



LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

IN BRIEF



Federal and Provincial Initiatives to Facilitate Electronic Commerce

Publication No. 2008-61-E
5 November 2008
Revised 18 July 2012

Maxime-Olivier Thibodeau

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

***Federal and Provincial Initiatives
to Facilitate Electronic Commerce***
(In Brief)

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

Ce document est également publié en français.

Papers in the Library of Parliament's ***In Brief*** series are short briefings on current issues. At times, they may serve as overviews, referring readers to more substantive sources published on the same topic. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations in an objective, impartial manner.

CONTENTS

1	LEGAL IMPEDIMENTS TO ELECTRONIC COMMERCE	1
2	FEDERAL INITIATIVES	1
3	PROVINCIAL INITIATIVES	2
4	CONSUMER PROTECTION AND PRIVACY CONCERNS	3
5	CONCLUSION	5

FEDERAL AND PROVINCIAL INITIATIVES TO FACILITATE ELECTRONIC COMMERCE*

1 LEGAL IMPEDIMENTS TO ELECTRONIC COMMERCE

Since the mid-1990s, the use of electronic communication over the Internet has increased exponentially. In Canada, the federal and provincial governments have taken steps to recognize the use of electronic communications in commerce by removing legal obstacles to it. This involves treating paper-based documents and electronic documents as functionally equivalent, and ensuring that electronic communications will not be discriminated against or denied legal effect simply because they are in electronic form.

Despite the enactment of federal and provincial legislation in this area, however, many legal and policy issues remain. First, as online commerce has evolved, consumer protection issues, such as electronic authentication, have come to the fore. Second, privacy concerns continue to present policy dilemmas for those engaged in electronic commerce.

2 FEDERAL INITIATIVES

At the federal level, the *Personal Information Protection and Electronic Documents Act* (PIPEDA)¹ implements measures to create functional equivalency between electronic and paper documents. Part 2 of the Act provides for “the use of electronic alternatives ... where federal laws contemplate the use of paper to record or communicate information or transactions.” Among other things, the Act provides for:

- making payments to the federal government in electronic form;
- submitting information to the federal government in electronic form;
- using electronic documents to satisfy a requirement under federal law for a document to be in writing;
- providing electronic documents when an original document is required; and
- using electronic signatures.

In some situations, the Act requires the use of a “secure electronic signature” – an electronic signature resulting from the application of a prescribed technology or process. Before a technology or process can be prescribed, it must be proved that:

- the electronic signature is unique to the person using it;
- the person whose electronic signature is on the document has control of the use of the technology to attach the signature;

- the technology can be used to identify the person using the electronic signature; and
- the electronic signature can be linked to an electronic document to determine if the document has been changed after the electronic signature was attached to it.

In addition, the Act:

- provides that notices and Acts published electronically by the Queen's Printer have the same legal authority as notices and Acts published in paper form; and
- gives official status to the electronic version of revisions of the statutes and regulations of Canada as well as the consolidated version of the statutes and regulations.

Finally, PIPEDA regulates how private-sector organizations collect, use and disclose personal information in the course of doing business.

3 PROVINCIAL INITIATIVES

In 1999 the Uniform Law Conference of Canada published a model law, the *Uniform Electronic Commerce Act*, to facilitate electronic commerce at the provincial level. Since that time, all provinces and territories, with the exception of the Northwest Territories, have enacted legislation based on the Act.

The legislation contains a series of “functional equivalency” rules that set out the conditions that must be met for an electronic communication to satisfy a legal requirement for written communication. Overarching these rules is the principle that an electronic document will not be denied legal effect and enforceability simply because it is in electronic form. When information or a document must be in writing, the electronic equivalent is acceptable if it is accessible so as to be usable for subsequent reference. Where there is a legal requirement to provide information or a document to a person in writing, an electronic document will satisfy the requirement if it is accessible and capable of being retained by the person to whom it is provided.

The provision of original documents is dealt with under the legislation. A legal requirement stipulating that an original document must be provided, retained or examined will be satisfied by providing an electronic document if the integrity of the information has been maintained.

The legislation also covers the retention of documents and provision of copies. Where a document has to be retained for a period of time, an electronic version can be retained if it is accurate and available to the same extent as the original document and for the same length of time. Where multiple copies of a document must be provided, a single electronic version will be acceptable.

Contracts can be formed through electronic means when certain established rules have been followed. These rules:

- allow a contract to be formed by using electronic communication;
- allow a valid contract to be made by way of electronic communication, even when automated at one or both ends of the transaction;
- permit a transaction entered into between an individual and an electronic agent (computer program) to be cancelled if a material mistake is made, if there is no opportunity to prevent or correct the mistake, if the individual notifies the other party of the mistake, and if the individual returns or destroys any consideration received under the contract and does not benefit from receiving the consideration; and
- determine when electronic messages are deemed to have been sent and presumed to have been received.

Under the legislation, electronic signatures satisfy a legal requirement for a signed document.

4 CONSUMER PROTECTION AND PRIVACY CONCERNS

While PIPEDA and corresponding provincial statutes are meant to provide the basis for online commerce, the means of electronic authentication used today by financial institutions and online retailers largely supersede the requirement of electronic signatures to complete certain transactions set out in PIPEDA and provincial legislation. Current authentication processes include the use of username and password systems, credit and debit cards, personal identification numbers (PINs) and biometrics. Industry Canada attempted to fill the security gaps that exist in the absence of an updated PIPEDA by formulating principles on electronic authentication in 2004, but these guidelines have not been revised since their inception and are voluntary.²

In the meantime, authentication procedures have been the subject of some discussion. In 2008, the Public Interest Advocacy Centre (PIAC) published a report on authentication procedures in electronic commerce.³ The report included the results of a survey, which concluded that consumers are increasingly wary of security and privacy threats associated with electronic commerce. The report cited identity theft and “phishing” as problems that contribute to a lack of confidence in the system and threaten the growth of online retail and banking transactions.⁴

PIAC suggested that federal and provincial governments should be playing a greater role in protecting consumers, and recommended stricter regulations governing authentication, such as instituting standards and protocols to match the risk levels of the transaction that is being entered into. PIAC also recommended amendments to the law to provide that, as between the online retailer or bank and the consumer, the consumer should not face any liability for losses due to fraud and hacking. PIAC’s report called for more consumer education about authentication, along with requirements that banks and retailers disclose problems with authentication systems.

The PIAC report suggested that federal legislation provide for oversight of authentication systems by amending the *Bank Act*⁵ to institute audits of financial institutions by the Office of the Superintendent of Financial Institutions of Canada, for example. A corresponding audit system would be instituted at the provincial level to oversee retail authentication systems.

To protect privacy online, the PIAC report recommended that the authentication principles include direct references to privacy standards in PIPEDA. In addition, PIAC stated that consumers should be given a choice about how their privacy is protected, by deciding, for example, what personal information can be used to authenticate the online transaction. The Privacy Commissioner of Canada has also expressed concern about authentication procedures, and has released guidelines designed to help businesses to identify and authenticate customers consistent with fair information practices in PIPEDA.⁶

In the 3rd Session of the 40th Parliament, two bills amending PIPEDA were introduced together: bills C-28 and C-29. Bill C-28, known as Canada's anti-spam legislation, received Royal Assent on 15 December 2010.⁷ The bill's summary states that the legislation "establishes a regulatory framework to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities." In short, it:

- prohibits the sending of commercial electronic messages without the recipient's prior consent;
- provides rules governing the sending of these messages, including a mechanism for withdrawing consent;
- prohibits other practices that discourage reliance on electronic means of carrying out commercial activities, such as those relating to the alteration of data transmissions and the unauthorized installation of computer programs;
- provides for the imposition of administrative monetary penalties by the CRTC;
- provides for a private right of action;
- amends the *Competition Act* to prohibit false or misleading commercial representations made electronically; and
- amends PIPEDA to prohibit the collection of personal information by means of unauthorized access to computer systems, and the unauthorized compiling of lists of electronic addresses.⁸

The anti-spam legislation has not yet come into force. The government is still working on Governor in Council draft regulations, which must come into force at the same time as the legislation and other related regulations.⁹

Bill C-29, the Safeguarding Canadians' Personal Information Act, died on the *Order Paper* with the dissolution of the 40th Parliament. It was reintroduced as Bill C-12 in the 41st Parliament and read a first time by the Minister of Industry on 29 September 2011.¹⁰ Bill C-12 amends PIPEDA in accordance with the government's response to the recommendations of the House of Commons Standing Committee on Access to Information, Privacy and Ethics following the first parliamentary review of PIPEDA in 2007.

Among other measures, Bill C-12:

- specifies the elements of valid consent for the collection, use or disclosure of personal information;
- permits the disclosure of personal information without the knowledge or consent of the individual in certain cases; and
- requires organizations to report material breaches of security safeguards to the Privacy Commissioner and to notify the affected individuals and organizations of breaches that create a real risk of significant harm.¹¹

The Privacy Commissioner considers the requirement for businesses to report any breach in the security of personal information to be an acceptable standard, but believes that stronger enforcement powers are necessary.¹² There is no penalty for businesses that do not report real risks of significant harm to the Commissioner or to consumers.

5 CONCLUSION

The PIAC report, which focussed on electronic authentication in online banking and retail transactions, recommended that reform could take place through amendments to the *Bank Act*. The second parliamentary review of PIPEDA, to be conducted soon, could shed light on the legislation's shortcomings regarding commercial electronic transactions, taking into consideration any amendments that will apply should Canada's anti-spam legislation and Bill C-12 be implemented. This review could also allow for proposing amendments to PIPEDA's electronic signature provisions to reconcile them with existing electronic authentication systems. In the process, legal standards that would provide additional consumer and privacy protection could be applied to these systems.

NOTES

- * The original version of this document was prepared by Margaret Smith and updated by Andrew Kitching, both formerly of the Library of Parliament.
1. [Personal Information Protection and Electronic Documents Act](#), S.C. 2000, c. 5. PIPEDA contains a number of provisions meant to facilitate economic commerce, but also sets rules for the use of personal information in the course of commercial activity in Canada.
 2. Industry Canada, [Principles for Electronic Authentication: A Canadian Framework](#), May 2004.
 3. Janet Lo and John Lawford, [Are You Sure You Want to Continue? Consumer Authentication at the Crossroads](#), Public Interest Advocacy Centre, September 2008.
 4. Ibid. Phishing refers to fraudulent attempts to acquire personal information such as usernames, passwords and credit card numbers by masquerading as a trustworthy entity in an email or other electronic communication.
 5. [Bank Act](#), S.C. 1991, c. 46.
 6. Office of the Privacy Commissioner of Canada, [Guidelines for Identification and Authentication](#), October 2006.

FEDERAL AND PROVINCIAL INITIATIVES TO FACILITATE ELECTRONIC COMMERCE

7. [*An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*](#), S.C. 2010, c. 23.
8. Ibid., “Summary.”
9. Government of Canada, “[Regulations](#),” *Canada’s Anti-Spam Legislation*.
10. [Bill C-12: An Act to amend the Personal Information Protection and Electronic Documents Act](#), 1st Session, 41st Parliament.
11. Ibid., “Summary.”
12. House of Commons, Standing Committee on Access to Information, Privacy and Ethics, [Evidence](#), 29 May 2012, 1155 (Jennifer Stoddart, Privacy Commissioner).