CRIMINAL LAW QUARTERLY
VOL. 51 (4)
2007

THE MEDIUM AND THE MESSAGE: PERSONAL PRIVACY AND THE FORCED MARRIAGE OF POLICE AND TELECOMMUNICATIONS PROVIDERS

Daphne Gilbert,[*] Ian R. Kerr [**] and Jena McGill[***]

1. Introduction

In July of 1993, a now famous cartoon was published in the New Yorker magazine.[1] The cartoon depicts a large black pooch with big floppy ears, sitting on an office chair in front of what is, by today's standards, a rather clunky PC. The pooch – who is talking to a smaller and extremely attentive pup – remarks that, "On the Internet nobody knows you're a dog." Besides being humorous, the cartoon demonstrated an important cultural discovery – in 1993, converging communications technologies created the possibility of online anonymity.

There is a less famous but perhaps more telling cartoon that appeared in April of the Year 2000, riffing on the observation

[*] Assistant Professor, Faculty of Law, University of Ottawa (*dgilbert@uottawa.ca*).
[**] Canada Research Chair in Ethics, Law & Technology, Faculty of Law, Faculty of Medicine, Department of Philosophy, University of Ottawa (*iankerr@uottawa.ca*).
[***] LL.B/M.A. candidate, Faculty of Law, University of Ottawa and Carleton University's Norman Paterson School of International Affairs (jmcgi032@uottawa.ca). The authors wish to express their thanks to the Social Sciences and Humanities Research Council, the Canada Research Chairs program, Bell Canada and the Ontario Research Network in Electronic Commerce for their generous contributions to the funding of the research project from which this article derives. Special thanks also to Dr. Hilary Young, Rafal Morek, Max Binnie, and Cynthia Aoki for their extraordinary efforts, their brilliance, and for the high quality of research support that they so regularly and reliably provide.

1. Peter Steiner, "On the Internet, nobody knows you're a dog" *The New Yorker* (July 5, 1993), p. 61.

made by those two dogs seven years earlier. In the Year 2000 cartoon, one dog opines to the other that, "The BEST thing about the Internet is THEY don't know you're a dog." But, as those words are barked, a voice from within the computer responds to the talking dog: "You're a four year old German Shepard-Schnauzer mix, likes to shop for rawhide chews, 213 visits to Lassie Web site, chatroom conversation 8.29.99 said third lassie on the right was hottest, downloaded 3rd Lassie 10.12.99, E-mailed them to 5 other dogs whose identities are…"[2]

This response signifies an important shift not only in the culture of the Internet but also in its architectures. As the second cartoon illustrates, there is often a commercial interest in knowing who is doing what online. In furtherance of this interest, persistent client state http cookies[3], keystroke monitoring[4] and a number of other surveillance technologies have been developed to gather data and otherwise track the movement of

2. Tom Toles, "Did you mark all that?" *Buffalo News* (April 9, 2000), online at <http://www.ucomics.com/tomtoles/>.

3. An http cookie is a simple package of data sent by a server to an Internet browser and then sent back by the browser each time it accesses the server. Cookies are typically used for user authentication, user tracking, and maintaining user-specific information including website preferences and electronic shopping carts, though they can also be used for network attacks. Cookies are a concern for Internet privacy since they can be utilized to unknowingly track the Internet browsing patterns of an individual. Cookies may then be used to compile a profile of a user's preferences that is made available to advertising agencies without the user's permission. Cookies are the subject of legislation in the United States and the European Union (*Wikipedia*, online at: <http://en.wikipedia.org/wiki/Http_cookies>).

4. Keystroke monitoring, or 'keylogging', is a diagnostic used in software development that picks up a user's keystrokes, or typing patterns. It can provide access to a user's passwords or encryption keys, bypassing other security measures and making it useful in identifying sources of error in computer systems, and in law enforcement and espionage. However, keyloggers in both hardware and software forms are widely available on the Internet and can be used for these same purposes by individuals who can download another's keystroke data without being traced. The privacy implications of such attacks are plentiful, as the keylogger may be able to record and access passwords for email accounts, online banking and credit cards without the permission of the individual being traced (*Wikipedia*, online at: <http://en.wikipedia.org/wiki/Keylog>).

potential online customers.[5] Such curiosity, however, is not unique to business. Concerned that computer networks and electronic information may also be used for committing criminal offences (and knowing that evidence relating to such offences may be stored and transferred through these networks), many countries[6] are considering[7] the adoption of or have already enacted legislation that would require telecommunications service providers[8] (TSPs) to build a communications infrastructure which would allow law enforcement agencies to gain access to the entirety of a specific telecommunication transmitted over their facilities.

In this article, we describe the changing role of TSPs from trusted stewards of clients' personal information to "agents of the state", from gatekeepers of privacy to active partners in the fight against cybercrime. We argue that the legislative

---

5. Associated Press, "Man Charged: e-Snooping on Wife", *Wired (*September 6, 2001), online at <http://www.wired.com/news/privacy/0,1848,46580,00.html>; S. Olsen, "Dot-coms See Gold in Consumer Data" *c|net News.com (*October 24, 2001), online at <http://news.com.com/2100-1023-274923.html>.
6. The legal blueprint from which many countries will derive such legislation is the Council of Europe's *Convention on Cybercrime* Council of Europe, Committee of Ministers, ETS No. 185 (November 23, 2001), online at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, which will be discussed further below.
7. Canada is among those countries that have considered adopting such legislation. In fact, the former Government of Canada proposed Bill C-74, the *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2004. Although Bill C-74 is no longer under consideration due to a recent change in Government, it is expected that a substantially similar form of legislation will be tabled by the new Government in the near future. In this article, we will use Bill C-74 as a model representative of the sort of approach that Canada is likely to adopt.
8. This article refers to "telecommunications service providers" rather than the narrower category of "internet service providers" (ISPs) and thereby reflects the language of Bill C-74. The term "TSPs", as defined in Bill C-74, includes both ISPs and providers of other telecommunications services, such as mobile telephone companies. It should be pointed out, however, that the role of ISPs differs from that of other TSPs, particularly those operating solely in the offline environment, in many important ways. For a comprehensive analysis of the role of ISPs and their specific relationship with Internet users, see: Ian R. Kerr, "Personal relationships in the Year 2000: Me and My ISP" in N. des Rosiers, ed., *No Person Is an Island: Personal Relationships of Dependence and Independence* (Vancouver: University of British Columbia Press, 2002), p. 78 (Kerr, *Me and My ISP*).

approach that has been or will soon be adopted in various jurisdictions around the world, including Canada, will lower the threshold of privacy protection and significantly alter the relationship between TSPs and the individuals who have come to depend on them to manage their personal information and private communications.

We begin with a brief investigation of the role of TSPs as information intermediaries. Then we examine a Canadian online search and seizure case, where a TSP acted as an "agent of the state" by sending to the police copies of a client's personal emails without his knowledge or consent.[9] We suggest that the *R. v. Weir* decision foreshadows a shift in the regulatory culture wherein TSPs will be expected to assist law enforcement agencies by providing them with expedited access to Internet users' personal information and private communications.

Next, we briefly examine the Council of Europe's *Convention on Cybercrime*, an instrument that calls for state signatories from around the world to ratify and implement provisions that will mandate a new marriage between telecommunications service providers and the police, bringing about a further shift in the landscape. Focusing on its potential implementation in Canada, we argue that Bill C-74[10] would lead to a lower threshold of privacy protection: there will be no judicial oversight of law enforcement's collection of certain kinds of information from TSPs, rendering the constitutional safeguards offered by the traditional "agent of the state" analysis irrelevant. Once these new cybercrime laws are passed in Canada, the only recourse may be to challenge their constitutionality based on the Canadian *Charter of Rights and Freedoms*,[11] which protects citizens against unreasonable search and seizure.

Finally, we conclude by considering the privacy implications of the evolving roles of TSPs and their shifting technological architectures. Privacy invasive practices which used to happen infrequently and with judicial oversight will soon become part

---

9. *R. v. Weir*, [2000] A.J. No. 527 (QL), 1998 ABQB 56 (Q.B.).
10. *Supra*, footnote 7.
11. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c.11, s.8 (the Charter).

of TSPs' business routine. In our view, the evolving roles of TSPs and the shifting architecture of our communications infrastructure must be built with various safeguards that will not only further the goals of national security and law enforcement but will also preserve and promote personal privacy.

2. Disintermediation

For nearly a decade, scholars have focussed their attention on the Internet as an instrument of *disintermediation*.[12] Recognizing that intermediaries are valuable to a transaction only if they are as inexpensive as equivalent functions found in an open market, many scholars have in fact predicted that the Internet – which reduces transaction costs by allowing direct interaction between manufacturers and consumers[13] – will have the effect of "killing the man in the middle."[14] Consider the following typical statement:[15]

---

12. It has been suggested, for instance, that the Internet made it possible for independent musicians and composers to make recordings of their work easily available for sampling and download. See for example: <http://www.garageband.com>). Similarly, writers are able to use digital networks to publish works directly. Stephen King's *The Plant* is probably the most famous example of the direct distribution model. See: M.J. Rose, "Stephen King's *Plant* Uprooted" *Wirednews* (November 28, 2000), online at <http://www.wired.com/news/culture/0,1284,40356,00.html>. As another example, Internet direct public offerings would represent disintermediation of the public offering market. See: William K. Sjostrom, Jr., "Going Public Through An Internet Direct Public Offering: A Sensible Alternative For Small Companies?" (2001), 53 Fla. L. Rev. 529. See also generally: Andrew L. Shapiro, "Digital Middlemen and the Architecture of Electronic Commerce" (1998), 24 Ohio N.U.L. Rev. 795.
13. Users (consumers) and providers (manufacturers) seek to "eliminate the middleman" to eliminate the costs associated with an intermediary function. The normal distribution chain of consumer goods is expensive to maintain and typically adds little value relative to the cost it imposes on the ultimate customer. This disintermediation of the "middleman" is one of the primary drivers of low-cost transactions on the Internet – See Walid Mougayar, *Opening Digital Markets: Battle Plans and Business Strategies for Internet Commerce* (New York: McGraw-Hill, 1998) pp. 29-32. For an interesting exploration of the persistence of intermediaries, see also Saul Levmore, "Efficient Markets and Puzzling Intermediaries" (1984), 70 Va. L. Rev. 645.
14. See for example: DePaul University's MIS 680 E-commerce Fundamentals (July 14, 2005), online at <http://www.versaggi.net/ecommerce/disintermediation/>.
15. N. Negroponte, "Reintermediated" (September 1, 1997), online at <http://web.media.mit.edu/~nicholas/Wired/WIRED5-09.html>.

> Unlike tomatoes or cars, real estate listings, stock quotations, and airline schedules are bits, easily and inexpensively shipped at the speed of light. Bits need no warehousing, and the cost to make more is effectively zero. For this reason, real estate agents, stockbrokers, and travel agents will disappear much more rapidly than food wholesalers or car dealers.

While it is perhaps true that the disintermediation phenomenon occurs in the context of some business transactions, disintermediation is *clearly not* a universal by-product of Internet communications.[16] In fact, online intermediaries remain quite relevant to other aspects of almost every networked communication. TSPs are the Internet's "middlemen." Because TSPs are the pipeline through which all of our telecommunications must flow, they are in a position of control. As technology improves and storage becomes cheaper, TSPs are increasingly in a position to observe and record everything that we say and do online. Thus we are forced to depend on them, not only to provide quality informational services but also to safeguard our personal information and private communications and to prevent that information from falling into the hands of third parties.[17] This gives TSPs power and discretion: power to control our online behaviour; and discretion to alter our outcomes.[18]

The shifting architectures of the networked world currently allow TSPs automatic access to their customers' and employees' personal information and private communications in a manner unparalleled by even the most powerful financial institutions or

---

16. For an overview of the opposing trends of disintermediation and reintermediation, see for example Alina M. Chircu & Robert J. Kauffman, "Strategies for Internet Middlemen in the Intermediation/Disintermediation/Reintermediation Cycle" in Beat F. Schmid *et al.*, eds., *EM - Electronic Commerce in the Americas & Local versus Global Electronic Commerce* 9 No. 2 (1999), online at <http://www.electronicmarkets.org/modules/pub/view.php/electronicmarkets-140>, or Julia King, "Disintermediation/Reintermediation" *Computerworld* 54 (December 13, 1999), online at <http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,37824,00.html>.
17. See Kerr, *supra*, footnote 8.
18. For an elaboration on this point see Ian R. Kerr, "Online Service Providers, Fidelity and the Duty of Loyalty" in B. Rockenbach & T. Mendina, eds., *Ethics and Electronic Information: A festschrift for Stephen Almagno* (Jefferson, North Carolina: McFarland & Co., 2003), p. 166.

arms of government. As will be further discussed below, one of the central strategies of the *Convention on Cybercrime* and corresponding legislation likely to be enacted in various jurisdictions around the world is to mandate a communications infrastructure that would allow law enforcement agencies to capitalize on the informational power of TSPs. In this respect, TSPs already play and will continue to play an absolutely critical role as *information intermediaries*. They are the stewards of our personal information and private communications. This fact is illustrated by a well-known Internet case in Canada: *R v. Weir*.[19]

3. TSPs as "Agents of the State"

Prior to the case of *R. v. Weir*, it was not clear how TSPs' role as intermediary would be understood in Canadian criminal law. In *Weir*, the defendant's TSP was found to be an "agent of the state."[20] The case therefore represented an important shift in TSPs' role in the investigation of crime. The facts of this case are as follows.

Having inadvertently exceeded his available disk quota, Mr. Weir was having trouble accessing his e-mail. Trusting his TSP to fix the problem on his behalf, Weir called to request the assistance of a technician and then went off to work. While Weir was at work, the technician discovered the problem. Mr. Weir had too many e-mails with large attachments residing on the host server. The excessive size of these files automatically disabled his account. The technician approached the problem in the standard way. Files were opened so that the attachments could be moved off the server. In so doing, the technician discovered that the names of certain files sent to Mr. Weir that

19. *Supra*, footnote 9.

20. An agent of the state is a person who is authorized to act for or in place of the state. Crown Attorneys and police officers who exercise statutory powers as agents of the government qualify as agents of the state. Canadian courts have been strict in defining and affirming the circumstances under which a person may be considered an agent of the state, requiring an identifiable, direct relationship between the agent and the state that can be found in a statute or clearly shown by convention. The agent of the state doctrine is particularly significant in Canadian criminal law and constitutional law, where it arises frequently with respect to an accused's right to remain silent, as embodied in s. 7 of the Charter. See for example *R v. Broyles*, [1991] 3 S.C.R. 595, 68 C.C.C. (3d) 308, 9 C.R. (4th) 1.

day sounded suspiciously like titles typical of child pornography. The technician informed his manager of his discovery who, in turn, decided to alert the Edmonton police. Without any form of warrant, the police insisted that the TSP forward copies of the files. It further instructed the TSP to re-enable Mr. Weir's account so that the files that he had been sent (but had not yet received) would come to be in his possession.[21] Weir's TSP capitulated to the demands of the police.

While there was a time when most observers would have said that TSPs must protect their client's privacy interests and that, absent a court order, TSPs have no business handing over personal communications to the police, the facts of the *Weir* case might be described as prescient of the role that TSPs are being asked to play in law enforcement with increasing frequency on a global scale. On the basis of the transactions that took place between his TSP and the police, a search warrant was obtained and Mr. Weir's computer was seized.[22] What is so telling about this case is that it was initiated entirely *at the discretion* of the TSP. Because it was the pipeline through which all of his private communications must flow, Weir's TSP was in a position to know the content of his and the sender's online communications and was in a position to choose whether to contact the police or let customers go about their private business. The important point to be gleaned from this case is that, *in the context of investigatory information, the architecture of the Internet does not disintermediate.* Rather, it has quite the opposite effect. It requires a TSP to *intermediate* between two potentially conflicting roles: (i) its role as the trusted steward of its clients' personal information and private communications; and (ii) its role as a party in possession of information that might assist in law enforcement.[23] The TSP is, in other words, the medium *and* the message.

---

21. Note that the files forwarded to the police were not yet in Mr. Weir's possession, as they had not yet been downloaded to his inbox. This is because his account had been disabled as soon as his available disk quota was exceeded.
22. Ironically, the warrant upon which the police were authorized to search and ultimately seize Weir's computer was itself founded on e-mails that he had neither received nor possessed. In fact, it remains unclear whether Weir knew at the time that the e-mails had been sent to him.
23. Needless to say, the role of TSPs is multifaceted. This article focuses on certain aspects of TSPs' relations with private citizens and state authorities. It does not

At trial, defence counsel argued that Weir had a reasonable expectation of privacy in his e-mail, as well as a constitutional right to be secure against unreasonable search and seizure. He argued that the manner in which the police used the TSP to obtain evidence against his client was unconstitutional. The trial court was not persuaded. Although it agreed that the police were constitutionally prohibited from conducting an unauthorized search, it held that the usual constitutional safeguards simply do not apply to searches conducted by a private sector service provider. According to Justice Smith:[24]

> …it cannot be said that the [TSP] was performing a governmental function. TSPs] are private organizations. They are unregulated… With international agreements, it may come to pass some time in the future that [TSPs] will be regulated … the wish found in Canadian Government documents for such regulation is no more than a 'pious hope' today.

Weir appealed this decision, arguing that the trial court erred in its finding that the TSP was *not* performing a governmental function. Relying on a doctrine in criminal law known as the "Broyles Test,"[25] Weir argued that his TSP was acting as an "agent of the state."

The agent of the state argument usually arises in the context of an investigation carried out by a private citizen. The most typical instance occurs when police send an informant rigged with a body pack into a holding cell with the aim of intercepting and recording a confession that is teased out of an accused. Where the accused has already invoked the right to silence and remains in the coercive environment of a jail cell, the agent of the state doctrine will prohibit the police from doing indirectly that which they cannot do directly. In such instances, the court will consider the collection of the evidence to be unconstitutional in

---

address concerns relating to the role of TSPs as independent market players and competitors. Yet it has become apparent that network providers may independently seek to interfere with the free flow of data on the Internet. Some TSPs have engaged in blocking or slowing data coming from competing sites or services. See: Michael Geist, "What Do You Want The Internet To Be?" *Toronto Star* (March 7, 2005), online at <http://www.michaelgeist.ca/resc/html_bkup/mar72005.html>.

24. *Supra*, footnote 9, at pp. 46 and 49.
25. *Broyles*, *supra*, footnote 20.

spite of the fact that it was obtained not by the police but by a private citizen. Although private citizens do not generally owe the same constitutional duties that are owed by the police, where the informant is carrying out a police-type function, he or she is considered an agent of the state and the evidence is therefore inadmissible. The test for whether a private informer is acting as an agent of the state in Canadian law[26] is as follows: "would the exchange between the accused and the informer have taken place, in the form and manner in which it did take place, but for the intervention of the state or its agents?"[27]

Applying the above test to the facts in the *Weir* case, the Court of Appeal held that the TSP was acting as an agent of the state when it forwarded, at the request of the police officer, a copy of the messages sent to Mr. Weir. On the basis of this finding, the Court of Appeal held that the police's subsequent search of Weir's home was unwarranted.

The application of the "agent of the state" doctrine to TSPs was extremely significant. By treating TSPs who cooperate with law enforcement as state agents, the courts have recognized the shifting role of TSPs. TSPs and other information intermediaries are no longer in a position to promise absolute confidentiality to their clients or to act as the guardians of their

---

26. In both Canadian and U.S. law, the decision about whether a person is "an agent of the state" has been traditionally made by considering all of the circumstances on a case-by-case basis. As Stout notes, under U.S. law, there is no bright-line test that distinguishes government conduct from private conduct. A search by a private individual may fall under the Fourth Amendment if "a government official affirmatively facilitates or encourages an unreasonable search performed by a private person." Thus, a certain degree of participation is required before a private citizen is transformed into an agent of the state. This participation must be more than incidental contact between the citizen and law enforcement agents before the search will be subject to Fourth Amendment analysis. Two factors that courts consider when determining whether the private person is an agent or instrument of the state are whether the government knew of, and acquiesced in, the intrusive conduct, and whether the party performing the search intended to assist law enforcement efforts or to further his or her own ends. The burden of establishing that the government involvement was sufficient to alter the character of the search is on the party objecting to the search. See generally Emily Michael Stout, "Bounty Hunters As Evidence Gatherers: Should They Be Considered State Actors Under The Fourth Amendment When Working With The Police?" (1997) 65 U. Cin. L. Rev. 665 at pp. 673-674.

27. *Broyles*, *supra*, footnote 20, at p. 24.

informational privacy. Nor are TSPs merely the conduit through which their clients' personal information and private communications flow. Rather, TSPs are a reservoir of personal information and private communications – a reservoir that can and will be tapped by the state for the purposes of law enforcement.

It is our position that the shifting nature of the relationship between TSPs and the state must be further studied and understood, as it clearly alters the manner in which investigatory information is collected in the context of criminal law in a way that affects personal privacy. Ironically, the importance of the *Weir* decision will be diminished – if not completely eclipsed – by the further shift in this relationship that will follow from the implementation of the *Convention on Cybercrime*, which calls for expedited procedures as well as lower standards of accountability in the collection of private information by TSPs. However, the *Weir* decision remains significant precisely because the proposed cybercrime legislation undermines *Weir*'s privacy-protecting agent of the state analysis.

4. The Convention on Cybercrime and its Implementation in Canada

On November 23, 2001, members of the Council of Europe, and several non-member States, signed the *Convention on Cybercrime* (the *Convention*).[28] The *Convention* is premised on a concern that computers can be used to commit criminal offences and on the fact that information stored or transmitted through computer systems might provide evidence of a crime.[29] Consequently, the *Convention* stresses the need for international cooperation in the detection, investigation and prosecution of

28. *Supra*, footnote 6. The Convention went into effect on July 1, 2004. Signatory nations as of December 1, 2005: Albania (ratified), Armenia, Austria, Belgium, Bosnia-Herzegovina, Bulgaria (ratified), Canada, Croatia (ratified), Cyprus (ratified), Czech Republic, Denmark (ratified), Estonia (ratified), Finland, Former Yugoslav Republic of Macedonia (ratified), France (ratified), Germany, Greece, Hungary (ratified), Iceland, Ireland, Italy, Japan, Latvia, Lithuania (ratified), Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania (ratified), Serbia and Montenegro, Slovakia, Slovenia (ratified), South Africa, Spain, Sweden, Switzerland, Ukraine, United Kingdom and United States.

29. *Supra*, footnote 6 at para. 6, Preamble.

criminal offences and the corresponding need for investigatory powers,[30] recognizing "…the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies."[31]

Importantly, the *Convention* also emphasizes human rights, including rights to freedom of expression and privacy, and it recognizes the need to protect personal data.[32] The *Convention*'s text demands two broad requirements: (i) measures at a national level to implement the *Convention*'s terms; and (ii) international cooperation to investigate criminal offences.

In Chapter II ("Measures to be taken at the national level"), the *Convention* divides its requirements into substantive and procedural criminal law. The substantive criminal law section asks signatories to create several offences, including unlawful interception, access or interference with a computer system computer-related forgery and fraud, and offences relating to child pornography and copyright. The procedural law section is our current focus. It outlines potentially sweeping new investigatory powers for law enforcement and mandates access to all information stored and transmitted on computer systems. Access to this information will be facilitated by TSPs.

While governments call for expedited access to Internet communications and find the *Convention* useful in their efforts against terrorism[33], privacy experts have made their opposition clear. *Convention* supporters claim that the *Convention* "provides

30. *Ibid.*, at paras. 8 -9, Preamble.
31. *Ibid.*, at para. 7, Preamble.
32. *Ibid.*, at paras. 10-11, Preamble.
33. Since the most recent terrorist attacks in London in July 2005, Great Britain and certain other countries have been calling for new legislation forcing TSPs to store the details of all e-mail and mobile phone communications for up to three years, so that they can be accessed by the security services when hunting terrorists. See for instance: Simon Freeman, "EU agrees to speed up anti-terror measures" *Times Online* (July 13, 2005), online at <http://www.timesonline.co.uk/article/0,,22989-1692393,00.html>. Changes in legislation relating to the ability to monitor e-mails and text messages are also expected in countries that have not been directly affected by terrorism. See for instance: Michael Gordon, "The sum of our fears" *The Age* (July 30, 2005), online at <http://www.theage.com.au/news/war-on-terror/the-sum-of-our-fears/2005/07/29/1122144020660.html?oneclick=true> (citing the Australian Attorney-General Philip Ruddock).

useful measures to combat attacks by terrorists and other criminals on computer systems, as well as to gather electronic evidence of terrorism and other crimes."[34] If the Internet has made terrorist groups more dangerous and more effective,[35] new international mechanisms for combating terrorism would appear to be necessary.[36] Privacy advocates, on the other hand, argue that the *Convention* is contrary to well established universal norms for the protection of the individual (such as the right to privacy of communication[37], freedom of expression[38], or the right against self-incrimination[39]), that it improperly extends police

34. Ministry of Foreign Affairs of Japan, "G8 Recommendations on Counter-Terrorism," online at <http://www.mofa.go.jp/policy/economy/summit/2002/g8terro.html>.

35. See generally Jen Lin-Liu, "The Web Has Made Terrorist Groups More Dangerous, Scholar Says" *The Chronicle of Higher Education* (October 12, 2001), online at <http://chronicle.com/free/2001/10/2001101203t.htm>. For instance, in 2001, the FBI suggested that terrorist groups, including Osama Bin Laden's al-Qaeda organisation, could hide messages in some "innocent" web images. See: Will Knight, "Massive search reveals no secret code in web images", *New Scientist* (September 25, 2001), online:<http://www.newscientist.com/article.ns?id=dn1340>.

36. See for example Jennifer Stoddart, "Response to the Government of Canada's "Lawful Access" Consultations: Submission of the Office of the Privacy Commissioner of Canada to the Minister of Justice and Attorney General of Canada" (May 5, 2005), online at <http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp> (noting that the government argues that the lawful access regime needs to "simply restore a level playing field in the fight against increasingly sophisticated criminals.")

37. The *Universal Declaration of Human Rights*, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948) [*Universal Declaration*] speaks directly to the obligations of governments to protect privacy of communication. Article 12 states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."

38. Article 19 of the *Universal Declaration* further states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

39. Provisions in many constitutions and laws prohibit the government from requiring a defendant to testify or otherwise give evidence against himself. For instance, the Fifth Amendment to the United States Constitution (U.S. Const. amend. V) states that "[n]o person shall be ... compelled in any criminal case to be a witness against himself." In Canada, equivalent rights exist under Section 11(c) of the *Charter*, *supra* note 11, which provides one cannot be compelled to be a witness in a proceeding against oneself.

authority, and that it will reduce government accountability in future law enforcement conduct.[40]

Canada signed the Convention on November 23, 2001, and thereby agreed in principle to its provisions. However, the treaty is not legally binding until ratified, and, to that end, Canada began a review of its lawful access[41] laws in 2000.[42] In 2002, a public consultation document[43] was released which contained legislative proposals including: compelling TSPs to build the capability to intercept a specific users' communications[44]; compelling the disclosure of subscriber data without a warrant[45]; and creating specific production orders with a low standard of judicial review for traffic data.[46] Response to the proposals was largely negative, with civil libertarians, privacy

40. See for instance: "Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime" (October 18, 2000), online at http://www.gilc.org/privacy/coe-letter-1000.html, or TreatyWatch.org, "The Council of Europe Cybercrime Treaty", online at <http://www.treatywatch.org/>.

41. Neither the *Convention* itself, nor the Explanatory Report attached thereto, uses the term "lawful access." However, this term has been commonly used in Canada since the "Lawful Access Consultation" was launched in 2002. As explained by Canada's Department of Justice, "lawful access" is one of the techniques used by law enforcement and national security agencies, such as the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS) and municipal and provincial police forces, as well as the Competition Bureau, when conducting investigations. It involves the lawful interception of communications and the lawful search and seizure of information, including computer data. Communications and information may be intercepted from: wireline technologies (e.g. telephones); wireless technologies (for instance, cellular phones, satellite communications, and pagers); and Internet technology (such as e-mail). See Department of Justice Canada, "Lawful Access FAQ," online at <http://canada.justice.gc.ca/en/cons/la_al/summary/faq.html>.

42. Some commentators argue that Canadian legislative amendments concerning lawful access originated in the 1990s, before the *Convention* was signed. Later, they became more pressing in light of Canada's implementation of its obligations under the *Convention* and the perceived heightened threat of terrorism. See: Canadian Internet Policy and Public Interest Clinic, "Canadian government proposals for updating criminal laws and facilitating law enforcement in the electronic age", online: <http://www.cippic.ca/en/projects-cases/lawful-access/>.

43. Department of Justice Canada "Lawful Access Consultation Document" (August 25, 2002), online at <http://www.justice.gc.ca/en/cons/la_al/law_access.pdf>.

44. *Ibid*., at pp. 7-9.

45. *Ibid*., at pp. 12-13.

46. *Ibid*., at pp. 11-12. More information on "traffic data" can be found in subsequent sections of this article.

activists, individual citizens, and even TSPs arguing that the proposed measures went beyond existing lawful access capabilities, violated privacy rights, and that the need for such measures has not been proven.[47] Nevertheless, despite concerns raised by privacy groups and members of the public[48], in November of 2005 the Canadian government proposed Bill C-74, the *Modernization of Investigative Techniques Act*.[49] The Bill largely codifies the Department of Justice's original proposals with regard to subscriber information, and additional legislation is expected that will set out TSPs' obligations with regard to other kinds of information. Although the Bill died on the order page with the recent defeat of the minority Liberal government, members of the privacy community speculate that this will likely only delay rather than defeat Canada's enactment of legislation and the resultant ratification of the *Convention* in Canada.[50] Recognizing that the bill that will ultimately be proposed is likely to be substantially similar to Bill C-74, in the following analysis we utilize Bill C-74 as a model in examining the implications of such legislation on the privacy interests of Canadians.

(1) Investigatory Information

Bill C-74 is likely to have significant repercussions for informational privacy. This is in part due to the categorisation of different types of investigatory information in the original *Convention*, which loosely describes three types of information in its various Articles: (i) content data; (ii) traffic data; and (iii) subscriber data.[51] Though the most recently proposed Canadian

47. Both authors participated in this process, one of them filing written submissions. See: "Summary of Submissions to the Lawful Access Consultation" Chapter 4: Comments by Industry (August 2003), online at <http://www.justice.gc.ca/en/cons/la_al/summary/4.html>.
48. Philippa Lawson has described the 2005 proposals as "largely the same as 2002, but more detailed." See: Philippa Lawson, "Lawful Access Proposals" Powerpoint slides (May 2005), online at <http://www.cippic.ca/en/projects-cases/lawful-access/lawful_access_iclmg.ppt>.
49. *Supra*, footnote 7.
50. It remains to be seen whether the newly formed minority Conservative government will increase or diminish the privacy impact of the soon-to-be proposed Bill.
51. *Supra*, footnote 6.

model would have adopted a more formal approach to definition that further refines the categories, its general scheme is likely to remain substantially similar to the *Convention*[52]. The basic approach is to treat different categories of investigatory information differently, supposedly reflecting the varying expectations of privacy that people have with regard to various types of data. In part, this is because the measure of a user's expectation of privacy in information is crucial to whether a search and seizure of that information requires judicial pre-authorization (through a warrant or intercept order) and is thus constitutionally protected.[53] The categorization of investigatory information in the *Convention* has important implications for privacy protection and is explored below with specific reference to Bill C-74's treatment of subscriber data and its implications for informational privacy.

(2) Gradations of Privacy Protection

The three categories of investigatory information described in the *Convention* comprise the various types of information sought by law enforcement during the course of a typical investigation. According to the proposed scheme the highest level of investigatory information, worthy of the greatest privacy protection, is content data. This category would include the text of e-mail messages and might also include the search terms entered into an Internet search engine. The medium level of investigatory information sought by law enforcement is traffic data, defined as:[54]

> …any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

---

52. These categories were subsequently adopted in Canada in the Department of Justice's original Lawful Access Consultation paper, the "Lawful Access Consultation Document", *supra*, footnote 43.
53. In Canada it appears undisputed that users have a constitutionally protected expectation of privacy in the information processed by TSPs. Yet, under US law, it has been argued that individuals "have no reasonable expectation of privacy in the contents of records compiled and maintained by entities such as TSPs." See: Susan W. Brenner, "Distributed Security: Moving Away from Reactive Law Enforcement" (2005), 9 Int'l J. Comm. L. & Pol'y 11.
54. *Convention on Cybercrime, supra*, footnote 6, c. I, art.1, definition d.

Conceivably, traffic data would include the information carried in the sender, recipient and subject lines of an e-mail and its size (which would in turn reveal whether there are attachments to the e-mail). They could also include the title of attachments (which might then indicate by the extension whether the files were photographs or video clips), and the Web sites visited by a user and the time spent at each. Traffic data can therefore be understood as a roadmap of a user's Internet communications as one travels along the information superhighway. Finally, the lowest level of investigatory information, corresponding to the lowest expectation of privacy, is subscriber data. Bill C-74 describes subscriber data as "any information… respecting the name and address of any subscriber to any of the service provider's telecommunications services and respecting any other identifiers associated with the subscriber."[55] It is obligations concerning subscriber information that are put forward by Bill C-74.

(3) Obligations Concerning Subscriber Data

According to Bill C-74, law enforcement would be empowered to obtain subscriber data in an expeditious manner from TSPs simply by asking for it.[56] The Bill does not require any judicial authorization. Nor is there a requirement for reasonable grounds to suspect wrongdoing. All that is required under Section 17(1) of the Bill is a written request for subscriber data by a designated individual, and a TSP must turn over the

---

55. *Supra*, footnote 7, s.17(1).
56. In accordance with section 17(3) of Bill C-74, the request would have to be made by a person "designated" by the RCMP Commissioner, the Director of CSIS or the chief of a police service. Section 17(3) of Bill C-74 defines designated persons as including, "[t]he Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the Commissioner of Competition and the chief or head of a police service constituted under the laws of a province may designate for the purposes of this section any employee of his or her agency, or a class of such employees, whose duties are related to protecting national security or to law enforcement." Section 17(2) of the Bill specifies that a designated person will only make a request for subscriber information in performing "a duty or function a) of the Canadian Security Intelligence Service under the *Canadian Security Intelligence Service Act*; b) of a police service, including any related to the enforcement of any laws of Canada, or a province or of a foreign jurisdiction; or c) of the Commission of Competition under the *Competition Act*." See Bill C-74, *supra*, footnote 7.

"name and address of any subscriber to any of the service provider's telecommunications services and respecting any other identifiers associated with the subscriber."[57] In fact, in the expedited process anticipated by Bill C-74, no justification is required whatsoever.[58] An online service, such as Gmail, could be required by law to divulge the local TSP identification of an e-mail user. The local service provider would then be asked to identify the name, address and billing information of its client.[59]

When one considers that Canada's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) currently empowers TSPs to refuse such requests unless accompanied by judicial authorization,[60] one begins to see a significant alteration in the procedural safeguards against excessive fishing expeditions by law enforcement agencies. By removing this option and thereby forcing TSPs to engage in active partnerships with the police, Bill C-74 would leave TSPs with no choice but to turn over subscriber names and addresses in response to specific requests by police. The police would become entitled to an all-you-can-eat investigatory smorgasbord. In addition to the fact that it remains unclear who would

---

57. *Supra*, footnote 7, s. 17(1).
58. Section 17(2) of Bill C-74 requires that designated persons (police officers, for example) be acting in the course of their duties and 17(6) sets out that records must be maintained of the information requested, but otherwise the ability of designated parties to request subscriber information is almost unlimited.
59. In 2002, the government raised the possibility of a national subscriber information database. This proposal was not repeated in the 2005 proposal, nor in Bill C-74.
60. Pursuant to section 7(3)(c.1) of the Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c.5. (*PIPEDA*),

> an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law; or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province.

This has been construed as a discretionary authority such that law enforcement agencies cannot compel production without a warrant or a court order.

pay for all of this, it is worth noting that the legislation would also enable a *secret* binge-fest. In other words, TSPs could be prevented from disclosing to their customers the fact that such requests have been made, that information was provided, and would be precluded from disclosing any other information regarding the request, unless specifically required by law.

(4) Privacy Implications of Increased Access to Subscriber Data

While subscriber data may carry a lower expectation of privacy than other types of investigatory information (it has been likened to information that is available in a telephone directory), its significance and potential privacy implications must not be underestimated. Name and address are keys to acquiring other personal information, including highly sensitive data such as health or financial records. For example, in the United States, research at the Laboratory for International Data Privacy has shown that 87% of the US population can be uniquely identified with just a few pieces of personal information, for example, zip code, gender and date of birth.[61] In other words, by using subscriber data fields, easily accessible under Bill C-74, content and traffic data can be determined. Information collected and stored for one purpose can be combined with information collected and stored for a completely different purpose through data mining,[62] and two pieces of seemingly

---

61. Latanya Sweeney, "Comments to the Department of Health and Human Services on Standards of Privacy of Individually Identifiable Health Information" (April 26, 2002), online at <http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.html> See also: Latanya Sweeney, "Protecting Job Seekers from Identity Theft" (2006) 10(2) IEEE Internet *Computing* 74, and Latanya Sweeney, "AI Technologies to Defeat Identity Theft Vulnerabilities" *AAAI Spring Symposium*: *AI Technologies for Homeland Security* (2005), online at <http://privacy.cs.cmu.edu/dataprivacy/projects/idangel/idangel1.pdf>, describing Sweeney's Identity Angel, a technology that searches the internet and notifies "people for whom information, freely available on the Web, can be combined sufficiently to impersonate them in financial or credentialing transactions."

62. "Data mining" is defined as "the intelligent search for new knowledge (such as personally identifiable information) in existing masses of data." See: Joseph S. Fulda, "Data Mining and Privacy" (2000), 11 Alb. L.J. Sci. & Tech. 105. See also generally Usama Fayyad, Heikki Mannila and Raghu Ramakrishnan, eds., *Data Mining and Knowledge Discovery* (Norwell, MA: Kluwer Academic Publishers, 2002); Lee Tien, "Privacy, Technology and Data Mining" (2004), 30 Ohio N.U.L.

innocuous information might prove damning in combination — an effect which is illegitimate in its failure to respect the original purpose behind the collection of each piece of data. The conclusions possible through data mining might also reveal something more akin to 'content'. Similarly, the information revealed by the roadmap of traffic data could itself be considered content. Queries to an Internet search engine are a good example.[63] It might also be said that the size of an e-mail and the names and extensions of attachments, especially when combined with other data, provide information that is just as revealing as content data.

These examples serve to blur the illusory bright-lines presupposed by the three levels of investigatory information laid out in the *Convention*. Although subscriber data may appear less revealing, and is therefore deemed less worthy of strong privacy protections, in combination it can be just as, or even *more* revealing than content or traffic data. Bill C-74's creation of expedited, warrantless procedures for accessing subscriber information is based on the *mistaken* assumption that subscriber

---

Rev. 389; and Tal Z. Zarsky, "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society" (2004), 56 Me. L. Rev. 13.

63. While some might describe search terms as steps towards accessing Internet content, it is worth noting that these queries could well be indicative of the content of a user's time surfing on the Internet, similar to the content of an e-mail. In 2005, a new feature was launched by Google, the Internet's most popular search engine, which allows users to see all of their past searches. The engine is also able to personalize and monitor previous searches to refine future results. See: Elinor Mills, "Google automates personalized search" *ZDNet News* (June 28, 2005), online at <http://news.zdnet.com/2100-9588_22-5766899.html>. According to Chris Hoofnagle of the Electronic Privacy Information Center, by integrating more and more diverse online services, Google is "becoming one of the largest privacy risks on the Internet." For instance, Google offers massive free storage for e-mail messages (Gmail) and has acknowledged plans to scan messages being sent and stored in order to deliver relevant text advertising alongside them. The existence of such huge databases "under a single digital roof" – makes e-businesses, such as Google, "a prime target for abuse by overzealous law enforcers and criminals alike." See: "Quality overriding privacy?", *Sauk Valley Newspapers*, online at <http://www.saukvalley.com/news/283881388111387.bsp> (accessed December 1, 2004).

data is somehow a lesser form of investigatory information, and C-74's procedures threaten individual privacy in a serious way. By erecting false distinctions between different kinds of data, and treating these categories of information differently, the government is in fact seeking enhanced search powers through expedited processes and lower standards, thereby slashing privacy safeguards and expectations.

(5) Interception Capabilities

The *Convention* requires TSPs to build and maintain an infrastructure specifically designed to assist law enforcement, in the form of a global intercept capability. It also provides that state parties should compel TSPs to collect and record traffic and content data in real-time.[64] In addition, TSPs would also be obliged to keep confidential both the fact of, and any information about, the collection.[65] Accordingly, the Canadian government had proposed, in Bill C-74, that all telecommunications service providers be required to integrate intercept capabilities into their networks.[66] TSPs would also be subject to several other obligations, for example a requirement to remove any compression, encryption or other treatment of intercepted information that the TSP applies.[67] Only small TSPs (*e.g.* TSPs who provide telecom services ancillary to their core functions as educational institutions or hotels) and TSPs who do not provide telecom services to the public would be partially exempt from these requirements.[68] As at least one commentator has observed, the benefits of this regulation in terms of effective law enforcement are questionable given that "criminals will logically migrate to small TSPs exempt from the requirements."[69] Before "downloading" responsibility

64. *Supra*, footnote 6, arts. 20 and 21.
65. *Ibid*., art. 20, s.3 and art. 21, s.3.
66. More precisely, TSPs would be required to maintain existing intercept capabilities, and to build in intercept capability as they make upgrades to their networks. See *supra*, footnote 7, s.7.
67. *Supra*, footnote 7, s.7.
68. The types of TSPs that are completely or partially exempt from the proposed Act are set out in Bill C-74, *supra*, footnote 7, Sch.1 and II.
69. Canadian Internet Policy and Public Interest Clinic, "Canadian government proposals for updating criminal laws and facilitating law enforcement in the electronic age", online at <http://www.cippic.ca/en/projects-cases/lawful-access/>.

for law enforcement onto private actors, the government should therefore provide clear and compelling evidence that the benefits of such a reconstruction are worth the cost – in terms of both dollars and, more importantly, constitutionally protected values. Yet several commentators have argued that Canada's government "has not produced any evidence that existing rules under the Criminal Code are inadequate for fighting cybercrime."[70]

(6) Interpretation and Implementation of the Convention

Signatory states are left with considerable discretion in implementing the *Convention.* It is not unusual for international treaties to be vague in application, given the array of legal systems that must adopt its provisions. It would have been helpful, however, if the *Convention* had outlined in greater detail the nature of the interests affected by the contemplated measures. While privacy is specifically contemplated in the introductory preamble to the *Convention* as an interest to be balanced,[71] it is not referenced in the text of the Articles. How should signatories factor privacy or other human rights concerns into the standard for the various orders envisioned? Can or should a State assume that the *Convention*'s failure to emphasize privacy

---

70. Canadian Civil Liberties Association, "Cyber Snooping", online at <http://www.ccla.org/privacy/cybersnoop.html> (citing the former Federal Privacy Commissioner George Radwanski). Even with the release of Bill C-74, no new arguments have been made to justify the need for new cybercrime legislation. See Michael Geist's comments online at <http://www.michaelgeist.ca/index.php?option=com_content&task=view&id=1009&Itemid=85>. This chapter does not attempt to address all of the major issues arising from the *Convention* and proposed lawful access legislation. Additional topics that need to be considered in the lawful access debate include: preservation and production orders, tracking and ancillary warrants, new and revised offences, etc.

71. The Preamble to the *Convention* refers to both "privacy" and "personal data":

> Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, (…) which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy; Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data…

Supra, footnote 6, at paras. 10-11.

rights is indicative of lowered value, when balanced against the international threat of cybercrime?

There are good reasons to favour a restricted application of the *Convention*'s measures, in keeping with an overarching framework that values privacy as a fundamental human right. In our view, the *Convention*'s terms must be implemented cautiously. Law enforcement should be made to justify requests for access to information at a high standard before judicial authorization is granted.[72] These orders should not be available for anticipated crimes, for example, but only when authorities believe that an offence has been committed. Law enforcement should be made to demonstrate that there are reasonable grounds for requesting data, and the scope of authorization should be construed as narrowly as possible, on a standard of necessity, not relevance to the investigation. In keeping with our observation that advances in data-mining techniques present significant danger in creating different standards of protection for different categories of investigatory information, we suggest that the justificatory standard for all categories of investigatory information should be treated the same. Our concern is that the proposal to create newly expedited means of obtaining subscriber information will almost certainly lower the threshold of protection to individuals since the so-called lower forms of investigatory information can easily be combined with other known information to build a data profile on an individual capable of revealing as much about that person as

72. Arguably, such standards should be established with due consideration given to requirements concerning other types of investigatory information, which currently exist in Canadian criminal law. For instance, Section 487.05 (1) of the Criminal Code sets out the threshold of "reasonable grounds to believe" in relation to information for warrant to take bodily substances for forensic DNA analysis. In that case, a judge must be satisfied by information on oath that there are reasonable grounds to believe: (a) that a designated offence has been committed, (b) that a bodily substance has been found or obtained (i) at the place where the offence was committed, (ii) on or within the body of the victim of the offence, (iii) on anything worn or carried by the victim at the time when the offence was committed, or (iv) on or within the body of any person or thing or at any place associated with the commission of the offence, (c) that a person was a party to the offence, and (d) that forensic DNA analysis of a bodily substance from the person will provide evidence about whether the bodily substance referred to in paragraph (b) was from that person.

would the more highly protected information that would require a search warrant.

5. Constitutionality

One possible barrier to the enactment of legislation implementing the *Convention on Cybercrime* in Canada is the *Canadian Charter of Rights and Freedoms.*[73] Concerns over the lack of conformity of the *Convention*'s "lawful access" regime with fundamental human rights have been raised not only in Canada, but also in several other jurisdictions.[74] In Canada, the Charter sets out the right to be free from unreasonable search and seizure in section 8.[75] The Supreme Court of Canada has equated this prohibition with the existence of a reasonable expectation of privacy.[76] Bill C-74 could be constitutionally challenged on the

---

73. Charter, *supra*, footnote 11.

74. For example, the international signatories of an open letter to Council of Europe Secretary General Walter Schwimmer and Council of Europe Committee of Experts on cybercrime have contended that Articles 14 and 15 of the *Convention* are incompatible with Article 6 of the *European Convention on Human Rights*. Likewise, in light of the jurisprudence of the European Court of Human Rights, Article 18 is inconsistent with Article 8 of the *European Convention on Human Rights.* See: "Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime" (October 18, 2000), online at <http://www.gilc.org/privacy/coe-letter-1000.html>.

75. The wording of section 8 of the *Charter* is: "[e]veryone has the right to be secure against unreasonable search and seizure". Section 7 of the *Charter*, stating that "[e]veryone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice," is also relevant to this discussion in that its right to liberty has been interpreted to include: "a narrow sphere of personal autonomy wherein individuals may make inherently private choices free from state interference" (*Godbout v. Longueuil (City)* [1997] 3 S.C.R. 844, 152 D.L.R. (4th) 577, 97 C.L.L.C. ¶210-031). Although new cybercrime laws could be challenged as violating security of the person under s. 7, it is more likely that a challenge based on s. 8, which is more directly applicable to informational privacy, would be tried.

76. In *Hunter v. Southam Inc*., Dickson J. equates protection from unreasonable search and seizure with a reasonable expectation of privacy (*Hunter v. Southam Inc*., [1984] 2. S.C.R. 145 at pp. 159-60, 14 C.C.C. (3d) 97, 41 C.R. (3d) 97 *sub nom. Dir. Of Inv. & Research, Combines Inv. Branch v. Southam Inc.*). In *R. v. Edwards*, Cory J. sets out that a reasonable expectation of privacy includes both "the existence of a subjective expectation of privacy" and "the objective reasonableness of the expectation" (*R. v. Edwards*, [1996] 1 S.C.R. 128 at para. 45, 104 C.C.C. (3d) 136, 45 C.R. (4th) 307).

grounds that the law authorises unreasonable searches and seizures of personal information. Although the Charter does not apply to private parties such as TSPs, the legislation would formalise their role as agents of the state[77] by requiring TSPs to conduct searches at the behest of law enforcement. TSPs' actions would therefore be subject to Charter scrutiny. Bill C-74 would require TSPs, as agents of the state, to conduct unconstitutional searches using expedited access and global intercept capabilities which infringe the s. 8 Charter right to a reasonable expectation of privacy.

Courts are wary of striking down laws passed by democratically elected governments on constitutional grounds, and even if a court determines that the legislation violates section 8, that is not the end of the matter: a section 1 analysis would follow, whereby the government would attempt to persuade the court that the breach of Charter rights is justified in a free and democratic society. Only if the breach is *not* justified in a free and democratic society will the law be declared unconstitutional. Although a full analysis of the likelihood of Bill C-74 surviving a Charter challenge is beyond our scope here,

---

Because of the relative nature of a reasonable expectation of privacy, it should be noted that the proposed cybercrime legislation, which would lower the current standard of privacy protection, will almost certainly have the effect of lowering the *expectation* of privacy that one can reasonably have in one's personal information. That is, the less privacy protection one has in a particular context, the less one is entitled to expect privacy in the same context.

The reasonable expectation of privacy test appears to be a universal means (existing in many civil-law and common-law jurisdictions), of delimiting private and public spheres of life. For example, as observed by Gomez-Arostegui, while Canada has adopted the reasonable expectation approach to interpreting section 8 of the *Charter*, the Constitutional Court of South Africa has used the test to interpret the right to privacy contained in section 14 of its Constitution. In addition, a court in Australia has used the concept of reasonable expectation to analyze the legality of drug testing police officers, and Israeli legislation has used the test to evaluate the secret monitoring of conversations. See: H. Tomas Gomez-Arostegui, "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations" (2005) 35 Cal. W. Int'l L.J. 153 at 164. For a comprehensive analysis of the reasonable expectation test in the United States, and particularly the role of the *Katz* decision, which has influenced many courts outside the United States, see: Susan Freiwald, "Online Surveillance: Remembering the Lessons of the Wiretap Act" (2004) 56 Ala. L. Rev. 9 at p. 38.

77. See discussion of *Weir*, *supra*, footnote 9, at para. 6.

especially given the uncertainty of the final form of the proposed legislation, it is useful to highlight in a preliminary manner some of the key issues that could arise in determining its constitutionality under s. 1 of the Charter.

Section 1 of the Charter states, "[t]he *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." The s. 1 test is well established in Canadian law and was set out in the case of *R. v. Oakes*.[78] It consists of two parts: the first asks whether the legislation infringes a Charter right. If it does not, the legislation will be deemed "constitutional." If it does infringe a Charter right, the second stage of the *Oakes* test comes into play. Here the court must determine whether the infringement meets the s. 1 requirement that the Charter-infringing legislation be "demonstrably justified in a free and democratic society." To determine whether a violation is "demonstrably justified," the court uses five criteria: (i) whether the law has a pressing and substantial objective; (ii) whether the means are proportional to the objective of the law; (iii) whether the law has a rational connection to the stated objective; (iv) whether the legislation violates the Charter as minimally as possible; and (v) whether there is proportionality between the aims of the legislation and its Charter-infringing effect. If all five are answered affirmatively, the law will be considered justified in a free and democratic society and will stand. If any of the five criteria is answered in the negative, the law will not be considered justified and will be declared unconstitutional.

There are two additional considerations that are important in carrying out a s. 1 analysis. The first recognizes an ongoing tension in the Supreme Court about whether the *Oakes* test becomes more or less stringent depending on the context of the challenged legislation. This contextual approach, originated in *Edmonton Journal v. Alberta (Attorney-General)*,[79] "requires that the courts assess the value or significance of the right and its restriction in

78. [1986] 1 S.C.R. 103, 24 C.C.C. (3d) 321, 50 C.R. (3d) 1.
79. [1989] 2 S.C.R. 1326, 64 D.L.R. (4th) 577, [1990] 1 W.W.R. 577.

their context rather than in the abstract."[80] In other words, the contextual approach "recognizes that a particular right or freedom may have a different value depending on the context."[81] The contextual approach is relevant to a second tension within the Court – the issue of when it is appropriate to "defer to the legislature's judgment about the need for, and effectiveness of, a particular limit on a *Charter right.*"[82] The Court has held that deference is more appropriate in some contexts than others, stating "the role of the legislature demands deference from the courts to those types of policy decisions that the legislature is best placed to make."[83] There remains ongoing and significant disagreement as to in exactly what circumstances deference is an appropriate option. For instance, the Court has held that "governments must be afforded wide latitude to determine the proper distribution of resources in society"[84] and that "greater deference to Parliament…may be appropriate if the law is concerned with the competing rights between different sectors of society than if it is a contest between the individual and the state"[85] Such distinctions are rarely easy to apply, and the Court appears to undertake deference on a contextual, case-by-case basis.

Having set the stage, it is possible to hypothesize about how the Court might situate Bill C-74 in the course of a s. 1 challenge. The Government would be likely to make the argument that the legislation is predominately in the interest of national security and, as a result, deference should be granted to the decisions of Parliament, as it is the body best equipped to assess and evaluate the needs of law enforcement and security. While such a claim is certainly not without some merit, it is overblown. A challenger is likely to mount a persuasive counter-claim that the impetus of Bill C-74 is *not* primarily as a national security instrument, pointing to

---

80. The Constitutional Law Group, *Canadian Constitutional Law*, 3rd ed. (Toronto: Emond Montgomery Publications Ltd., 2003), p. 763.
81. *Edmonton Journal*, *supra*, footnote 79, at para. 51.
82. *Supra*, footnote 80, at p. 764.
83. *M. v. H.*, [1999] 2 S.C.R. 3 at p. 78, 171 D.L.R. (4th) 577, 121 O.A.C. 1.
84. *Eldridge v. British Columbia (Attorney-General)*, [1997] 3 S.C.R. 624 at para. 85, 151 D.L.R. (4th) 577, [1998] 1 W.W.R. 50.
85. *RJR Macdonald Inc. v. Canada (Attorney-General)*, [1995] 3 S.C.R. 199 at para. 124, 100 C.C.C. (3d) 449, 62 C.P.R. (3d) 417.

the substantive criminal law provisions specified in the *Convention*, which were developed and published prior to the events of 11 September 2001: (i) computer-hacking crimes such as "illegal access," "illegal interception," "data/system interference," "misuse of devices"; (ii) computer-related forgery; (iii) computer-related fraud; (iv) child pornography; (v) copyright infringement; etc.[86] Likewise, Canada's "Lawful Access Consultation Document"[87] includes a veritable "laundry list" of crimes that Bill C-74 is meant to address, including: "money laundering," "price fixing," and "deceptive telemarketing." That the Government requires broad intercept and access powers to combat cybercrime was never contemplated solely as a national security issue, thus the context of this legislation is not one in which the government should be owed a particular deference. This conclusion is further supported by the fact that the legislation pits the privacy interests of individual citizens against the intercept and access interests of the government, a situation where the Court has already established the precedent that deference is less appropriate.[88] Consequently, a stringent s. 1 analysis is warranted.

Even the most stringent s. 1 analysis is sure to commence with a finding that the objective of Bill C-74 is both pressing and substantial. Its stated purpose of enabling law enforcement agencies some ability to intercept communications[89] is already a well established practice in the context of wire-line telecommunications, and there is no good reason to think that these law enforcement practices are wholly inapplicable to the internet or other wireless communications networks. The goal of furthering law enforcement and national security in the online setting, particularly in the post-9/11 world, will without question be accepted as pressing and substantial, thus passing the first prong of the *Oakes* test.

Admittedly, the outcome in the remainder of the *Oakes* analysis is less certain. However, it is our view that the measures taken to meet the pressing and substantial goals set out in Bill C-74 would fail at a number of points in the proportionality test. In

86. *Supra*, footnote 6.
87. *Supra*, footnote 43.
88. *RJR Macdonald Inc. v. Canada (Attorney-General)*, *supra*, footnote 85.
89. *Supra*, footnote 7, s.3.

particular, we draw attention to two critical prongs of the test that find conflict with the cybercrime legislation: the minimal impairment requirement and the requirement of proportionality between the legislation's aims and its Charter-infringing effects.

(1) Proportionality: Means and Objective

The ability to commit crimes online clearly creates new challenges for conventional investigative techniques, many of which are woefully inadequate in the online context. In attempting to justify Bill C-74 under section 1, the Government has claimed that the global nature of cyberspace, the ability of users to interact with relative anonymity, and the potential to cause tremendous harm at a distance necessitate broader and more expeditious investigatory powers if the Government is to meet the legislative objective of effectively fighting cybercrime.

While this may be true to an extent, the appropriate constitutional question is whether the breadth of expansion in investigatory powers, the reduction of procedural safeguards, and the drastic expedited means by which law enforcement agencies may obtain personal information about citizens without pre-authorization or oversight, as set out in Bill C-74, is proportional to the objectives it seeks to fulfill. In the five years since Canada signed the *Convention*, Canadian law enforcement has demonstrated an ability to investigate and prosecute cybercrime and has even garnered international success in online investigations,[90] and has done so without the expedited access and mandatory intercept capabilities provided for in Bill C-74. While there may be good reason to update current laws to address the challenges of law enforcement online, the requirement of mandatory interception capabilities and an automated, unsupervised process for mining subscriber information is an excessive and over-inclusive response. While these two procedural shifts may make it easier and more convenient for law enforcement officials to undertake

90. See for example: "Toronto police find hotel where child-porn pictures taken" *CBC News* (February 4, 2005), online at CBC Online <http://www.cbc.ca>; "Toronto Police use internet to save sexually exploited girls" *CBC News* (March 26, 2004), online at CBC Online <http://www.cbc.ca>; "Web expands to fight online sex crimes" *Edmonton Journal* (June 5, 2005) p. A6; "Online trail can lead to Court", *The New York Times* (February 4, 2006), p. 1.

cybercrime investigations, ease and convenience are not sufficient justifications for violating the privacy rights of Canadian citizens.

(2) Rational Connection

Under the rational connection component of *Oakes*, the Government is likely to argue that the objectives of the legislation as set out above are rationally connected to mandating TSPs to integrate intercept capabilities into their frameworks and to expediting access to subscriber information in order to allow law enforcement officials to access all and any personal information they may require to carry out investigations quickly and efficiently. There is an obvious connection between surveillance and the ends that the cybercrime legislation aims to achieve. Bill C-74 calls for largely unrestricted access to subscriber information for law enforcement personnel, and although the breadth of the legislation is problematic from a proportionality perspective, it is rationally connected to the goal of reducing the problem of international cybercrime.

That said, there is a persuasive argument that the exceptions built into the legislation, exempting small TSPs[91] from the need to build an intercept capability, is not rationally connected to the objective of the legislation because it would allow criminals to migrate to those networks and thereby evade law enforcement altogether. These smaller TSPs could become cybercrime havens and could in fact be built as such.

---

91. Bill C-74, *supra*, footnote 7, Sch.I. and Sch. II. Schedule I to Bill C-74, entitled "Exclusions from the Application of the Act," specifies in Part I that "[a] telecommunications service intended principally for the use of its provider and the provider's household or employees and not by the public," is exempt from the legislation, as are, in Part 2, "[t]elecommunications service providers whose principal function is operating a registered charity…or operating an educations institution, or operating a hospital, a place of worship, a retirement home or a telecommunications research network…" Similarly, Schedule II, "Partial Application of the Act," sets out in Part 2 that Bill C-74 applies only in part to

> Telecommunications service providers whose principal business or function is operating a post-secondary educational institution, a library, a community centre, a restaurant or an establishment that provides lodgings or residential accommodations, such as a hotel, an apartment building or a condominium, only in respect of telecommunications services that they provide ancillary to their principal business or function.

(3) Minimal Impairment

Canada's implementation of the *Convention* will require most TSPs to incorporate mandatory intercept capabilities into their architectures for the specific purpose of assisting law enforcement. This obligation would mean that communications networks will have a built-in "back door," always completely open and accessible by TSPs and, when warranted, by a significant proportion of the law enforcement community. The looming possibility of an open back door makes for an insecure home. It also creates what social theorists refer to as a virtual *Panopticon.* This notion stems from the Greek neologism signifying an 'all-seeing place'. Panopticism is premised on vision and transparency, but vision and transparency operating only in one direction – i.e., in the service of power. Since the time that Bentham first proposed it,[92] the essence of Panoptic power is that it is highly visible and yet completely unverifiable. In Bentham's original architecture, the prison inmate could not see the inspector, only the looming tower; a prisoner never knew for sure whether he or she was actually under surveillance. This uncertainty, along with the inmates' loss of privacy was Bentham's means of achieving compliance and subordination. Uncertainty, he recognized, becomes the principle of the prisoner's own subjection. It assures, as Foucault would later put it, that "surveillance is permanent in its effects, even if discontinuous in its action."[93]

Requiring TSPs to build global intercept capabilities creates a Panoptic effect.[94] As the Supreme Court has articulated in the context of ubiquitous audio/video surveillance, being forced to live with the *continuous possibility* that any communication could be intercepted is antithetical to a free and democratic society:[95]

> While there are societies in which persons have learned, to their cost, to expect that a microphone may be hidden in every wall, it is the hallmark of a

92. Bentham first laid down his plans for a Panoptic prison in a series of letters written in 1787. See: Jeremy Bentham, "Panopticon" in Miran Bozovic, ed., *The Panopticon Writings* (London, Verso: 1995), p. 29.
93. Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. by Alan Sheridan (New York:Vintage, 1977), p. 201.
94. James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors" (1997), 66 U Cin. L.R. 177.
95. *R. v. Wong*, [1990] 3 S.C.R. 36 at para. 13, 60 C.C.C. (3d) 460, 1 C.R. (4th) 1.

> society such as ours that its members hold to the belief that they are free to go about their daily business without running the risk that their words will be recorded at the sole discretion of agents of the state.

Speaking in the context of video surveillance, the Court went on to say that, "the notion that the agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconcilable with what we perceive to be acceptable behaviour on the part of government."[96] The court also recognized that such concerns apply to "all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future."[97]

The Panoptic effect of a mandatory global intercept capability in all telecommunications media, by definition, creates the possibility of continuous surreptitious surveillance of the many different communications devices which we use with increasing regularity within our homes. As the Supreme Court of Canada has more recently stated, "the spectre of the state placing our homes under technological surveillance raises extremely serious concerns."[98] Therefore, mandatory intercept capability *is not* a minimal impairment of the privacy rights of citizens and Bill C-74 would therefore fail this prong of the *Oakes* test.

A second consideration under the minimal impairment portion of a s. 1 analysis is the expedited process by which law enforcement officials can access subscriber information under Bill C-74.[99] As described earlier, without any need for judicial preauthorization, the expedited procedures for accessing personal information invite law enforcement officials to an all-you-can-eat investigatory smorgasbord with absolutely no say on the part of citizens who are concerned about the collection, use, or disclosure of their personal information. In fact, under the proposed expedited process, TSPs are not obliged, and in some cases may

---

96. *Ibid.*, at para.15.
97. *Ibid.*, at para. 8. This statement from *Wong* reiterates a similar claim in *R. v. Duarte*, [1990] 1 S.C.R. 30, 53 C.C.C. (3d) 1, 74 C.R. (3d) 281 *sub nom. R. v. Sanelli.*
98. *R. v. Tessling*, [2004] 3 S.C.R. 432 at para. 55, 189 C.C.C. (3d) 129, 23 C.R. (6th) 207.
99. See *supra*, footnote 56.

even be *required not to disclose* to their subscribers that their personal information has been sought by designated law enforcement official.[100] Bill C-74 provides only minimal restrictions on who can access subscriber information and under what circumstances,[101] and offers no real oversight mechanism to safeguard the process. The excessive range of personal information that becomes available in conjunction with the lack of accountability measures in place to monitor expedited access in Bill C-74 *does not* impair Charter rights as minimally as possible.

If the proposed cybercrime legislation were an attempt to truly impair privacy rights as minimally as possible, the legislation would have incorporated privacy-protective measures, oversight mechanisms and additional democratic safeguards. The Government may have legitimate concerns that such counter-measures and safeguards are onerous and could in some instances jeopardize efficacious law enforcement in a world where time is of the essence. Taking the time to jump through "accountability hoops" will in some instances limit the ability of law enforcement officers to effectively execute online investigations.[102] However, the solution to this problem is not to drastically diminish accountability measures at the expense of Charter values like privacy and personal autonomy. The Government could have crafted time-sensitive procedures could while still leaving room for proper and adequate institutional oversight and other democratic safeguards. By not introducing a sufficient degree of accountability into the process for expedited

100. If, in his or her written request to a TSP for subscriber information, a designated law enforcement officer stipulates that the request not be disclosed to the subscriber whose information is being obtained, the TSP will be obliged to comply.

101. See section 4(3) above, "Obligations Concerning Subscriber Data" at 16.

102. Speed is a critical consideration in accessing information relevant to cybercrime. Section 18 of Bill C-74 specifies that a law enforcement official may make a request other than those in writing for subscriber information from a TSP, as opposed to a written request as indicated in s. 17 in "exceptional circumstances, " which include, "the officer believes on reasonable grounds that the urgency of the situation is such that the request cannot, with reasonable diligence, be made under subsection 17(1)," and "the officer believes on reasonable grounds that the information requested is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property." See *supra*, footnote 7, s.18.

access to subscriber information, the legislation once again fails to meet the Charter's minimal impairment requirement.

(4) Proportionality: Deleterious Effects

A further consequence of the insufficient privacy safeguards in Bill C-74 relates to the final prong of the *Oakes* analysis, which asks whether there is proportionality between the aims of the legislation and its *Charter* infringing effect. Without sufficient safeguards in the legislation, it is impossible to ensure that subscriber information will not be used by law enforcement for fishing expeditions or other purposes unrelated to cybercrime activity.[103] The work of Professor Sweeney and others, cited above,[104] illustrates that basic subscriber information, once obtained, can easily be combined with other publicly available information through automated software programs in a way that is deeply revealing.[105] This makes it possible for those who obtain basic subscriber information to translate that into more personal levels of information, including traffic and content data.

As the Ontario Court of Justice has recently stated, "Information about name and date of birth is information which can be a key in unlocking other database information about an individual of an intimately personal nature."[106] It is not difficult to imagine the serious, deleterious risks that could inevitably result if one's health, financial or other personal information was improperly collected, used or disclosed in this way. In fact, the courts have recognized this possibility and noted that it "is capable of creating substantial hardship."[107]

Consequently, the practically unfettered access to subscriber data provided for in Bill C-74 will bestow upon law enforce-

---

103. Section 19 of Bill C-74 does provide one important safeguard: "Information that is provided in response to a request made under subsection 17(1) or 18(1) shall not, without the consent of the individual to whom it relates, be used by the agency in which the designated person or police officer is employed except for the purpose for which the information was obtained or for a use consistent with that purpose." Although this provision safeguards against a shifting purpose, it can be abused simply by stating a broad purpose and does not address situations where the stated purpose has nothing to do with the objectives of the original cybercrime mandate.

104. *Supra*, footnote 61.

105. See section 4(4) above, "Privacy Implications of Increased Access to Subscriber Data".

106. *R. v.E. (M.)*, 2006 ONCJ 146 at p. 32.

107. *R. v. Bryan*, [1999] O.J. No. 5074 (QL) at para. 14.

ment officials a reservoir of personal information from which to fish. These deep basins will allow officials to cast their nets wide, enabling access to personal information that reveals core biographical data. The Supreme Court has explicitly noted the importance of protecting biographical information, stating:[108]

> [i]n fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.

While the Government is correct in maintaining that subscriber information does not *in and of itself* reveal intimate details, it has not adequately addressed the deleterious risks associated with data-mining – for example, the ability to mine intimate data through the combination and processing of less intrusive sorts of information such as the kind that would be offered up by TSPs about their subscribers. The point cannot be sufficiently underscored: *typical subscriber information of the sort made available under the proposed legislative scheme will become the means by which a biographical core of personal information is assembled.*[109] This is not a novel point. The courts have acknowledged this possibility within the s. 8 jurisprudence for more than a half decade. For example, building on Supreme Court of Canada's privacy jurisprudence, the Newfoundland Supreme Court held that:[110]

> The linkage of a name to [account] information creates at once the intimate relationship between that information and the particular individual, which is the essence of the privacy interest. I do not accept the Crown's suggestion that the mere obtaining of the name of the owner of an account about which information is already available is not deserving of protection under s. 8.

The deleterious effects of allowing core biographical information to be revealed through an easy and expeditious disclosure of subscriber information, made available to law enforcement

---

108. *R. v. Plant*, [1993] 2 S.C.R. 281 at para. 20, 84 C.C.C. (3d) 203, 24 C.R. (4th) 47.
109. Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004).
110. *R. v. Eddy*, [1994] N.J. No.142 at para. 175, 192 Nfld. & P.E.I.R. 167 (Nfld. S.C.).

merely because they request it, are potentially staggering. The ease with which expedited subscriber information could be misused will have a significant Charter-infringing effect that cannot be justified in a free and democratic society.

Together, the expedited access to subscriber information and the mandatory intercept capabilities provided for in Bill C-74 fly in the face of citizens' reasonable expectation of privacy. In the Panoptic architecture mandated by Bill C-74, people will never know who or whether someone is collecting, using, disclosing or intercepting their personal information. Such a state of informational insecurity represents a serious diminishment of individuals' privacy rights, and undermines the importance of privacy in Canadian society, consequences that are disproportionately deleterious to the aims of the legislation.

Finally, the implementation of cybercrime legislation could have a significant deleterious effect on the prosperity of Canadians in a global economy by creating an arms race that might ultimately undermine the possibility of a flourishing global e-commerce.[111] There is sure to be a backlash to a global intercept requirement in the cryptography community. While cryptographic technologies can "provide a foundation for establishing trust in electronic commerce because they safeguard information, protect communications, and authenticate parties to transactions,"[112] certain uses of cryptography can make it computationally infeasible for law enforcement to decipher or comprehend the encoded communications that they are intercepting. With various motivations (ranging from a sincere desire to protect privacy to money-making and malice) cryptographers are sure to develop techniques that undermine the Government's continued efforts to intercept communications. In addition to the huge sums of wasted money spent building an intercept capability that has a Panoptic effect on the average law-abiding citizen but is potentially useless against criminals using crypto, such a backlash may force the government to revisit its cryptography policy estab-

111. This would indeed be ironic, given that a central aim of internationally harmonized cybercrime legislation is to promote global commerce.

112. John Manley, "Canada's Cryptography Policy," Speaking Notes (October 1, 1998), online at <http://www.fas.org/irp/news/1998/10/981001-crypto.htm>.

lished in 1998,[113] which supports the freedom of Canadians to "develop, import and use whatever cryptography products they wish."[114]

Canada's cryptography policy, which made the commitment not to impose strict regulations on the use of cryptography, has played a significant role in the development of the infrastructure of global e-commerce and the delivery of government services online.[115] Such a policy, it is well known, best supports innovation and progress. A potential deleterious effect of Bill C-74, its likely backlash, and the ensuing arms race may be that the Government feels compelled to regulate cryptography and other internet infrastructures and services. In fact, the mandatory intercept capability standards that will be prescribed in the Regulations that accompany the Bill C-74 arguably already have the deleterious effect of stifling innovation and technological progress in that very manner.[116]

Taking into consideration all of the points articulated above, there is a strong case to be made that Bill C-74 will *not* satisfy the *Oakes* test and will therefore be rendered of no force or effect. The Supreme Court has affirmed that "[a] society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."[117] Similarly, a society which lays bare our personal information with insufficient democratic safeguards may be perfectly suited to fight cybercrime, but, as the Supreme Court of Canada has also noted, "has the potential, if left unregulated, to annihilate any expectation that our communications will remain private."[118]

---

113. *Ibid.*
114. *Ibid.*
115. Electronic Privacy Information Centre (EPIC), *Cryptography Policy*, online at <http://www.epic.org/crypto>.
116. See: Ian R. Kerr, *Lawful Access Consultation Document: Submission* (December 16, 2002), online at: <http://www.lexinformatica.org/cybercrime/pub/kerr_la.pdf>, and Information Technology Association of Canada, *Lawful Access: ITAC Comments on Lawful Access Consultation Document* (December 2002), online at <http://www.lexinformatica.org/cybercrime/pub/itac_la.pdf>.
117. *Duarte*, *supra*, footnote 97, at para, 22.
118. *Ibid*., at para. 22.

6. Conclusion

In this article we have said that law enforcement must maintain high standards of privacy protection in its extension of "lawful access" to Internet communications. There are two underlying rationales. First, there is significant value in preserving the integrity of Internet communications, especially as the Internet becomes increasingly prominent as a mode of communication. Individuals use e-mail, voice-over Internet protocol and other forms of online discourse to communicate with friends, transact with trading partners, and participate in democracy. Citizens should be able to expect such interactions to be secure and private. Privacy safeguards must therefore be built into cybercrime legislation out of respect for individual autonomy and in recognition of the power of technology to create relationships of dependence.

Second, it is a trite observation that once lost, privacy cannot be regained. By treating TSPs as reservoirs of personal information, we fundamentally shift the relationship between these private entities and those who use them. There is an increasing tendency to shift "much of the responsibility for controlling crime from a cadre of designated professionals to the individuals and entities who use cyberspace."[119] The new approach in Bill C-74 calls for easy and expedited access to personal data and private communications. In this chapter, we suggest that the legislation not only creates new powers for law enforcement, it also *requires* TSPs to exercise new discretion and to exercise state-like powers. This shift in the regulatory oversight from the public to the private sphere is unprecedented, complex, and is potentially mired with unforeseen consequences.

Finally, it is evident that Bill C-74, while addressing a worthy objective in its fight against cybercrime, will run into significant constitutional discord in terms of the means and methods the legislation puts forth to meet this goal. Based on our section 1 analysis, above, Bill C-74 would not survive a Charter challenge. This speaks to the value of privacy rights in Canada and

119. Susan W. Brenner, "The Privacy Privilege: Law Enforcement, Technology and the Constitution" (2002), 7 J. Tech. L. & Pol'y 123.

is indicative of the caution with which legislators must proceed in balancing those rights with the needs of law enforcement in the ever-changing technological landscape. With Bill C-74, this delicate but critical balance has simply not been struck.

Technology is Janus-faced.[120] Just as a stethoscope can be used to hear a beating heart in crisis or to crack a safe, Internet technologies can be used to breathe life into our global village, or to trample on individual rights. In our view, privacy considerations are a first-order concern that must be adequately accommodated in any proposed cybercrime legislation. Such is not the case with the recent Canadian proposal. Lesser intrusions or better justifications for increased interception capability and expedited access to investigatory information are necessary in order for an implementation of the *Convention* to satisfy constitutional scrutiny. TSPs have, until recently, helped preserve personal privacy by acting as the stewards of our personal information and private communications. With the *Convention on Cybercrime* and its implementation in Canada, TSPs will likely be required to shift allegiance to the State, assisting law enforcement by building and maintaining systems of interception and preservation that could result in damaging incursions into individual privacy. Our right to privacy is a fundamental human right, one that allows us to define our individuality free from unjustified interference by the State and its agents, and the value of which must not be trampled by new technologies or the law.

120. Janus was a Roman god who protected doors and gateways. The god is typically represented in art with two faces looking in different directions, symbolic of entrances and departures through the gateway. Janus also represented beginnings, thus the first month of our year is named "January".