Terrorism, Trade, and Internet Privacy

Martin R. Dowding
University of British Columbia

Abstract: It became evident that Canada’s ISPs could become party to the work of the Canadian security establishment when the Department of Justice released its consultation document on “lawful access” in August, 2002, proposing unprecedented intervention by the state into citizens’ privacy in order to fight terrorism. Since September 11, 2001, there has been an increase in surveillance within the structure of globalized markets and in information technology. Potentially repressive legislative responses to terrorism and other crime, such as those from the U.S. and European countries, have caused many communities to call for a heightened response to sustain the right to gather and exchange information freely. This essay addresses the potential threat to our communicative privacy posed by increased “lawful access.”

Résumé: Les fournisseurs de service internet (FSI) canadiens deviennent membres de la communauté de sécurité canadienne, selon le Ministère de la Justice dans son document sur l’« accès légal. » Nombreuses mesures ont été prises pour protéger la sécurité des données personnelles relatives aux citoyens et citoyennes canadiennes. Cependant, étant donné la diminution des droits civils depuis le 11 septembre 2001, dans des Etats se voulant pourtant démocratiques (Les Etats Unis et pays European), groupements de communautés croient qu’il est nécessaire de faire preuve d’une vigilance accrue quant au droit de rassembler et échanger l’information librement. Cette rédaction adresse la loi proposée que constitue une menace pour la souveraineté et les libertés individuelles.

Keywords: Privacy; Internet; Legislation; Terrorism; Rights and Freedoms

Could Internet Service Providers (ISPs) in Canada become part of the national security apparatus? That possibility became evident in August 2002, when the Canadian Department of Justice (DOJ) released its Lawful Access—Consultation Document, a response to international efforts such as the Council of Europe’s Convention on Cybercrime (2001) and the USA Patriot Act (2001), developed to stem terrorism and other crime. The consequence has been an emerging discourse of concern, articulated largely in the medium most likely to be affected by such legislation—the Internet.

Martin R. Dowding is Assistant Professor, School of Library, Archival, and Information Studies, University of British Columbia, Vancouver, BC V6T 1Z3. He specializes in Information Policy issues. E-mail: dowdingm@interchange.ubc.ca.
“Lawful access” is a long-standing and widely accepted concept that allows law-enforcement authorities to conduct a variety of surveillance activities, including wire-tapping, the opening of mail, and gaining photographic evidence covertly. At the same time, “lawful access” also deprives citizens of the right “to be let alone,” the often-quoted fundamental definition of privacy first used by U.S. Justice Louis Brandeis and others in the late nineteenth century (Goode, 1983, p. 6).

The Canadian Lawful Access proposal, like the U.S. and European models, would require ISPs to harvest and retain client information. It would also require them to submit this information to the state, at great cost to the ISPs, and deny them the right to let anyone know that they have been subject to search and seizure of the information held by their ISP. Given the history of privacy legislation and other privacy guarantees in Canada, it is not clear that such legislation in Canada is necessary, just, or even wise, given the social and potential economic cost.

When does the adoption of a new information technology warrant expanded state surveillance power? According to Stephen Goode (1983), increased surveillance has always followed new information technology in the U.S., from intercepting telegraph messages during the Civil War to wire-tapping telephones, which has been sanctioned by the Supreme Court from the 1920s until today. In Canada historic precedents that have challenged the right “to be let alone” include, for example, the treatment of Japanese-Canadians during World War II, surveillance in the 1970s by the RCMP during the FLQ separatist crisis, and more recently, Canadian citizen Maher Arar’s case, in which the Canadian Security Intelligence Service (CSIS) may or may not have been responsible for passing on information that led to Arar’s arrest and deportation to Syria on suspicion of being a terrorist.

Will justice be done with current legislation?
Since the 1980s measures have been taken to protect the privacy and security of Canadian citizens’ information, including guarantees in legislation such as the Privacy Act (first enacted in 1983); the Canadian Charter of Rights and Freedoms (1982); Part VI of the Criminal Code, which restricts state intrusion to “reasonable search and seizure;” and more recently, the Personal Information Protection and Electronic Documents Act (2000). However, given the conditions of heightened surveillance since September 11, 2001 (Shields, 2002), NGOs, communities of citizens, and individuals have called for correspondingly heightened defence of the right to gather, exchange, and control personal (and otherwise sensitive) information without fear of state intervention, as is evident in the concerns expressed by groups such as the American Civil Liberties Union, American Library Association (2004), Canadian Civil Liberties Association, Canadian Library Association, Electronic Frontier Foundation, and National Coalition Against Censorship.

The provisions that call for diminished privacy rights in the Convention on Cybercrime and the USA Patriot Act, as well as similar ones in the Canadian Lawful Access proposal, come into conflict with some of the guarantees of security and privacy embedded in the matrix of Canadian legislation, regulations, and
standards referred to above. In Canada, as in many other countries, laws and regulations exist that either allude generally to the security of the individual or address specific conditions of privacy in particular contexts. For example, Canada’s *Charter of Rights and Freedoms* does not guarantee privacy per se, but Section 8 of the Charter guarantees the right to be protected from “unreasonable search and seizure”—although “unreasonable” has had a variety of interpretations in the courts. In the event that the proposed Canadian equivalent of the Convention and the Patriot Act is invoked, could we be certain of “reasonable search and seizure”?

**Origins of privacy protection**

While privacy legislation had been developed in Canada in 1983, in 1984, the Organization for Economic Cooperation and Development (OECD), the international social-policy and economic-analysis group to which Canada and more than 30 other countries belong, developed its own “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” That document was signed by Canada at the time it was developed. To one degree or another, the OECD guidelines have subsequently been adopted by most of the provinces in Canada in their provincial freedom-of-information and privacy legislation. The OECD guidelines also formed the foundation for a privacy protocol developed by the Canadian Standards Association (CSA) in the early 1990s, designed very much in response to the questions cited above, that addresses concerns about the reasons for collecting information, the duration of information retention, the ability for a person to know what is being done with his or her information, and whether their information can be corrected or controlled.

Because it is considered more complete than the OECD guidelines, the CSA standard was adopted by Canada as a national standards code in 1996 and was officially appended to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in recognition of the influence of the CSA standard on the legislation. Canada was the first country in the world to adopt such a well-defined code. The CSA standard has 10 information principles that address issues primarily appropriate to the relationship between commerce and personal information (Canadian Standards Association, 2004). The standards strive to ensure compatibility with other national and international commercial and security regimes. The CSA principles are clear and speak directly to the questions that arise from the Council of Europe’s Convention and Canada’s Lawful Access proposal about how carefully and fairly information is used once it is collected.

Despite the principles of balance and fairness, however, the CSA standards state that a person’s knowledge of and consent to having their personal information collected may be “deemed inappropriate—by Law Enforcement agencies, for example” (CSA, 2004, Standard 3), which defers to (or anticipates) the perceived need for more expansive principles of security and surveillance being afforded law enforcement today in the *Convention on Cybercrime*, the *USA Patriot Act*, and the Canadian *Lawful Access* proposal. That is to say, the new anti-terrorism sur-
veillance laws may outweigh all the other rights in the CSA standards and previously established Canadian privacy legislation.

Although the concept of “lawful access” legislation is not new, this most recent manifestation grows, in part, out of the effects of economic and cultural-colonial globalization, which in themselves are long standing (McPhail, 1981; Porter, 2004). “Lawful access” also derives from a long-standing backdrop of international economic treaties that lock Canada (and other countries related by trade) into data-flow protection (compatible encryption technologies, for example) for the sake of economic purposes and security measures (OECD, 1981; Reidenberg, 1995). Such agreements are now seen to be part of a mandatory international economic-corporate regime designed to defend many contested agreements, such as NAFTA, WTO, and GATS. Since September 11, 2001, a new kind of communicative convergence has developed: new technologies, a combination of counterterrorism measures (e.g., heightened surveillance, war, diminished privacy), and promises, which may or may not be destined to fail, that trade and economic prosperity will “engender peace, prosperity and good governance” (Moore & Schrank, 2003, p. 112).

A new communication agenda
It is clear to privacy specialists such as Cavoukian and Hamilton (2002) and Radwanski (2003) that the post-September 11 security-driven communications agenda has exacerbated a jurisdictional gap between individual privacy, intellectual freedom, and political autonomy in sovereign states. The effects of the new agenda also include responses from many academics, non-governmental organization (NGO) groups, and individuals in Canada who were asked to respond to the Lawful Access proposal by Canadian Department of Justice. Many groups have voiced their views in the U.S. as well, in response to the Patriot Act, such as the Association of American Universities, American Libraries Association, American Civil Liberties Association, Massachusetts Institute of Technology, and National Coalition Against Censorship.

Despite those objections, countries anxious about their international trade obligations have argued that it is necessary to also adopt a common security agenda—for the sake of business. Writing prior to September 11, 2001, Dan Schiller (2000) pointed out that the recent worldwide communication model had been primarily about the economy, consistent with a 50-year history of cross-border market-based information flow. Canada’s role in developing electronic information and communication networks and in joining other countries in treaties such as NAFTA, WTO, and GATS has supposedly been to encourage greater economic and social opportunity. And while the “information economy” (and to a lesser extent, the “information society”) has been dominant in Industry Canada reports (1995, 1997), a culture (or cult?) of information security may be overtaking the once-democratic “information highway” model that was proposed prior to September 11.
European standards: Others follow?
The Council of Europe’s *Convention on Cybercrime* was already being prepared prior to September 11, 2001. The preamble of the *Convention* makes it clear how mindful the authors are of the “balance between the interests of law enforcement and respect for fundamental rights and freedoms as enshrined” (2001, p. 2) in a variety of preceding conventions and treaties to which the Council of Europe, the UN, the G-8, the OECD (all of which include Canada), and others are signatories.

The *Convention’s* Article 1 defines a variety of straightforward technical terms, including “computer system,” “computer data,” and “traffic data.” But it also refers to “service provider,” a particularly problematic term in the Canadian document, as I will point out. While many of the *Convention’s* articles speak to historic and well-established legal issues, such as copyright, forgery, child pornography, illegal interception of messages, fraud, and corporate liability, the powers and procedures designed to undermine privacy assumed in the *Convention* are worrisome.

According to the *Convention*, when suspicion of crime, especially related to terrorism, justifies state intervention of communication, privacy guarantees may be suspended. Nowhere, however, is the threshold of suspicion defined. Requests for *Convention* signatories (one of which is Canada) to undertake costly “expedited preservation of stored data” (Council of Europe, 2001, Article 16, p. 10), to compel the production of data on demand (Article 18), to undertake “search and seizure of stored computer data” (Article 19, p. 11), and to carry out “real-time collection of traffic data” (Article 20, p. 12) might be considered reasonable, provided they are used to reduce the justifiably suspected criminal activity to which I have just alluded, and provided that authorized, competent authorities conduct the searches. However, *Convention* Article 21(b) puts the obligation of surveillance into the hands of public and private Internet service providers. To use the *Convention’s* term: ISPs can be “compelled” by the state

i. to collect or record [communication] through the application of technical means…

ii. or to co-operate and assist the competent authorities in the collection or recording of, content, data, in real-time, of specified communications in its territory transmitted by means of a computer. (p. 12)

But who the service providers actually are and what their ultimate responsibilities are appear to be open to interpretation. The *Convention* is particularly vague on this, as is evident in Chapter 1, Article 1(c), “Definitions:”

Service provider means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service. (p. 4)

The Canadian *Lawful Access—Consultation Document*, likewise, provides a vague, broad-ranging working definition when it says: “‘Service Provider’ means a person who owns or operates a transmission facility that is used by that person or
another person to provide telecommunications services to the public in Canada” (Canada, Department of Justice, 2002, p. 4).

Like the Convention on Cybercrime, the Canadian Lawful Access proposal appears to put the onus on even the most basic Internet service providers to become partners in surveillance. As it is written, ISPs could be defined to include schools, libraries, or social-service agencies. The Lawful Access document also attempts to justify creating new legislation because:

There is currently no mechanism that can be used to compel service providers to develop or deploy systems providing interception capability… (p. 7)

But, once they have been compelled to deploy such apparatus, the question of compliance arises. Who is complying with whom? Who will watch whom?, as critics of the now-discredited U.S. Total Information Awareness program (also known as “TIPS”) (Defense Advanced Research Projects Agency, 2003; Electronic Frontier Foundation, 2003) asked, because TIPS was thought to be too like Orwell’s 1984, or the former East Germany’s real-life Stasi.

The Canadian Lawful Access—Consultation Document also provides for greater state-sanctioned power to acquire personal information, particularly without the permission or knowledge of the party being investigated.

The USA Patriot Act is also notable for granting permission to search and seize information and for not informing the parties being investigated. Interestingly, it does not use the term “Internet service provider,” which prompts the question, if not specifically by way of ISPs, then which media in the U.S. will be used for investigation? The Patriot Act poses a universal threat to communicative privacy, particularly with regards to Internet surveillance, by allowing the use of the FBI’s “Carnivore” information-harvesting system, which (in simplistic terms) “trolls” the entire Internet indiscriminately looking for predetermined terms related to crime (Graham, 2004). The Patriot Act includes sections that identify the Act’s broad-ranging intentions, such as Section 206, which allows indiscriminate trolling and secret court orders to monitor electronic communication, and Section 215, which allows a variety of U.S. law-enforcement agencies to obtain search warrants, relatively easily, for a wide number of public and private institutions whose businesses include the use of computers—without any justification other than that the electronic records might be related to terrorism (American Library Association, 2004).

The Canadian Lawful Access document also uses vague language, but it is not the first time unclear language and unforeseen consequences in proposed legislation have come to the attention of legal and policy critics in Canada. In response to the first reading of the Criminal Law Improvement Act (1996), developed to address the search and seizure of computer data in wide-ranging pieces of legislation, co-founder of the Legal Group for the Internet in Canada, Dov Wisebrod, made the following observations:

The volume of data available in computers is growing dramatically, as is the number of sources of that data. As a result, the scope of a search warrant for a computer system under the new [legislative] regime is extremely broad. Since
any data contained in any computer anywhere in the world is available to any
other computer located anywhere else, when each has a modem and a phone
line, virtually all data would be covered by a warrant…. All information on the
Internet online service would be covered. (Wisebrod, 1996)

Given the potential universality of computer searches and the uncertainty of
who and what will be subject to searches in the “lawful access” proposal and legis-
lation, are employees of private companies, such as publishers and bookstores,
or public institutions that provide Internet service, such as libraries and educa-
tional or social-service institutions, going to be pressed into secret service, as they
are in the USA Patriot Act? Who would know about the surveillance in such instit-
ations? What would be done with the information? How long would it be held?
Who would see it and why? Who would know that their communication is under
investigation? Would someone under surveillance be given the opportunity to
explain or correct information that has been misinterpreted or poorly handled?
These issues, which have become standard concerns in the creation of corporate
privacy policies and legislation worldwide (OECD, 1981; Canada, 2000; CSA,
2004), are in jeopardy of being inadequately addressed.

Ironically, prior to September 11, 2001, privacy lawyers in Canada were con-
cerned about Canadian privacy laws affecting U.S. corporations (Klosek & Krza-
stek, 2001). We are experiencing quite the opposite issue now, as we are more
concerned, for example, that Canadian citizens’ information outsourced to U.S.
companies may be subjected to unreasonable search and seizure.

An array of objections

NGOs such as the computer rights advocate Electronic Frontier of Canada (EFC),
the Canadian Library Association, and others have criticized the Canadian Lawful
Access proposal. Electronic Frontier Canada criticises the Convention on Cybercrime
as vague and lacking firm justification for surveillance. EFC also notes that Canada’s
Lawful Access proposal is unnecessary in light of existing Canadian legislation.

Objections to the concept of “lawful access” itself have been heard from a
variety of other sources, including Canada’s former privacy commissioner,
George Radwanski. In a series of news releases and reports published in early
2003, Radwanski pointed to what he saw as the federal government’s growing dis-
regard for privacy and the systematic construction of a surveillance state. Citing
the federal government’s sporadic proposal for a national ID card, support for
police video surveillance, the potentially draconian anti-terrorist Public Safety Act
(which received Royal Assent in May 2004), and Lawful Access, he said, “The
government is, quite simply, using September 11 as an excuse for new collections
and uses of personal information about all of us Canadians that cannot be justified
by the requirements of anti-terrorism and that, indeed, have no place in a free and
democratic society” (Radwanski, 2003).

The Electronic Frontier Canada (EFC) concurred with Radwanski in its 20-
page response about Lawful Access submitted to the federal government:

The Proposal cannot be evaluated in isolation; it must be viewed in light of
other proposed erosions of privacy and freedom. For instance, it makes no
sense to contemplate a centralized database of Internet subscribers without also considering the plan of the Canada Customs and Revenue Agency (CCRA) to establish a database on the foreign travel activities of Canadians. (Electronic Frontier Canada, 2002, p. 2)

But is it necessary?
The Lawful Access—Consultation Document itself cites several justifications for its implementation, including coming into full compliance nationally with other proposals, such as the Council of Europe Convention; gaining lawful access to information transferred through “rapidly evolving technologies” (Canada, 2002, p. 3) (the document implies that current laws do not allow law enforcement to apply current “search and seizure” law to some new technologies); and bringing to bear rules that apply to some, but currently not all, wireless services (such as ISPs), which force them to have the appropriate technical capacity to carry out lawful access.

The Lawful Access proposal also cites three pieces of existing legislation that, if amended only slightly, would apparently guarantee law-enforcement agencies access to any Canadian citizen’s information: the Criminal Code, Canadian Security Intelligence Service Act, and Competition Act. The conviction rates for crimes investigated under these laws are already higher than 90% (Canada, 2002, p. 3), although it is not clear for what crimes convictions were achieved. With such a success rate, why is new legislation necessary?

Because electronic-surveillance work and upgrading technology to carry out surveillance are expensive, the issue of cost is also recognized in the Lawful Access document. The proposal specifies that as new technology is deployed, ISPs will have to bear the cost of upgrading their systems to accommodate new information-interception techniques. The proposal does allow ISPs to maintain their systems as they currently exist. But this is a hollow gesture, since the document acknowledges that rapidly changing technology is the raison d’être for proposing the new legislation. What thriving, competitive ISP could let its technology fall behind or tell anyone that its technology had become obsolete and expect to survive?

The task of collecting information for the government would fall to what is referred to in the Lawful Access—Consultation Document as the “custodian of documents” (Canada, 2002, p. 10). That (intentionally?) vague term implies that bank officials, academics, journalists, archivists, librarians, medical staff, or anyone who analyzes, gathers, organizes, or transfers information electronically could be responsible for covertly collecting personal information for the state. The prospect of training, or actually being part of, a cohort of state informers would signify an extreme departure from the laissez-faire origins of the “information society.”

The Lawful Access—Consultation Document considers, but does not clarify, what information should be collected, how long it should be stored, and when it should be destroyed (unlike the obvious concern for those issues in the CSA document and PIPEDA legislation). The Lawful Access document also explores the question of whether to seek out a specific person’s information occasionally
known as “data preservation”) or everybody’s personal information and communication all the time (“data retention”) or some variation on that theme. This is troubling—not just for its Orwellian implications, but also as a practical question. Once again, who will do this? How will the state decide what to collect, retain, use, and destroy? The Lawful Access—Consultation Document states:

The Criminal Code generally provides that law enforcement agencies cannot obtain documents of information without having reasonable grounds to believe that an offence has been or will be committed. This requirement is a safeguard that balances the state’s need to obtain evidence of a crime with the privacy interests of a person holding information. [italics added] (p. 11)

The Lawful Access proposal, however, could well render the concept of reasonable grounds irrelevant, because the investigation of database technology can be so intrusive and non-specific (as in the case of the U.S. Carnivore technology) that no grounds for reasonable search and seizure may even exist any longer.

Conclusion
It is unclear whether ISPs could be co-opted as de facto agents of the state. But no one in the Canadian government has said they would not be. If we no longer have the chance to maintain privacy, or even to contextualize the information the state has collected about us, the ramifications are extremely worrisome. While the issue of “lawful access” is not yet settled, it is incumbent upon citizens, as well as a responsible government, to be mindful of the necessary balance between privacy and security in a democratic society. Without such a balance, privacy becomes impossible, and much more than our privacy will be at stake.

References


