CANADIAN PRIVACY LAW REVIEW

Volume 12 • Number 2 January 2015

In This Issue:

Are There Legal Foundations for CRTC Staff's Guidance on CASL's Computer Program Provisions?

Timothy M. Banks
Partner, National Lead for the Privacy and Security Practice
Dentons Canada LLP

Introduction

On January 15, 2015, provisions in Canada's Anti-Spam Legislation ("CASL")[1] relating to the installation of computer programs come into force. These provisions require express consent to the installation of computer programs (and updates and upgrades to those computer programs) in certain circumstances. Among the many difficulties with these provisions is that they apply to all types of computer programs (consumer or industrial) and all types of systems (including those that may not have a traditional user interface).

Recently, the Canadian Radio-television and Telecommunications Commission (the "CRTC") released guidelines on the computer program provisions.[2] The staff guidance is not binding on the CRTC and is not contained in a formal *Compliance and Enforcement Information Bulletin*. The informal nature of the advice weakens its value to industry participants. Moreover, during a recent presentation to the Canadian IT Law Association,[3] CRTC staff were challenged on whether some aspects of the guidelines could even be properly grounded in the legislation.

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

Design and compilation © LexisNexis Canada Inc. 2015. Unless otherwise stated, copyright in individual articles rests with the contributors.

ISBN 0-433-44417-7 **ISSN 1708-5446**
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $280.00 (print or PDF)
$425.00 (print & PDF)

Editor-in-Chief:

Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Editor:

Boris Roginsky
LexisNexis Canada Inc.
Tel.: (905) 479-2665 ext. 308
Fax: (905) 479-2826
E-mail: cplr@lexisnexis.ca

Note: This Review solicits manuscripts for consideration by the Editor-in-Chief, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Canadian Privacy Law Review* reflect the views of the individual authors and do not necessarily reflect the views of the advisory board members. This Review is not intended to provide legal or other professional advice and readers should not act on the information contained in this Review without seeking specific independent advice on the particular matters with which they are concerned.

The approach to CASL in the guidance is very helpful to industry participants because CRTC staff have made interpretive choices that narrow the application of CASL's installation of program provisions. However, whether the CRTC staff guidance can be properly grounded in CASL and the accompanying regulations is a matter of considerable concern, given the private right of action, which will come into force in approximately three years' time. This article examines key aspects of the staff guidance and begins the process of developing an analysis to support or ground the CRTC staff's views as a first step in assessing the risks of relying on that guidance to form the basis of a compliance program.[4] Although this article outlines an argument that largely supports the CRTC staff guidance, alternative views are, of course, possible. This article seeks to contribute to only the early stages of a debate that is likely to last for several years and in several forums.

Summary of CRTC Staff Guidance

For the purpose of this article, four positions in the CRTC staff's guidance are of interest. These positions and their potential compliance implications are set out below.

1. CASL does not apply when installing software on a computer of which the person performing the installation is the owner or authorized user.

    - This means that the express consent provision (with the mandatory disclosures) should not apply to mobile app downloads by consumers to their own devices from an App store or to pre-installed programs.

    - The express consent provisions and mandatory disclosures should not apply in the enterprise context where the installation is initiated by the organization onto its own devices used by its employees.

2. A person "causes to be installed" a computer program on another person's device if there is concealed software or undisclosed features within an installation. In these cases, CASL will apply.

- User-initiated installations may fall within CASL if there are hidden features in the software that would not be expected by the user. Therefore, disclosure of the purpose and features of software, prior to download and installation, is critically important.
- The mere making available of software or code to facilitate an installation probably does not result in the organization being deemed to be "installing" or "causing the installation".

3. If the installation is not initiated by the owner or authorized user, then consent is required.
    - Automatic updates that are not controlled by the owner or authorized user do require express consent. This can be obtained at the point of installation.
    - There may be significant compliance problems in obtaining consent to updates and upgrades where the computer system lacks a traditional user interface.
4. Certain spyware-like or malware-like features may require enhanced consent, but only if these functions would normally not be expected by the user.
    - These special features include programs that (1) collect personal information from the device; (2) interfere with the user's control of the device; (3) change or interfere with user's settings, preferences, or commands without the user's knowledge; (4) change or interfere with data in a manner that will obstruct the user's access to that data; (5) cause the device to connect to or send messages to another device without the user's authorization; or (6) install an application that can be activated remotely without the user's authorization.
    - Importantly, the CRTC appears to have agreed that the mere inclusion of these types of features does not require enhanced consent. The features must be unexpected, given the nature of the program.

CRTC staff's interpretation of what it means to *install* or *cause to be installed* a computer program is controversial. Adding to the controversy is how CRTC staff envision consent might work for updates to pre-installed software. Essentially, CRTC staff took the position during their presentation that a manufacturer or distributor (as an owner or authorized user) could provide consent to itself to the installation of pre-installed software and to all future updates or upgrades. If this position is correct, it would obviate the need to obtain consent from the ultimate owner or authorized user for updates to pre-installed software, except in limited situations.

Key Provisions of CASL

For the purpose of assessing the CRTC staff guidance, the key legislative provision is s. 8 of CASL. That section contains two restrictions. First, it states that a person must not (in the course of a commercial activity) "install or cause to be installed" a computer program on another person's computer system without consent. Consent must be obtained in the prescribed manner. Essentially, consent must be express after making certain disclosures, including identifying the person who is seeking the consent and clearly and simply describing, in general terms, the function and purpose of the computer program that is to be installed if the consent is given.[5] Second, s. 8 prohibits a person from causing the computer system to send messages from that computer system without the consent of the owner or authorized user. These prohibitions are subject to an exception if the person is acting under a court order and to limitations on extraterritorial reach.

For ease of reference, the full text of s. 8 states as follows:

> 8. (1) A person must not, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system, unless
>
> (a) the person has obtained the express consent of the owner or an authorized user of the computer system and complies with subsection 11(5); or
>
> (b) the person is acting in accordance with a court order.
>
> (2) A person contravenes subsection (1) only if the computer system is located in Canada at the relevant time or if the person either is in Canada at the relevant time or is acting under the direction of a person who is in Canada at the time when they give the directions.

In assessing enterprise risk, organizations must also pay attention to s. 9 of CASL. This section prohibits "aiding and abetting". Section 9 states:

> 9. It is prohibited to aid, induce, procure or cause to be procured the doing of any act contrary to any of sections 6 to 8.

The interpretation of these provisions should begin with the fundamental rule of statutory interpretation repeatedly adopted by the Supreme Court of Canada. That rule of statutory interpretation is that "the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament".[6]

In the case of CASL, s. 3 of the legislation contains a purpose clause to guide the application of the fundamental rule. Section 3 states:

> 3. The purpose of this Act is to promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities, because that conduct
>
> (a) impairs the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities;
>
> (b) imposes additional costs on businesses and consumers;
>
> (c) compromises privacy and the security of confidential information; and
>
> (d) undermines the confidence of Canadians in the use of electronic means of communication to carry out their commercial activities in Canada and abroad.

In the Regulatory Impact Analysis Statement for CASL, Industry Canada articulated the objective of CASL as follows:

> The general purpose of Canada's Anti-spam Legislation (CASL) is to encourage the growth of electronic commerce by ensuring confidence and trust in the online marketplace. To do so, the *Act* prohibits damaging and deceptive spam, spyware, malicious code, botnets, and other related network threats.[7]

In convenient shorthand, the purposes of CASL seem to boil down to discouraging unfair and deceptive practices that (1) undermine trust in electronic means to conduct commercial activities, or (2) increase costs of using electronic means of doing business. Faced with an interpretive choice, therefore, it would be absurd to choose an interpretation of ss. 8 and 9 of CASL that would lead to consequences imposing additional costs on businesses and consumers or would impair the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities unless there were some other benefit such as preventing the compromise of privacy or security of confidential information. Therefore, in interpreting the scope and application of ss. 8 and 9, we should keep in mind the remedial purposes of the legislation and not assume that Parliament intended to upend legitimate commercial activities or radically change the way in which Canadians use the Internet or Internet-connected devices.

Understanding *Install* and *Cause to Be Installed*

The terms *install* and *cause to be installed* are critical to defining the scope of s. 8 of CASL. There is no reason to believe that Parliament intended a technical interpretation of both terms. Indeed, there is a presumption of statutory interpretation against attributing technical meanings to words in legislative provisions.[8] There is a presumption that legislators are using the "language of the people".[9] It is too easy to forget that the legislation speaks to all Canadians, not just IT lawyers and their tech industry clients. Therefore, an interpretation of s. 8 of CASL should begin with an ordinary commonsense meaning of the terms *install* and *cause to be installed* in light of the overall purposes of the Act.

Dictionaries are a useful starting point to determine the ordinary meaning of words. However, the dictionary meaning of a word must be approached with caution because the dictionary meaning lacks the context of the Act's scheme, the object of the Act, and the intention of Parliament, which are critical to arriving at a proper interpretation of the legislative provision. In this case, the online *Oxford English Dictionary* defines *install* as to "place or fix […] in position ready for use".[10]

According to this definition, one installs a computer program when one downloads and makes the computer program ready for use on the computer system. This is the experience of installing a program that individuals have when downloading and selecting "install" on their laptop or desktop, or selecting "install" from an App store on a mobile device or tablet. The use of the ordinary meaning of the word *install* is evident in the CRTC staff guidance, which states, "CASL does not apply to owners or authorized users installing software on their own computer systems (e.g., personal devices such as computers, mobile devices or tablets)".[11] CASL simply does not apply because the person who is installing the software is not installing it on another person's device.

The ordinary meaning of *install*, as used by CRTC staff, disregards alternative interpretations that could have focused on the technical aspects of the installation process, such as the process of retrieving the file for download, saving the file to the device's memory, launching an installer program, and the completion of the installation by the installer program that may have been provided by the developer with the computer program or may be a more general purpose installer program already on the device. Rather, CRTC staff have chosen a non-technical interpretation that focuses on the user's perspective. If an individual chooses to make a program ready for use on his or her own device, the program is installed by that individual.

Leaving aside the fact that the CRTC staff's interpretation is supported by the presumption against non-technical interpretations of ordinary words, is such interpretation of *install* grounded in the scheme of the Act, the object of the Act, and the intention of Parliament? The purpose clause of CASL and the description of the object of CASL in the *Regulatory Impact Analysis Statement* suggests that the intention of CASL is not to regulate all installations of computer programs but to target certain unfair or deceptive practices, particularly the installation of spyware and malware, which compromise the confidentiality of information, increase costs to consumers, and diminish confidence in electronic means to conduct commerce. There would be no reason to regulate a user-initiated installation (even if aspects of the installation are controlled by the developer or platform) unless the installation was procured by deception or the program contained spyware or malware. Accordingly, the interpretation of *install* provided by CRTC staff, which limits the application of CASL, appears to be appropriately grounded in the stated purposes of CASL.

Can the same be said for CRTC staff's interpretation of *cause to be installed*? To illustrate what this term means, CRTC staff provide the following example in their guidance:

> Sometimes, malicious software (malware) is installed along with other software. For example, a free Tic Tac Toe app may include concealed malware that is not disclosed to the user. In this situation, the user would be installing the Tic Tac Toe app, so CASL would not apply. However, CASL would apply to the installation of the malware since the software developer would be causing it to be installed.[12]

This example may be maddening to those who are inclined to a technical interpretation of CASL. From a technological perspective, after all, the same process is being used to install the Tic Tac Toe app and the malware. Why then is one aspect of the app being installed by the user, and another by the developer?

However, returning to the purpose of CASL, the interpretation of *cause to be installed* may not be absurd at all. A person is the proximate cause of an installation when he or she intends to download and make available the program for use on his or her device. The causal relationship between the person and the installation is already inherent in the verb. However, the same cannot be said if the person did not mean to make the particular features of the program ready for use. Although an ordinary person may be the "cause in fact" of installing the spyware or malware (due to selecting *install* or clicking on the link to initiate the installation), he or she is not likely to perceive the situation this way. An ordinary meaning of *install* suggests some level of intention, control, or choice on the part of the person as to whether the computer program is made ready for use. In the case of deceptive spyware or malware, the individual would quite properly see himself or herself as having been duped into installing the software. In other words, the true cause of the installation originated somewhere else—"it was not *this* that I bargained for".

Perhaps, therefore, the CRTC staff guidance properly reflects the fact that understanding the terms *install* and *cause to be installed* in the context of the purpose of the legislation requires understanding who the proximate cause of making the computer program (and its features) ready for use on the device is. If the user initiates that process, the user will usually be the person who is installing the computer program. By contrast, the developer or platform will be the proximate cause of making the program ready for use in situations where the owner or authorized user of the device (1) has not intended to install the computer program or (2) has no control or choice over the installation. However, in addition, the developer or platform will be the proximate cause of the installation in cases where the owner or authorized user of the device has acted on a deceptive or misleading description of the functionality of a computer program, including in the sense of omitting to disclose functionality that would affect a reasonable person's decision to install or not to install a computer program. In this last situation, the owner or authorized user is simply a means through which the installation is initiated and not the proximate cause of making those hidden computer program features ready for use. In other words, the installation is procured through a deceptive representation. But for the deception, the computer program features would not be made ready for use.

One potential criticism of extending the interpretation of *causes to be installed* to include situations in which the installation is procured through deceptive representatives is that there are already provisions regarding deceptive and unfair practices that could address the evil of deceptive practices. For example, s. 74.01(1) of the *Competition Act*[13] provides that "a person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, the supply or use of a product […] makes a representation to the public that is false or misleading in a material respect". However, the fact that there are general consumer protection provisions does not necessarily lead to the conclusion that this interpretation is without merit. It is plausible that Parliament enacted a provision targeted at a particular type of conduct.

Pre-installed Computer Programs

Pre-installed programs create vexing problems. In these situations, the manufacturer or distributer is installing the computer program on its own device. Based on the interpretation of *install* discussed above, CASL does not apply. This means that the ultimate purchaser of the device never consents to the installation of the computer programs on the device. Does this undermine the validity of the interpretation given to *install* by CRTC staff? Moreover, it would be possible for a manufacturer or lessor of a device, or any intermediate owner, to install malware or spyware on the device that the manufacturer or lessor could then sell or lease to an unsuspecting user.

Is it necessary for CRTC staff to assert an interpretation of CASL that would address pre-installed spyware or malware? Perhaps not. An argument against the CRTC staff's interpretation would have more force if CASL were viewed as a complete code governing the purchase, sale, and use of computer programs. However, CASL's purpose clause and the *Regulatory Impact Analysis Statement* suggest more modest objectives. CASL complements the *Competition Act*, provincial consumer protection legislation, provincial *Sale of Goods Act* legislation, and the Quebec *Civil Code*.[14] CASL's purpose is to address perceived issues relating to conduct that discourages the use of electronic means to carry out commercial activities. Online installation of computer programs is properly within the scope of that purpose. Regulating the purchase and sale of goods (which include pre-installed software) treads into matters more traditionally within the purview of provincial jurisdiction.

Even if we restrict our analysis to federal legislation, there are indications that CASL is intended not to be a complete code but to complement other federal legislation. CASL itself amends and is to be read in conjunction with the *Competition Act* and the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*].[15] Just as Parliament may be considered to have enacted specific provisions to deal with certain activities that might be dealt with more generally by other statutes, CASL could leave certain issues to be dealt with by broader provisions in other statutes, such as s. 74.01(1) of the *Competition Act* (*e.g.*, deceptive representations) or *PIPEDA* (covert collection of personal information). The fact that CASL regulates installations of computer programs in some cases does not mean that it must regulate all types of installations and uses of computer programs.

Automatic Updates and Upgrades

Issuing of automatic updates and upgrades is only one of the areas causing significant concern for software developers and platforms.[16] CRTC staff appear to have taken the position that updates or upgrades that are "pushed" to devices by developers or platforms require express consent. CRTC staff's guidance provides the following example:

> If a person installs an app from an app store on their own device, CASL would not apply. As a result, their consent for future updates may not have been requested by the app developer. If the software developer wishes to install an update to the app at a later date, they must obtain the person's consent to do so. Alternatively, when the user self-installs the app, the developer can use that opportunity to request consent to automatically install future updates.[17]

This guidance is grounded in s. 10(7) of CASL, which provides:

> Subsections (1) and (3) [the prescribed disclosures for, and means of, obtaining express consent] do not apply in respect of the installation of an update or upgrade to a computer

> program the installation or use of which was expressly consented to in accordance with subsections (1) and (3) if the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent and the update or upgrade is installed in accordance with those terms.

During their presentation, CRTC staff suggested that express consent would not be required for updates or upgrades of pre-installed software if the manufacturer or intermediary had already consented to the installation of updates and upgrades.[18] There are a number of problems with this interpretation of which two are particularly important for the analysis in this article. Aside from the absurdity of providing consent to oneself, the CRTC staff's interpretation results in updates and upgrades to pre-installed software being treated very differently from user-initiated software, without any particular purpose for doing so. This is different from the distinction between pre-installed software and user-installed software. The reason for treating those differently is supported by the fact that one occurs pre-sale and the other post-sale. However, this is not the case with respect to updates and upgrades. The updates and upgrades that we are concerned about are post-sale installations. The trope of using an intermediary consent to work around the problem is not satisfactory.

Is there an alternative interpretation that builds on the CRTC staff's understanding of the terms *install* and *cause to be installed*? One approach would be to consider the update functionality from the user perspective. Software may contain functionality to check for updates programmatically and to install those updates automatically or install updates only when manually accepted by the user. The update feature is, therefore, controlled at the device level by the user. The default may be set to auto-update, but the feature can be configured by the user. In this situation, who is installing or causing the update to be installed? An argument could be made that the installation of the updates and upgrades is simply an extension of the user-initiated installation and the configuration of the device/programs by the user. In these cases, the user remains in control. The update is made available to the user, but it is still a "pull" update. By contrast, a true "push" update would not be managed by the user's device or would override the update settings on the user's device. Such updates could be considered as "caused to be installed" by the developer or platform.

This interpretation would also fit with the CRTC staff's view that the owner or authorized user must provide consent to an update or upgrade that would install a new feature requiring enhanced consent. Consistent with the prior interpretation of *cause to be installed*, there is a limit to what the owner or authorized user can be considered to be installing. The developer or platform would be considered to have caused the installation of the update or upgrade if the developer has included a feature in the update or upgrade that the developer or platform knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system.

This interpretation might be criticized, perhaps, for relying on a technical understanding of the update process. However, it is consistent with the overall purpose of CASL and does not require differentiating updates and upgrades to pre-installed software from those of user-installed software.

Of course, this leaves open the problem of devices without obvious user interfaces, such as components in machinery or appliances. For these types of devices, there may be no controls for the automatic updates or upgrades to the software. Other than not using the device, there may be no practical way to permit an owner or authorized user of the device to refuse updates and upgrades. The situation is not insurmountable, since there is deemed consent in s. 10(8) of CASL for the installation of operating systems. For machinery and appliances that do not have a user interface, it would not be a stretch to conclude that the programs that run on these devices are part of the operating system of the device, even if, as a technical matter, one could differentiate the base operating system from additional programs running on that system. The CRTC staff guidance recognizes this when it notes that operating systems include software that controls automobile components—such as braking systems. There would, of course, be a caveat that the spyware and malware features enumerated in s. 10(5) of CASL would require express consent, as it would not be reasonable to conclude that consent is deemed to the update or upgrade that would include features that the developer or platform pushing the update knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system. This answer is not wholly satisfactory, but it does have the merit of giving "operating system" a non-technical, ordinary meaning that is consistent with the purposes of CASL.

Conclusion

Overall, CASL is very problematic legislation. The computer program provisions are no exception. The recent CRTC staff guidance appears to be an attempt to outline an interpretation of key concepts that would restrain the application of CASL to limited situations that are consistent with the core purposes of the legislation. This interpretation is not beyond doubt by any means. It is possible that a court or the Commission could ultimately come to a different view. This creates material risk for any organization that relies on the CRTC staff guidance. Nevertheless, the CRTC staff guidance may be supportable by the principles of statutory interpretation. This article is only one early and tentative step in the development of a defensible interpretation.

[*Editor's note*: The views in this article are those of the author and do not necessarily reflect the views of his colleagues at Dentons or Dentons' clients. The interpretation of CASL by commentators and the CRTC is evolving. The author's own views may change.]

[1] CASL's full title is *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. The legislation has no official short title but has come to be referred to as "Canada's Anti-Spam Legislation" or "CASL".

[2] Canadian Radio-television and Telecommunications Commission, *CASL Requirements for Installing Computer Programs*, <www.crtc.gc.ca/eng/info_sht/i2.htm>. The guidance of the CRTC staff does not bind the Commission acting as a tribunal.

[3] CRTC presentation by Dana-Lynn Wood and Lynne Perrault on November 11, 2014; Andy Kaplan-Myrth of Industry Canada also participated.

[4] This author is no apologist for CASL. The commercial electronic provisions were, in this author's view, ill advised and overly complex. However, that issue goes beyond the scope of this article.

[5] *See* CASL, ss. 10(1), 10(3) and *Electronic Commerce Protection Regulations* (CRTC), SOR/2012-36, s. 4.

[6] Elmer Driedger's definitive formulation has been adopted in many cases, including *Bell ExpressVu Ltd. Partnership v. Rex*, [2002] S.C.J. No. 43, [2002] 2 S.C.R. 559, para. 26.

[7] Industry Canada, *Regulatory Impact Analysis Statement*, <http://fightspam.gc.ca/eic/site/030.nsf/eng/00271.html>.

[8] Ruth Sullivan, *Sullivan on Construction of Statutes*, 6th ed. (Markham: LexisNexis Canada Inc., 2014), 58–59.

[9] Although most commonly cited in insurance law, the presumption is not restricted to that context but reflects the presumption of the ordinary and grammatical sense of words in statutes. See *Stats v. Mutual of Omaha Insurance Co.*, [1978] S.C.J. No. 56, [1978] 2 S.C.R. 1153, para. 25;

Gibbens v. Co-operators Life Insurance Co., [2009] S.C.J. No. 59, 2009 SCC 59, para. 21; *Bishop-Beckwith Marsh Body v. Wolfville (Town),* [1996] N.S.J. No. 195, 135 D.L.R. (4th) 456 (N.S.C.A.); Sullivan, *ibid.*, 28–29.

[10] <http://www.oxforddictionaries.com/definition/english/install>.

[11] *Supra* note 2.

[12] *Ibid.*

[13] R.S.C. 1985, c. C-34.

[14] L.R.Q., c. C-1991.

[15] S.C. 2000, c. 5.

[16] It should be noted that CASL contains exceptions for certain types of updates and upgrades. For example, consent is deemed for the installation of an operating system, which should include any updates or upgrades to the operating system (CASL, s. 10(8)). Consent is also deemed for the following installations (*Electronic Commerce Protection Regulations*, SOR/2013-221, s. 6):

(a) a program that is installed by or on behalf of a telecommunications service provider solely to protect the security of all or part of its network from a current and identifiable threat to the availability, reliability, efficiency or optimal use of its network;

(b) a program that is installed, for the purpose of updating or upgrading the network, by or on behalf of the telecommunications service provider who owns or operates the network on the computer systems that constitute all or part of the network; and

(c) a program that is necessary to correct a failure in the operation of the computer system or a program installed on it and is installed solely for that purpose.

[17] *Supra* note 2.

[18] The problems with this interpretation were outlined by Barry Sookman in a recent blog post. See Barry Sookman, "CASL: Getting Consents for Upgrades to Computer Programs on Pre-installed and Resold Devices", *Barry Sookman* blog, November 24, 2014, <http://www.barrysookman.com/2014/11/24/casl-getting-consents-for-upgrades-to-computer-programs-on-pre-installed-and-resold-devices/#sthash.BdcOs0pt.hhAn5PBD.dpuf>.

A Higher Price Tag on Privacy? An Ontario Court Certifies a Class Action for Breach of Privacy

Christopher McClelland
Partner
Blaney McMurtry LLP

Organizations that collect or handle personal information are generally aware that they have an obligation to protect that information from loss or misuse. However, recent developments in the area of privacy law have highlighted the significant financial liabilities such organizations may face if they are found to be directly or indirectly responsible for privacy breaches.

In a recent example, the Ontario Superior Court of Justice (the "Court") certified a class action on behalf of 643 customers of a bank who allegedly had their private and confidential information misappropriated by a bank employee named Richard Wilson. In the case of Evans v. The Bank of Nova Scotia [*Evans*],[1] the plaintiffs have claimed damages against Mr. Wilson for breaching their privacy rights. However, the plaintiffs have also claimed damages against the bank on the basis that it was negligent in its supervision of Mr. Wilson and is vicariously liable for his improper acts.

Background

Mr. Wilson was employed by the bank as a mortgage broker. In the normal course of his duties, he had access to a significant amount of confidential information about the bank's customers, including sensitive financial information. During a period of approximately ten months beginning in 2011, Mr. Wilson copied the information belonging to 643 customers and provided it to his girlfriend, who then disseminated the information to third parties for fraudulent and improper purposes. At least 138 of the bank's customers subsequently complained that they were the victims of identity theft or fraud, which negatively affected their credit rating. Two of those customers brought a class action against Mr. Wilson and the bank.

The Claims against the Bank

For purposes of the certification motion, the Court found that the plaintiffs had made out a viable cause of action against the bank on the following grounds:

- **Negligence:** The bank acknowledged that it had failed to adequately supervise Mr. Wilson's activities, which, in turn, provided Mr. Wilson with the opportunity to access and remove confidential information for improper purposes. Mr. Wilson was able to access numerous customer accounts in a short period (as many as 47 customers' profiles in 46 minutes on one occasion) and at odd hours during the night. Accordingly, it was possible that the bank could be found liable for being negligent in its supervision of Mr. Wilson.

- **Vicarious liability:** Mr. Wilson did not defend the case and therefore was deemed to admit that he had misappropriated the plaintiffs' information and breached their privacy rights. By failing to properly supervise its employees, the bank created a situation where there was a risk that Mr. Wilson could engage in the wrongful conduct that harmed the plaintiffs. It was therefore possible that the bank could be found vicariously liable for the breach of privacy committed by Mr. Wilson.

The plaintiffs relied on the tort of "intrusion upon seclusion" in support of their claim that their privacy rights had been breached. This tort was initially recognized in the decision of the Ontario Court of Appeal in Jones v. Tsige.[2] In that case, the Court of Appeal noted that the tort was limited to "deliberate and significant invasions of personal privacy"[3] involving "financial or health records, sexual practices and orientation, employment, diary or private correspondence".[4] In the *Evans* case, the Court found that the claim against Mr. Wilson (and, indirectly, against the bank) met that standard.

Implications for Employers

The decision in *Evans* was limited to the preliminary issue of whether to certify the plaintiffs' action as a class proceeding. The determination of whether the bank is ultimately liable for damages in this case will require a full trial. However, the Court of Appeal in *Jones* held that a single individual who suffered a breach of privacy was entitled to damages of $10,000. If the bank is found vicariously liable for the breach of privacy suffered by 643 individuals, the potential damages are significant.

There are steps employers can take to minimize the likelihood that they will find themselves the subject of a class action for breach of privacy:

- Most employers will collect personal information from their employees and customers in the course of doing business. Employers must keep in mind that they are responsible for protecting this information from loss or misuse.

- Employers should be proactive in avoiding privacy breaches by establishing both administrative safeguards (policies on privacy and confidentiality and training on how to handle personal information) and technical safeguards (electronic monitoring and encryption technologies).

- Employers should monitor and supervise employees who have access to private and confidential information to protect against the actions of a "rogue employee" for whom they might be held vicariously liable.

While none of the above steps will eliminate the risk of a privacy breach, they could be critical in demonstrating that the employer is not responsible for creating the situation that led to the breach.

[1] [2014] O.J. No. 2708, 2014 ONSC 2135.

[2] [2012] O.J. No. 148, 2012 ONCA 32.

[3] *Ibid*., para. 72,

[4] *Ibid*.

INVITATION TO OUR READERS
Do you have an article that you think would be appropriate
for *Canadian Privacy Law Review* and that you would like to submit?
Do you have any suggestions for topics you would like to see featured
in future issues of *Canadian Privacy Law Review*?
If so, please feel free to contact Michael A. Geist
@mgeist@uottawa.ca
OR
cplr@lexisnexis.ca