



October 23, 2009

**VIA FACSIMILE**

The Honourable Tony Clement, P.C., M.P.  
Minister of Industry  
C.D. Howe Building  
235 Queen Street  
Ottawa, Ontario K1A 0H5

Email: [Minister.industry@ic.gc.ca](mailto:Minister.industry@ic.gc.ca)

RE: Privacy Issues with Bill C-27 - the *Electronic Commerce Protection Act*

The Canadian Chamber of Commerce and the Information Technology Association of Canada (ITAC) are writing to you regarding the proposed amendments to the *Personal Information and Protection of Electronic Documents Act* (PIPEDA) being proposed in Bill C-27, the *Electronic Commerce Protection Act* (ECPA). In particular, we would like to raise concerns we have with s.78 of the Bill which renders inapplicable to Section 7.1(3) all of the exceptions listed in s.7 of PIPEDA. We also want to raise concerns we have about the proposed amendments to that Section.

As you know, the Canadian Chamber and ITAC support the principles of the ECPA and we urge the government to move expeditiously to have it enshrined in law. The Canadian Chamber and ITAC testified before the Industry Committee to recommend ways to improve the Bill. The government heard the recommendations from the Chamber, ITAC and other businesses and has made many beneficial changes to it.

However, we are still very concerned that the proposed changes to PIPEDA would have significant and adverse effects on public safety, security and privacy both on and off the Internet. We are writing to you to urge you to introduce appropriate amendments in the review of the Bill to correct the serious problems with the proposed language in the Bill.

We understand that one of the purposes of Section 7.1(3) is to prevent a person from collecting personal information from the Internet to send spam or create a spam list that can be used for this purpose. However, it is obvious that the Section is not so limited. In fact, this purpose is not even referred to in the Section.

Another possible purpose might be to prohibit computer hacking to obtain personal information. However, it is also clear that the Section is not limited to computer hacking, or even to any unlawful access to a computer in order to collect personal information.

The new proposed Section 7.1(3) is so broad that it will prevent the collection of personal information over the Internet for any purpose where the access is not authorized. Its breadth will prevent Canadians subject to PIPEDA from relying on crucial PIPEDA exceptions that are universally available in the offline world, in the online world, in order to collect or use personal information to combat and deal with emergencies, where needed in the interests of individual members of the public, or for the purposes of investigating a breach of an agreement or the contravention of Canadian or Provincial laws.

As you know, it is proposed that Section 7.1(3) of PIPEDA read as follows:

7.1(3) Paragraphs 7(1)(a) to (d) and (2)(a) to (c.1) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of

- (a) the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed without authorization; or
- (b) the use of personal information that is collected in a manner described in paragraph (a).

This provision is very broad. The term “any means of telecommunication” includes using a phone, handheld device or accessing the Internet with a computer; “accessing a computer system or causing a computer system to be accessed” is not limited to malicious acts like hacking into a computer or bypassing data security or a firewall but includes simply visiting a website using an Internet browser since anytime somebody visits a website they are “accessing a computer system” using a means of telecommunication; and “without authorization” simply means without consent.

So, when you put this together, the Section extends to prohibiting the collection of publicly available personal information over the Internet (or any other network) without first obtaining consent to do so from someone.<sup>1</sup>

The Section does not specify whether the authorization has to be express or implied. If the consent has to be express, it would not be available in the circumstances set out in Sections 7(1) or 7(2) of PIPEDA, as these exceptions were meant to apply precisely because consents cannot be obtained in such circumstances.<sup>2</sup>

---

<sup>1</sup> It is not clear who the authorization has to come from.

<sup>2</sup> If consent can be express or implied it is unclear when the consent must be express and when it can be implied. It is also unclear whether the principles set out in Section 3.4 of Schedule 1 will apply directly or by analogy, thus further complicating the interpretation of the Section.

However, even assuming that authorization includes “implied authorization”, it is uncertain whether Canadians could ever rely on an implied authorization in the circumstances set out in Sections 7(1) or 7(2) of PIPEDA. A chief problem is that since consent to collection or use of personal information cannot be obtained by implied consent in those situations, there is no basis to believe that the person would give implied authorization to access the person’s computer for the purpose of collecting personal information in those circumstances either. It would even impede the legitimate, and today fundamentally useful, function of search engines.

It simply cannot be assumed, as Bill C-27 does, that because a person makes available information over a website, blog, or another Internet or other networked connected device, the person will impliedly consent to someone accessing that site or device for a purpose that the person would not otherwise consent to. This is especially the case where access is for a clearly unwanted purpose such as investigating that person’s commission of a crime or other civil wrong (such as those set out below) that could have significant adverse effects and impose penalties and other sanctions on the person.

Moreover, it would be simple for a person seeking to avoid detection to make access to the person’s public website “unauthorized” to unwanted investigators by posting terms on the site that exclude access to investigators or any other persons who might monitor site activities to detect or collect evidence to combat illegal activities occurring at the site.

The exclusion of the usual PIPEDA exceptions listed in Sections 7(1) and 7(2) would impact activities far beyond matters of spam or spyware. Under the proposed legislation it would now become illegal for businesses to collect personal information over the Internet related to the investigation of any of following activities:

- Fraud, including bank, insurance, and credit card fraud
- Money laundering
- Securities violations
- Extortion, including online extortion
- Theft, misappropriation, or unauthorized use of confidential information/personal information
- Violations of business practices legislation
- Defamation
- Workplace-related sexual harassment
- Computer hacking, including committing the criminal offenses associated with theft of telecommunications services, making unauthorized use of a computer, or mischief in relation to data
- Identity theft or personation

- Violating the spyware or spam provisions in the ECPA
- Creating blocklists of email addresses of known scammers and spammers
- DNS attacks
- Violations of copyright by peer-to-peer networks and other infringers

Other important activities such as screening potential employees for positions of trust or where they may interact with minors would be seriously impeded.

So would efforts by online sites that are frequented by minors to investigate online crimes such as child grooming or luring. Online investigations of Internet harassment or stalking by companies trying to protect users would also potentially violate the law.

Further, the proposed exclusion of Section 7(2)(b) of PIPEDA could prevent using personal information publicly available on the Internet for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual without the consent of that individual (which may be unavailable at the time of the emergency). The proposed exclusion of Section 7(1)(a) would make it illegal to collect personal information even where clearly in the interests of the individual.

Moreover, this new exception to PIPEDA could make it illegal for Canadian businesses to develop and provide Canadians Internet privacy enhancing tools such as programs like Malware Patrol.<sup>3</sup> Programs such as these are designed to block spam, spyware, Trojans, viruses and other malware from an end-user's computer. These programs work by automatically crawling the Internet (using a means of telecommunication), collecting information from malware sites (accessing a computer) without obtaining any consent from the site owners (unauthorized access) and creating block lists to prevent malware from reaching end users. Information that these programs collect to create these block lists could be considered to be "personal information" under PIPEDA, such as email addresses and Internet Protocol (IP) addresses. Other programs use similar crawling technologies to create lists of email addresses of known spammers to protect end-users from spam. The development and updating of these programs could become illegal under s.7.1(3) of PIPEDA. This would inhibit the ability of Canadians to protect themselves against malware threats, a result that is directly contrary to the purposes of the ECPA.

The above examples are meant to be illustrative only.

It has been alleged that the only industries that would have problems with the breadth of Section 7.1(3) are the copyright industries. This contention is plainly false. Every Canadian subject to PIPEDA, in all fields of commerce and business, will be adversely affected by it.

As an example, under the ECPA, it may be impossible to learn about adaptive, intuitive or distributed network attacks by collecting information because it is not possible to obtain consent.

---

<sup>3</sup> <http://www.malware.com.br/>

As a further example, due to the ever increasing complexity of the wireless computing environment, attacks can now be launched unknowingly from handheld smartphones. It is essential that telecommunications service providers (TSPs) retain the ability to collect information about computerized terminals and smartphones that are connecting to their networks. In many cases it would be impossible to obtain necessary authorizations to collect personal information about cyber-attacks from such sources. As a result, there is a very strong possibility that this section may actually serve as an invitation to hack a commercial network or a server located on a TSP's infrastructure located in Canada.

The same impediments to obtaining authorization would apply to the detection of fraud, attempted theft of telecommunications, or gaining unauthorized use of a network or terminal device. Detection and prevention of these activities almost universally requires the collection of large amounts of information without the possibility of obtaining consents.

The exclusion of s.7(2)(a) from s.7.1(3) would also make it illegal to use personal information that an organization becomes aware of in the course of its activities about a crime that is being or is about to be committed for the purposes of investigating that contravention. This would make it illegal, for example, for Canadian businesses such as telecommunications providers to use information they might acquire to secure their networks and customers against cyber-terrorists.

None of the above concerns are being addressed in any of the proposed government amendments to the ECPA. We need to ensure that we don't make errors in the ECPA that will hinder investigating and taking counter-measures against cyber-criminals and cyber-terrorists.<sup>4</sup>

Note that in every other country, including the countries after which our proposed SPAM law has been modeled, such as Australia, New Zealand and Singapore, the provisions dealing with collecting electronic addresses or personal information are limited solely to collection for the purpose of sending spam or providing addresses to someone for that purpose. It seems to us that this would be a more appropriate approach to take in Canada. It would target the real problem – spam – without creating the very serious consequences that this provision will create for Canadians. We believe that your officials can readily put together appropriate wording to avoid the unintended negative consequence referred to above.

We want to emphasize that, in our view, the proposed amendments to PIPEDA in the ECPA have the real potential to significantly affect public safety, security and privacy on and off the Internet. They could lead to fraudsters, criminals, and other lawbreakers being immune from private investigations over the Internet and hamper the ability of Canadians to collect information that would assist public authorities in dealing with serious crimes. They would impede the functionality and usefulness of search engines.

Because violations of Section 7.1(b) will carry stiff penalties of up to \$1 million for each day on which a contravention occurred, the uncertainty regarding what access is authorized would chill

---

<sup>4</sup> See, Rodney Joffe, "The Cybercrime Epidemic", The National Post October 23, 2009, available at <http://www.nationalpost.com/scripts/story.html?id=2135828>

October 23, 2009

6

online investigations of very serious crimes and this could have very grave implications for security, safety and privacy of Canadians.

We strongly urge the government to reconsider its position with respect to amending Section 78 of the ECPA. This provision should be amended so that it targets only preventing persons from collecting electronic address information and personal information over the Internet or other means of telecommunication for the purposes of sending spam or enabling someone else to do so. It should not prevent accessing publicly available information for legitimate, indeed publicly beneficial, purposes.

Sincerely,



Perrin Beatty, President and CEO  
Canadian Chamber of Commerce



Bernard Courtois, President and CEO  
Information Technology Association of Canada

cc: Members of Industry Committee  
Jennifer Stoddart, Privacy Commissioner of Canada  
Elizabeth Denham, Assistant Privacy Commissioner of Canada