, and a number of software and hardware vendors are working hard to deliver."[15]

C. Approaches Taken to Protect Data Collection on the Internet

One of the first sets of principles related to data protection was developed in 1980 by the Organization for Economic Co-operation and Development (OECD). Relatively early on, the OECD realized a need for minimum legal standards surrounding the collection and use of personal data on the Internet throughout different jurisdictions.[16] In establishing the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[17] (*Guidelines*) the OECD set the stage for jurisdictions around the world to begin considering legislation as a means of protecting the right to privacy on the Internet.

Quebec, among the first North American jurisdictions to adopt legislation regulating the collection of personal information in the private sector, enacted *An Act Respecting the Protection of Personal Information in the Private Sector*[18] (Quebec Legislation), effective January 1, 1994. On April 13, 2000, the Federal government followed suit and enacted the *Personal Information Protection and Electronic Documents Act*[19] (PIPEDA), which establishes a framework for privacy protection in the private sector throughout Canada.[20] Specifically, its application regulates the

---

14 *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (SDNY 2001).

15 Colin Tener "Clickstream Data Alone Doesn't Provide a Complete Picture " *Strategy* (22 May, 2000) D9, cited in Andrew McClug, "A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling" (2003) 98 Nw. U.L. Rev. 63 at 85 [McClug].

16 See MacDonnell, *supra* note 3 at 359.

17 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980), online: OECD <http://www.oecd.org>.

18 *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1 (while Quebec may have been the first province to regulate in this area, this has not been the trend throughout Canada; as such, PIPEDA applies in Ontario and all other Canadian provinces, except Quebec, and recently Alberta and British Columbia).

19 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

20 *Ibid*. s. 30(1) and 30(1)(1.2) (it also included a transitional provision, limiting its application from any organization that fell within provincial jurisdiction for three years, effectively providing the provinces with an opportunity to either pass their own legislation regarding data collection in the private sector or allowing PIPEDA to apply).

collection, use or disclosure of personal information in the course of any commercial activity by any organization.[21]

In Europe, the *Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data*[22] (*Directive*) was adopted by the European Council (EC) in 1995. The EC took a forceful approach by restricting the transfer of data to non-member countries unless the recipient country had adequate levels of protection in place.[23] This had an impact in both Canada and the United States (U.S.), as the *Directive* potentially threatened business opportunities between Europe and North America. As discussed above, Quebec had already established legislation in order to ensure that transatlantic e-business opportunities would not be threatened and Canada had followed suit with PIPEDA in 2000.

The landscape in the U.S. was different. Certain legislative attempts were made, including the *Bono Bill*[24] and *Edwards Bill*,[25] but ultimately failed on the basis that direct government regulation anywhere near the Internet could threaten the online industry. In order to avoid difficulties in transatlantic e-business opportunities, a safe harbour agreement was reached with the European Union (EU).

Part III and IV of this paper will assess the effectiveness of direct legislative regulation and industry self-regulation at protecting online privacy. Both analyses will measure the effectiveness of each approach in light of three objectives: protecting a user's consent, balancing the burden of protection between the user and organizations and ensuring adequate enforcement.

II. Analysis of Legislative Schemes Aimed at Protecting Online Privacy

A. Protection of User Consent

One of the earliest legal characterizations of the right to privacy is the right "to be let alone."[26] In the context of personal information on the Internet, it means that a user has the right not to have his or her personal information collected and manipulated. As a result, organizations have attempted to circumvent liability through the use of online license agreements, terms of use and privacy policies, to name a few. The difficulty throughout the various legislative attempts at protecting online privacy

---

21 *Ibid*. s. 4(1)(a) (personal information is defined as information about an identifiable individual, not including a person's name, title or business address, or telephone number of an employee of an organization; commercial activity is defined as any particular transaction that is of a commercial character).

22 EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] O.J. L. 281/31.

23 *Ibid*. s. 25.

24 U.S., Bill H.R. 2929, *Securely Protect Yourself Against Cyber Trespass Act*, 108th Cong., 2004.

25 U.S., Bill S. 197, *Spyware Control and Privacy Protection Act*, 107th Cong., 2001.

26 See Thomas M. Cooley, *A treatise on the law of torts, or the wrongs which arise independent of contract* (Chicago: Callaghan and Company, 1907) at 192.

has been the regulation of such agreements, including the requisite elements surrounding a user's consent. In fact, because of the complex nature of data collection practices and the pace of technological advances, it is difficult to effectively define the role of consent in such agreements.

PIPEDA is a good illustration of a legislative scheme where the requirements for valid consent are not sufficiently defined. The reasonability requirement included in PIPEDA establishes that an organization must take into account the sensitivity of the information that it collects when determining what form of user consent is necessary.[27] In attempting to define what is reasonable, it provides an analogy whereby the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information, but the names and addresses of subscribers to a special-interest magazine might be considered sensitive.[28] This illustration is difficult to apply for a number of reasons, but mainly because it allows for a large amount of interpretation. How is a newsmagazine differentiated from a special-interest magazine? Would such a characterization change if there were no contractual relationship between the user and the organization, and if so, how?

It is not suggested that an element of reasonability is not an important tool in defining the requisite level of consent. To the contrary, various considerations of reasonableness appear throughout legal regimes and jurisdictions. However, a reasonability requirement is not effective in protecting a user's right to online privacy as technological advances create circumstances that go beyond the reasonable person's considerations and expectations. Most Internet users may not understand the types of threats present online, nor the types of technologies available. Further, personal information in a digital world has varying significance to different people. Some users may appreciate that the Amazon.com website tracks their usage in order to provide them with specialized product recommendations while others may find such a practice abhorrent.

The conflicting interpretations of reasonableness, as discussed above, are highlighted in *Englander v. Telus Communications Inc.*[29] (*Englander* 2004), the first PIPEDA complaint handled by the Federal Court. The case concerned two primary issues: whether the level of disclosure provided to new customers by Telus Communications Inc. (Telus) met the statutory standard and whether Telus could charge customers a monthly fee for its non-published number service. The decision, however, illustrates the consequences resulting from the reasonability requirement included in PIPEDA.

One of the issues examined concerned the consent provided by the applicant, Mathew Englander, to having his personal information included in Telus' directories. The Federal Court, Trial Division, concluded that his consent was valid for all of Telus' directories, including its online and CD-ROM versions, as it was open for him

---

27 *PIPEDA*, *supra* note 19 s. 4.3.4.

28 *Ibid*.

29 *Englander v. Telus Communications Inc.*, [2004] F.C.J. No. 1935, 2004 FCA 387 (F.C.A.) [*Englander* 2004].

to inquire as to the scope of such directories.[30] However, the Federal Court of Appeal did not agree. Justice Decary, for the Court, held that

> [t]hese services were not identified at the time of enrolment and there [was] no evidence that they were so connected with the primary purposes of telephone directories that a new customer would reasonably consider them as appropriate.[31]

Although these circumstances are not directly related to online data collection, the reasoning provided by the Court is relevant. PIPEDA sets out that a commercial organization must seek consent for the collection of any personal information and in doing so, fails to effectively set the boundaries of what constitutes valid consent. In order for users and organizations to be able to meet the requisite elements of consent, legislation that aims to protect a user's right to privacy while online must define the boundaries of consent more explicitly.

One might question why PIPEDA does not provide a more clear definition of consent. The Federal Court of Appeal addressed this question in *Englander*. The Court recognized that PIPEDA is a compromise in both substance and form. In substance, a consumer's right to privacy is balanced by a commercial organization's need for access to personal information.[32] In an era where e-business is becoming more dominant, there is a need to balance the impact of regulation. In form, the Court iterated that Schedule 1 of PIPEDA is an exact replica of the *CSA Standard* adopted in 1995,[33] which itself was largely based on the 1980 OECD *Guidelines*. The Court stated that this is entirely problematic as they both "[we]re the product of intense negotiations between competing interests [e-commerce development and consumer protection], which proceeded on the basis of self-regulation and which did not use nor purport to legal drafting."[34]

An example of a more clear definition of consent is provided in the EU *Directive*. While PIPEDA stipulates a reasonability requirement for consent, the EU *Directive* requires that an organization must seek explicit consent before the collection of any personal information.[35] By removing the ambiguity underlying the role of consent, users are in a better position to ensure that they are not implicitly

---

30 *Englander v. Telus Communications Inc.*, [2003] F.C.J. No. 975, 2003 FCT 705 (F.C.T.D.) [*Englander* 2003], Blais J. ("As such, I believe that once a TELUS representative has asked a new subscriber how he or she would like his or her listing information to appear in the telephone directory, it is open to that subscriber to enquire on the options available to him or her. If the privacy of such information is fundamental or simply desired by a subscriber, it is his or her responsibility to educate him or herself, either by asking the representative or through the various tools which have been put at the public's disposal by TELUS", at para. 47).

31 *Englander* 2004, *supra* note 29 at para. 65.

32 *Ibid*. at para. 38. See also Michael Geist, *Internet Law in Canada*, 3rd ed. (Concord, Ont: Captus Press, 2002) at 303.

33 Canadian Standards Association, *Model Code for the Protection of Personal Information (CAN/CSA-Q8390-95)* (March 1996), online: CSA <http://www.csa.ca/standards/privacy/code> [*CSA Standard*].

34 *Englander* 2003, *supra* note 30 at para. 43.

35 *Directive*, *supra* note 22 s. 7.

agreeing to a use that they otherwise would not consent to and businesses can better protect themselves from potential complaints based on making a wrong discretionary choice. PIPEDA should strive to make the threshold of consent easier to ascertain.

B. Balancing the Burden of Protection

Legislative schemes have, as one of their objectives, to balance competing interests between Internet users and industry. In mediating between these rival concerns, the obligations imposed by the regulations may be more heavily weighted on the user or on the organization. The following section will compare PIPEDA and the Quebec Legislation to illustrate this more clearly.

The obligation to update or amend personal information collected by an organization differs between PIPEDA and the Quebec Legislation. In PIPEDA, the burden lies with the users to have their information updated. In the Quebec model, the burden is placed on the organization to prove that the information does not need to be amended. Similarly, PIPEDA merely recommends that an organization explain the scope and purpose of their collection practices, while the Quebec Legislation places a positive obligation on organizations to notify consumers, in obtaining consent, of the scope and manner in which they will collect information. These are clear examples where depending on the compromise reached in the legislation, the burden of protection may lie with the Internet user rather than with the organization.

Another characteristic of where the burden of protection lies is the ability of a user to choose not to have their information collected. The *Bono Bill* and *Edwards Bill*, the two failed attempts in the U.S. to enact online privacy legislation mentioned previously, were both aimed at regulating the use of Spyware in collecting personal information online. Interestingly, both required explicit consent to collect any personal information through the use of such applications. The *Edwards Bill* contained a mandate for consumers to have the ability to turn off the data collection feature of the software without affecting its use.[36] Effectively, this puts pressure on the organization to provide users with enough information concerning their privacy practices in order to deter users from barring any collection whatsoever.[37] This type of inclusion went further than both PIPEDA and the EU *Directive* by inherently stimulating industry practice. Rather than being reactionary, it is likely that the bills would have encouraged industry players to approach data collection in a different manner. The design of opt-in and opt-out mechanisms will be discussed in Part IV of this paper, when assessing the impact of self-regulatory approaches to online privacy protection.

---

[36] *Ibid*. s. 2(a)(1)(c).

[37] Schwartz, *supra* note 9 at 2121.

C. Adequacy of Enforcement Scheme

Legislative attempts at protecting online privacy are only as effective as are their enforcement mechanisms. The predominant problem, however, with enforcing privacy legislation in the private sector is that enforcement is generally dependant on a consumer's willingness to file a complaint. Furthermore, as is the case in PIPEDA, the enforcement scheme may not provide for an efficient and effective mode of resolving privacy infringements. Professor Geist summarizes these weaknesses: "It is evident that privacy laws without effective enforcement and genuine transparency may provide Canadians with little more than placebo privacy protection."[38]

In PIPEDA, enforcement is ultimately in the hands of the Federal Court, as the Privacy Commissioner's powers are advisory and not binding.[39] To illustrate this, an individual can file a written complaint against an offending organization with the Privacy Commissioner. The Commissioner's discretion is limited to conducting an investigation and issuing a non-binding opinion. While attempts may be made by the commissioner to settle the matter through mediation or conciliation, there is no such requirement. Where the complainant is not satisfied with the outcome achieved by the Commissioner, an appeal may be made before the Federal Court Trial Division. Yet, the Federal Court may not have the required expertise to be able to effectively adjudicate over these types of matters. While privacy protection may not be "rocket science", it is clearly important to maintain a familiarity with the issues and an appreciation of continued changes in technology.[40]

An alternative to the present enforcement mechanism under PIPEDA is the composition of a privacy tribunal, with the jurisdiction to adjudicate over all complaints falling under the privacy legislation, limiting appeals to matters of jurisdiction and questions of law only. A body that deals exclusively with privacy concerns has a greater ability to develop consistent jurisprudence. Such a body is also better able to ensure an accessible and transparent process, ultimately strengthening the effectiveness of the legislation as a whole.[41]

This approach has been taken in several jurisdictions, including Quebec and certain EU member countries. For example, Quebec Legislation includes a well-built enforcement mechanism whereby decisions made by the *Commision d'accès à l'information* are final, except for questions of law and jurisdiction.[42] The EU *Directive* also establishes a strong basis for enforcement regimes. In the UK, for example, the Information Commissioner has the authority to issue an enforcement notice detailing what violations need to be resolved and when they are not followed,

---

38 Micheal Geist "Weak enforcement undermines privacy laws" *Toronto Star* (19 April 2004), online: The Star <http://www.thestar.com>.

39 *PIPEDA*, *supra* note 19 Part 1 divisions 2 through 4.

40 Christopher Berzins, "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building" (2002) 27 Queen's L.J. 609 at 636-637.

41 *Ibid*. at 641.

42 *Quebec Legislation*, *supra* note 18 s. 61(1) and 61(3).

the complainant may take an action in either the Magistrate's Court or in the Crown Court.[43]

Nevertheless, irrespective of the adjudicating body, enforcement is fully dependant on consumers' willingness to pursue commercial organizations.

III. Self-Regulation

Part III of this paper attempted to demonstrate that legislation, on its own, is ineffective in protecting a user's consent to having his or her information collected, balancing the burden of protection and establishing adequate enforcement schemes. The following part of this paper will address certain areas where industry self-regulation may be more effective at protecting online privacy.

The U.S., as per the Federal Trade Commission, has encouraged the Internet industry to take a self-regulatory approach in addressing consumer concerns regarding the collection and use of personal information.[44] Industry attempts aimed at protecting privacy on the Internet include the use of online privacy policies, operation of opt-in processes, integration of P3P technology,[45] and certification of online privacy seal programs. In evaluating mechanisms aimed at regulating the collection and use of personal information in the private sector, the discussion will follow the three objectives discussed earlier: consent, burden and enforcement.

A. Protection of User Consent

Online privacy policies are prevalent on most websites today. Most organizations include information relating to their online collection practices and use of personal information in online privacy policies posted on their websites. In most cases, such policies are accessed via a link at the bottom of the website's main page. Their intended purpose is to inform the user of the website's privacy practices in order to limit the organization's potential liability. One fundamental flaw, however, lies in whether such forms of agreement are in effect binding and where they are, whether the scope of the user's consent is effectively weighed.

To begin, what kind of relationship exists between an organization and a user visiting its website? Does the mere availability of a privacy policy constitute the terms of a contractual relationship? It is established that a shrink wrap license, placed on a box of computer software, serves to bind a consumer to the full terms of the license included inside the box, subject to contractual terms that would otherwise be enforceable.[46] It is recognized that click wrap licenses, where a user must click on an

---

43 See Charlie Wood *et al.*, "Great Britain" in Gerald Spindler and Pritjof Börner, ed., *E-Commerce Law in Europe and the USA* (Berlin: Springer, 2002) 241 at 303.

44 See Milina, *supra* note 12 at 266.

45 For further information on this subject, see Part B, below.

46 See George S. Takach, *Computer Law*, 2nd ed. (Toronto: Irwin Law, 2003) at 283. See also *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 at 1449 (7th Cir. 1996).

"I agree" icon during installation of software, also serves to enforce the full terms of the software license.[47] However, can the presence of an online privacy policy be analogous to the enforceability of shrink wrap and click wrap licenses?

A 2002 American appellate decision indicates that it is unlikely that browse-wrap licences are enforceable. In *Specht v. Netscape Communications Corp.*[48] (*Specht*), the plaintiff downloaded free software from the defendant's website, where the software's license terms were only presented at the bottom of the web page. The Court found that "a reasonably prudent Internet user in circumstances such as these would not have known or learned of the existence of the license terms before responding to the defendant's invitation to download the free software, and that defendants did not provide reasonable notice of the license terms."[49] Accordingly, the presence of an online privacy policy may only serve to define the terms of a contractual relationship in circumstances where the user is presented with an explicit opportunity to accept or reject those terms.[50]

Reliance on online privacy policies without a clear opportunity for the user to accept or reject the terms included therein threatens the viability of a user's right to privacy online. Where no contractual relationship is clearly defined or enforceable, the organization is free to disregard its commitments without fear that it will be liable for a breach of contract. Additionally, organizations have the ability to set out a wide ambit in their policy in an overly technical manner and can amend their policy as needed.

B. Balancing the Burden of Protection

In assessing the allocation of burden in protecting online privacy, it is evident that the practice of making a privacy policy available on a website places an excessive burden on users. In order to be effective, users must locate and read the privacy policy of every website that he or she visits in order to inform themselves of that website's privacy practices. Additionally, as is discussed below, the use of opt-out policies incorporated into many websites places a heavy burden on users to ensure an adequate level of protection while online.

Opt-out policies are designed to provide users with the option to opt out of an organization's online data collection practices. Where a user does not want his or her personal information to be shared with a third party, the user can opt out by expressly communicating this choice (usually by downloading an opt-out cookie). Many organizations argue that an opt-out system serves to strengthen the user's

---

47 See *Rudder v. Microsoft Corp.* (1999), 2 C.P.R. (4th) 474, 40 C.P.C. (4th) 394 (Ont. S.C.J.). See also *Electronic Commerce Act*, S.O. 2000, c. 17, s. 19(1) (the section iterates that an offer or acceptance of an offer can be expressed by "touching or clicking on an appropriate icon or other place on a computer screen").

48 *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002).

49 *Ibid*. at 20.

50 See Barry B. Sookman, *Computer, Internet and Electronic Commerce Law* (Toronto: Carswell, 2002) at 10-18.1.

consent to have their personal information collected, on the basis that if a consumer does not opt out, they are implicitly consenting to the terms of the agreement.[51] This type of reasoning is similar to the contentions surrounding the reliance of online privacy policies. However, for users to exercise such an opt-out option, they need to be aware of it and of the implications underlying their acquiescence to it. This, in and of itself, may be unreasonable on the basis that most Internet users are not aware that websites are collecting user information. And even where Internet users may be aware of data collection practices, they may not be aware of the extent to which such data can be manipulated and processed.[52] As iterated in *Specht*,[53] where a user is not provided with an explicit opportunity to make an informed decision, the scheme may not be enforceable.

There are other industry mechanisms designed to reduce users' burden of protecting their privacy online. Such practices include opt-in policies, the integration of P3P compliant privacy notices and certification by online privacy seal providers.

An opt-in policy, in contrast to an opt-out policy, requires that users perform an explicit function in order to opt in to the website's data collection practices. Rather than having the website, by default, set at automatic collection, the organization needs to entice users to allow them to collect certain types of identifiable information.

Similarly, another industry mechanism available to remove excessive burden on users is the integration of P3P compliant browsers and online privacy policies. The Platform for Privacy Preferences (P3P) is a new language that "is designed to enhance the privacy of computer users by making website privacy policies more transparent, allowing people to make intelligent choices about which sites they visit."[54] P3P is a computer protocol that would enable Internet browsers to translate the provider's online privacy policy. This type of technology avoids a large number of concerns discussed earlier:

> Once informed of the site's information collection practices, consumers can avoid sites whose policies they find inadequate without spending a lot of time struggling to understand the extensive legal jargon contained in a typical site's privacy policy. In effect, sites with substandard policies will be provided strong incentives to catch up consumer demands, thus stimulating the creation of a 'privacy market'.[55]

P3P is designed in a manner whereby users have the ability to set their privacy preferences on their P3P enabled Internet browsers. While surfing the web, the browser continuously compares the user's privacy preferences with the P3P compliant privacy policies attached to each website. The user is made aware of any

---

51 See McClug, *supra* note 15 at 133.

52 See Schwartz, *supra* note 9 at 2078; Jeff Sovern, "Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information" (1999) 74 Wash. L. Rev. 1033.

53 *Supra* note 50 at 20.

54 McClug, *supra* note 15 at 92-93.

55 Milina, *supra* note 12 at 280.

websites where the privacy policy does not meet their privacy requirements as set out in their browser. However, the majority of websites have not converted their HTML-based privacy policies, which is integral to the effectiveness of P3P as a protective tool.

C. Adequacy of Enforcement Scheme

As discussed in Part III of this paper, enforcement mechanisms incorporated into legislative schemes are problematic. A number of factors, including a lack of resources, prevent governmental agencies from ensuring that fair practice principles are being followed. As a result, legislative attempts at protecting the right to privacy online equate to complaint driven regimes, effectively placing the burden on consumers, the weakest of the parties involved. However, the realm of industry initiatives at enforcing online collection practices has evolved into a promising industry of its own. The business of managing online privacy seals was first initiated by TRUSTe in 1997 and has been followed by many others, including BBBOnline and WebTrust.

Online privacy seals act as intermediaries between the user and the website's owner. As the intermediary, the seal provider vouches for the collection practices referred to in the website's privacy policy. When a user visits a website, the user can verify whether that organization is a member of a certain seal. Compliance is necessary to maintain a seal and a seal provider's livelihood depends on its continued reputation. Where the seal maintains a strong reputation in the market, the user can associate their trust in the seal with the website. This creates a market incentive for companies to attain such seals in order to remain competitive. User confidence is essential for further growth in e-commerce and online privacy seals are a way to instil confidence in users.

Despite a promising position in the market for online privacy protection, privacy seals have yet to overcome various shortcomings. As users may not generally be aware of the various implications surrounding online privacy policies and seal programs and as seal programs themselves are not specifically regulated, their internal policies may lack the necessary measures to ensure that a user's right to privacy is fully protected. For example, of the three above-mentioned privacy seals, at the time this article was written, none would meet all the requirements as set out in PIPEDA.[56] Since such seals are an effective manner for enforcement of company privacy policies, one type of seal that may be effective for Canadians is the development of a Canadian privacy seal that meets the requirements of PIPEDA and other provincial legislative schemes.[57] This will be further discussed in the following section when assessing recommendations.

Current industry mechanisms aimed at protecting online privacy are inadequate on their own. Reliance on online privacy policies and opt-out policies fails

---

[56] See MacDonell, *supra* note 3 at 385.
[57] *Ibid*.

to properly seek a user's consent to a website's data collection practices and places an undue burden on the user to locate, read and understand the policy itself. While opt-in policies and P3P compliant privacy notices have a better opportunity to attain a user's consent in a non-burdensome manner, the effectiveness of such mechanisms depends on the willingness of organizations.[58]

*** * ***

In evaluating the effectiveness of legislative and self-regulatory approaches aimed at protecting privacy on the Internet, this paper contends that neither ideology, on its own, provides an adequate level of protection to individuals. Both government and industry have a responsibility to protect a user's right to privacy online. The following section will outline several recommendations, attempting to find the right balance between effective legislation and efficient self-regulation.

Firstly, the enforcement provisions within PIPEDA need to be strengthened. While there are clear constraints on PIPEDA, including the growth of e-commerce and limited resources, the effectiveness of the legislation as a whole relies on its enforcement. The creation of a binding privacy tribunal, as is provided in the Quebec Legislation and in various EU jurisdictions, provides a more efficient framework to handle privacy complaints. A privacy tribunal with the authority to issue binding decisions provides a logical framework for resolving privacy complaints. As information technology continues to push the boundaries of privacy on the Internet, a body that is able to develop consistent and expedient jurisprudence can better produce a greater level of awareness among individuals, businesses and other government bodies.

Secondly, the Privacy Commissioner's Office needs to take a more proactive role in stimulating pressure on industry players to improve their privacy practices. This entails a greater educational role for the Commission. Through education, Internet users in Canada may be in a better position to put pressure on the market to institute more effective privacy protection schemes, such as further incorporation of opt-in policies.

As mentioned previously, the integration of opt-in policies, in contrast to opt-out policies, requires that users perform an explicit function in order to opt in to the website's data collection practices. This can effectively put pressure on the industry to entice users to opt-in, which invariably will have an effect on how the collection and use of data is handled. Additionally, such an approach maintains the flexibility to adapt and grow. As online privacy notices are now second nature to any website and most organizations take their privacy policies seriously, so too could opt-in policies become common.

---

[58] McClug, *supra* note 15 at 94.

The Canadian Internet Registration Authority (CIRA) is the body that manages the dot-ca domain. As Professor Geist notes, in the midst of re-evaluating its policy on public access to domain name registration information, CIRA will no longer require that such information be publicly available through its directory service.[59] Rather, registrants will have the option to opt-in to have their information included in the directory.

Thirdly, the development of a Canadian privacy seal should be considered by the Privacy Commissioner as a useful program to initiate. As there are various legislative schemes in place throughout Canada, it is difficult for Internet users to understand their implications and the differences between them. It is even a greater constraint for most businesses as online services transcend borders. A Canadian seal that meets the requirements of PIPEDA and other provincial legislative schemes would prove beneficial to both individuals and industry players. Users would be able to quickly determine whether a website is compliant with Canadian privacy legislation. Further, businesses would be able to design their privacy practices based on the specifications set by the seal authority, rather than evaluating each legislative scheme within Canada. Where the seal maintains a strong reputation in the market, the user can associate their trust in the seal with the website. This would create a market incentive for companies to attain such seals in order to remain competitive.

Information technology continues to push the boundaries of privacy protection. The Internet is distinctive; it is a world of its own. It should not be regarded in terms of conventional ideologies. A multi-faceted approach would be more effective in both protecting the right to privacy on the Internet and in establishing a flexible framework to meet future needs and concerns that arise from developments in information technology.

---

[59] Michael Geist, "Dot-ca privacy plan a Canadian compromise" *Toronto Star* (22 November, 2004), online: The Star <www.thestar.com>.