



CANADA'S ANTI-SPAM LEGISLATION COMPUTER PROGRAM COMPLIANCE

- 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**

THE PROHIBITION - PURPOSE



- Meant to reduce instances of malware and spyware ... but goes beyond that

- Incorporates broad *Criminal Code* definitions:
 - “*computer program*” = data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function

- “*computer system*” = a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function

- “install” is not defined
- IC: CASL applies to installing computer programs on someone else’s computer system, not installations by persons on their own computing devices

- Requires express consent, not implied (requirements for express consent as discussed previously)
- 2 possible levels of disclosure when getting consent

- Clearly and simply state the purpose for which consent is sought and prescribed information identifying the person seeking consent (same as for CEMs)
- Clearly and simply describe, in general terms, the computer program's function and purpose

- If computer program performs certain functions, must clearly and prominently, separately from the license agreement:
 - Describe the program’s material elements that perform the function, including the nature and purpose of those elements and their reasonably foreseeable impact on the operation off the computer system, and
 - Bring those elements to the person’s attention

- Bring those elements to the person's attention separately from other information provided in request for consent
- Get written acknowledgement that the person understands and agrees that the program performs the specified functions

CONSENT – ENHANCED DISCLOSURE TRIGGERS



- Programs that the person seeking consent knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or authorized user:
 - Collecting personal information stored on system
 - Interfering with control of the system
 - Changing or interfering with settings, preferences, etc., without owner's knowledge

CONSENT – ENHANCED DISCLOSURE TRIGGERS



- Changing or interfering with stored data in a way that obstructs, interrupts or interferes with lawful access to or use of the data
- Causing system to communicate with another system or device without authorization
- Installing a program that may be activated by a third party without knowledge
- Any other prescribed function

- Person who receives express consent for installation of an “enhanced disclosure” program must:
 - For 1 year after installation, ensure that the consenting person is provided with an electronic address through which to request program’s removal or disabling
 - If consent based on inaccurate description program’s material elements, on receipt of that request within the 1-year period assist the person in removing or disabling the program as soon as feasible, without cost to the person

- Enhanced disclosure requirements do not apply to computer programs that performs any of those listed functions if the function only collects, use or communicates “transmission data”

- Relates to the telecommunications functions of dialing, routing, addressing or signaling;
- Is transmitted to identify, activate or configure an apparatus or device (including computer program), to establish or maintain a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- Does not reveal the substance, meaning or purpose of the communication

- Deemed to have expressly consented to installation of listed computer programs if person's conduct is such that it is reasonable to believe that the person consents to the installation
 - Cookies
 - HTML code
 - Javascripts
 - Operating systems

- IC regs allow telecom service providers to install programs on customers' computers/devices to:
 - Protect network security
 - Update/upgrade network
 - Prevent failure of computer system or program

- Telecom service provider = a person who, independently or as part of a group or association, provides telecommunications services
- Telecom service = a service, or a feature of a service, that is provided by means of telecom facilities
- Telecom facilities = any facility, apparatus or other thing that is used for telecommunications or for any operation directly connected with telecommunications

- 10(8) specifically mentions cookies in list of “deemed consent” computer programs – so are they “computer programs” and subject to CASL?
- IC: cookies are not programs – they are not executable, cannot carry viruses and cannot install malware
- CRTC: cookies are programs but are not “installed” and so not subject to CASL prohibition

- Cannot send CEMs to “electronic address”
- IC: IP address is not “electronic address” because not linked to identifiable person or account (and so banner advertising not subject to CASL)
- CRTC: IP address may be “electronic address”, at least in some situations

- No consent required for update/upgrade if:
 - Express consent to the installation and use of original program
 - Person who gave consent is entitled to receive the update/upgrade under the terms of the express consent
 - The update/upgrade is installed in accordance with those terms

- Effective: January 15, 2015

- Transition: if program already installed, consent to update/upgrade implied until earlier of:
 - Consent withdrawn
 - January 15, 2018 (3 years after s. 8 in force)

- Issue = program rules require express not implied consent

- Altering or causing to be altered the transmission data in an EM so it's delivered to a destination other than or in addition to that specified by sender

PHISHING



From: CIBC Online Banking [mailto:alert@cibc.com]
Date: July-30-13 11:36 AM
Subject: Access Card Blocked

Your Online Banking is Blocked



Because of unusual number of invalid login attempts on your account, we had to believe that, their might be some security problem on your account.

So we have decided to put an extra verification process to ensure your identity and your account security.

Please click on continue to the verification process and ensure your account security.

It is all about your security.

Thank you.

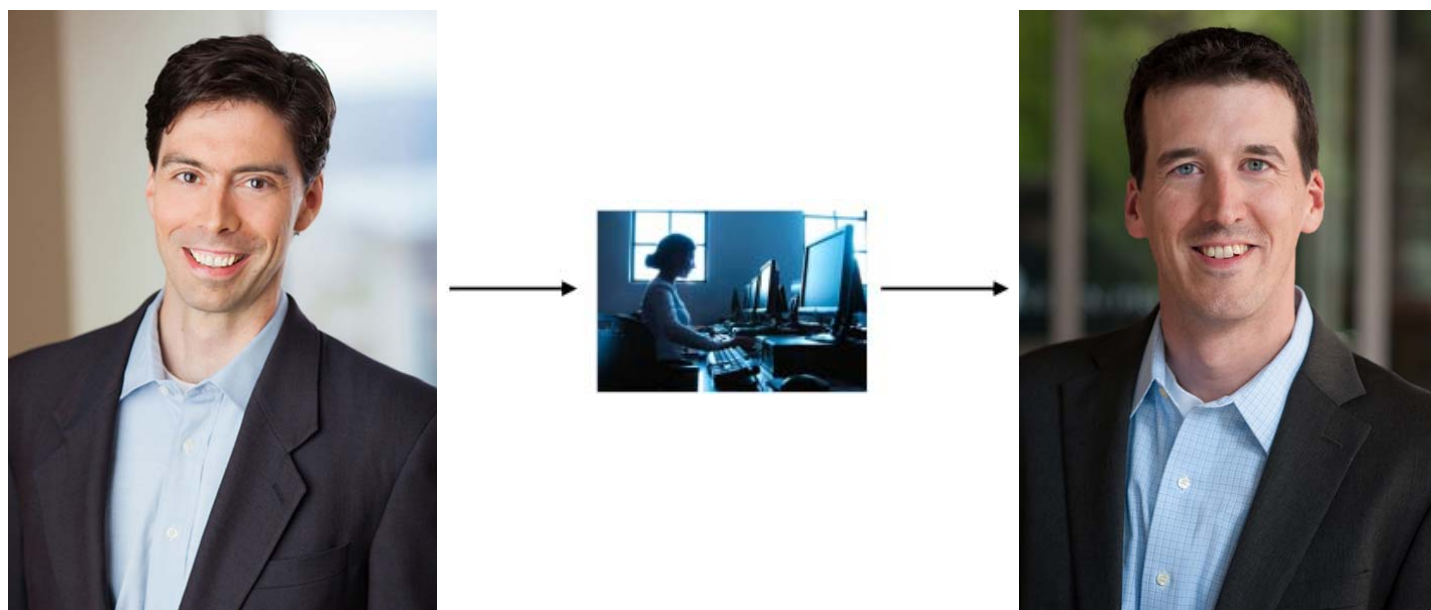
CIBC

Continue To Online Banking

MAN IN THE MIDDLE ATTACK



WOMAN IN THE MIDDLE ATTACK



- Not in the course of commercial activity
- Court order
- ISP
- Express Consent

- Same express requirement rules as discussed above

- If you have express consent:
 - Must also provide an electronic address to which person may send notice of withdrawal of consent

 - Give effect within 10 business days

- CASL amends PIPEDA to prohibit address harvesting
- Cannot collect individual's electronic address with a computer program designed primarily for generating or searching for, and collecting, electronic addresses
- Cannot use an individual's electronic address collected by such a program

- Cannot collect personal information through any means of telecommunications by accessing a computer system in contravention of an Act of Parliament
- Cannot use personal information collected that way