

Privacy Law and CASL

Issues, Updates and Lessons from 2016

Timothy M. Banks
Karl Schober

30 November 2016

Agenda

• Privacy

- **Consent**
 - Is implied consent a thing of the past?
 - Evolving definition of consent
- **Privacy Litigation**
 - Tort update
- **International Developments**
 - GDPR and what it means for Canada

• CASL

- **First Compliance and Enforcement Decision**
 - Insight gained from Blackstone
- **Additional Enforcement Activities**
 - Compu-Finder
 - Kellogg
- **Private Right of Action**
 - Preparing for July 1, 2017
- **Records! Records! Records!**

Canada's Anti-Spam Legislation

30 November 2016

3

大成 DENTONS

CASL

First compliance and enforcement decision

30 November 2016

4

大成 DENTONS

Blackstone Learning Corp.

- First CRTC compliance and enforcement decision (CRTC 2016-428)
 - In 2014, Blackstone sent over 385,000 CEMs to Canadian government employee email addresses obtained through various government websites
 - CEMs advertised education and training services offered by Blackstone, including technical writing, grammar and various management programs.
 - CRTC's Spam Reporting Centre received more than 60 complaints prompting investigation
 - [January 30, 2015](#): Notice of Violation to Blackstone
 - [February 14, 2015](#): Blackstone challenges Notice to Commission

Challenges:

1. Blackstone argued it had implied consent to send CEMs, and
2. Blackstone argued the penalty imposed by Notice was “unreasonably high”

Implied consent

- Implied consent to send CEMs based on “conspicuous publication exemption”
 - [Not so fast](#) – conspicuous publication does not automatically provide “persons sending commercial electronic messages with a broad licence to contact any electronic address they find online” and is evaluated on a “case-by-case basis”.
- Lack of supporting information of required conditions to rely on exemption:
 - where and when public email addresses were obtained
 - publication was conspicuous
 - that no statement indicated that recipient did not want to receive unsolicited commercial electronic messages
 - how it determined that CEMs sent were relevant to the business role or function of the recipient
- **Lesson:** Records required to demonstrate how email addresses are obtained online as well how to establish link between email sent and recipients business role or function.

Reasonable penalty?

- Initial administrative monetary penalty (AMP) of \$640,000 in Notice
- Reduced to \$50,000 following review by Commission against several factors under CASL (sub. 20(3):
 - purpose of penalty – to promote compliance, not punish
 - nature and scope of violation
 - ability to pay
 - cooperation and self-correction
- **Lessons:** Challenging a Notice may provide value in limited circumstances, however, as enforcement and guidance increases, organizations are expected to know CASL and have proper records and cooperate with CRTC.

CASL

Additional enforcement activities

Compu-Finder

• OPC

- May 2016 - Report of Findings
 - use of address harvesting programs to search, collect and use emails without consent
 - **records**: Inadequate and at times contradictory to Compu-Finder's position
 - compliance agreement requiring destruction of email addresses improperly collected and prohibition of use of address harvesting programs, etc.
- August 2016 – Knowledge Session
 - Commissioner-initiated investigation and the reasonable grounds burden
 - sharing of investigative information between agencies

Status: **Closed**

• CRTC

- March 2015 – Notice of Violation
 - allegations of lack of consent to send CEMs as well as unsubscribe mechanisms did not function as required
 - “substantial” complaints to Spam Reporting Centre for particular industry sector
- Evidence of lack of cooperation with CRTC

Status: **Ongoing**

Kellogg Canada Inc.

- Compliance and Undertaking and **\$60,000** AMP
 - alleged violations by Kellogg and its service provider
 - from October to December 2014
 - sending of CEMs without consent
- **Take away**: liable for your **third party** agencies
 - responsibility and obligations over authorized third party service providers who assist in sending CEMs
 - compliance programs must cover such service providers, including monitoring and auditing rights

CASL

Private right of action

Private right of action

- Kicks in **July 1, 2017**
 - Any individual or organization may launch action against violating individuals or organizations
 - affidavit of allegations and if applicable, any actual loss or damage suffered, or expenses incurred as a result
 - hearing of the application
- **Liability:**
 - Officers, directors and agents can be jointly and severally liable for contraventions if they directed, authorized, assented to, acquiesced in or participated in the breach.
 - Businesses are vicariously liable for acts of its employees

Private right of action

- Actual and statutory damages may be awarded:
 - Lack of consent, missing identification information or failed unsubscribe = \$200 for each contravention of CASL, up to \$1 million, for each day in which contravention occurred
 - Installation of computer program without consent = \$1,000,000 for each day on which the breach occurred.
- Some factors that must be considered by Courts for statutory damages:
 - Nature and scope of contravention
 - Whether the sender financially benefited from contravention
 - Ability to pay
 - Other factors established by regulations
 - additional Regulations in near future?

Private right of action

- Some recommendations in getting ready for July 1, 2017
 1. Compliance Programs
 - develop a documented program (if none currently exists)
 - review and update existing program as necessary
 2. Internal or external audit of communication systems
 - For example, audit and report by outside counsel
 3. Review procedures with any third parties
 4. Review complaints process
 - Can a quick and efficient internal customer service process minimize risk of potential complaints to CRTC or worse, private right of action?
 5. Records...

CASL

Records! Records! Records!

Records: advisory and guidance

- Emphasis that records should document:
 - All evidence of express or implied **consent** from individuals who agree to receive CEMs, for each CEM sent.
 - evidence can be in various forms such as audio, copies of signed consent forms, copies of business agreements, data capturing electronic forms or other consent.
 - CEM recipient consent logs
 - Procedures and methods through which senders collect consent
 - All **unsubscribe requests** and subsequent actions taken
 - **Written** compliance program
 - policies
 - procedures
 - training
 - audits

Although the pre-existence of a corporate compliance program may not be sufficient as a complete defence to allegations of violations under the Rules or CASL, a credible and effective documented program may enable a business to demonstrate that it took reasonable steps to avoid contravening the law.

– Compliance and Enforcement Information Bulletin
CRTC 2014-326, 4

Implied consent & privacy

Choosing the form of consent

PIPEDA Report of Findings #2015-001, Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program

- In April 2015, the Office of the Privacy Commissioner concluded that express opt-in consent was required for the Bell Relevant Advertising Program
- Why?
 - Bell would use and keep sensitive URLs (the specialized dating site example)
 - Bell had highly detailed and multi-faceted profiles (albeit 90 day data)
 - Users were paying for telecommunication services and the use of data for advertising was a secondary use
 - Heavy focus on the “nature of telecommunications services”

Implied consent is permissible, sometimes

- Implied consent was always permissible under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).
 - See clause 4.3 of Schedule 1
- However, the form of consent depends on a number of factors including the expectations of the individual and the sensitivity of the information.

Cl. 4.3.6

The way in which an organization seeks consent may vary, **depending on the circumstances** and the type of information collected.

An organization should generally seek **express consent** when the information is likely to be considered **sensitive**.

Implied consent would generally be appropriate when the information is **less sensitive**.

Explicit requirement for “informed” implied consent

- PIPEDA was amended in June 2015 and included an explicit requirement for consent to be informed.

[...] the consent of an individual is **only valid** if it is reasonable to expect that an individual to whom the organization's activities are directed **would understand the nature, purpose and consequences** of the collection, use or disclosure of the personal information to which they are consenting.

- Did this increase the burden? Hard to say.
- Need to reconcile with cl. 4.3.2.

cl. 4.3.2

The principle requires “knowledge and consent”. Organizations **shall make a reasonable effort** to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can **reasonably understand how the information will be used or disclosed**.

Royal Bank of Canada v. Trang: implied consent

- Bank wants to levy execution on property owned by the judgment debtors
- Problem: the property has a mortgage on it
- Mortgagee says it cannot disclose the amount left owing without consent
- Judgment creditor tries to get the information through a judgment debtor exam but could the debtors are no shows
- Bank seeks order to compel mortgagee to produce the information but the mortgagee refused
- Bank examined the mortgagee but mortgagee refused to produce the information
- Bank seeks order to compel the information but this is again refused
- Bank appeals

Where the courts disagreed

Court of Appeal (majority)
2014 ONCA 883

- **Two relevant criteria** for implied consent: sensitivity of the information and the reasonable expectations of the individual
- Sensitivity in the total context of the relationship between the individual and the organization
- **Interests of a third party organization are irrelevant**

Supreme Court of Canada
2016 SCC 50

- **Whole context is relevant** - sensitivity of the information must be assessed in light of what else is already in the public domain, the purpose served for making that related information public, and the relationship between the mortgagor, the mortgagee and directly affected third parties
- **Not merely a private matter** between mortgagor and mortgagee

On legitimate business concerns

SCC says:

In my view, when determining the reasonable expectations of the individual, the **whole context is important**. [...]

Indeed, to do otherwise **would unduly prioritize privacy interests over the legitimate business concerns** that PIPEDA was also designed to reflect, bearing in mind that the overall intent of PIPEDA is “to promote both privacy and legitimate business concerns”.*

*L. M. Austin, “Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices” (2006), 44 *Can. Bus. L.J.* 21, at p. 38.

Some life left in the old dog

- Whole context is important to considering sensitivity and reasonable expectations
- But effectively, the onus is on an organization to demonstrate:
 - not sensitive in context (objective standard)
 - individual has (subjective) or would have (objective standard) knowledge of the purposes
 - the purposes are appropriate (objective standard)
- Problem with an objective analysis is that it is dependent upon on the decision-maker’s views and beliefs (in the Bell case, the OPC explicitly rejected survey evidence)
- The OPC is running a consultation right now; there will be continued pressure towards express consent

Litigation update

Intrusion upon seclusion

- **John Stevens v Glennis Walsh, 2016 ONSC 2418**
 - plaintiff and defendants were pilots; defendant was given access to plaintiff's calendar (known as a family calendar that lets people know where you are); but defendant accessed calendar to give the information to the plaintiff's estranged wife;
 - why it is important: the court found that the access for the improper purpose was an intrusion
- **St. Patrick's Home of Ottawa Inc. and CUPE, Local 2437, 2016 CarswellOnt 3234 (Arb)**
 - in response to requests from employer A, employer B released medical information that had been provided to employer B in response to "fitness to work" and workplace accommodation issues; employer A was suspicious of the employee's requests for accommodation
 - why it is important: low damages of \$1,000 awarded even though this was clear breach
- **Jane Doe 464533 v. D. (N.), 2016 ONSC 541**
 - ex-boyfriend solicits plaintiff to send him a video that the posts; the video is online for about three weeks and had showed it to mutual friends;
 - concurrently liable for breach of confidence, infliction of mental distress; tort of publicity
 - general damages of \$50,000 plus punitive damages \$25,000
 - why it is important: court fashioning its own remedy for revenge porn

Tort of publicity (publication of private facts)

- Jane Doe 464533 v. D. (N.), 2016 ONSC 541
 - tort was successful in the revenge porn case
 - why it is important: tort has been recognized in Ontario
- Canada v. John Doe, 2016 FCA 191
 - decertified tort of publicity in medical marijuana case; test: (a) give publicity to a matter concerning the private life of another person where the matter publicized is of a kind that (a) would be highly offensive to a reasonable person and (b) is not of legitimate concern to the public
 - failed the publicity part of the test; mail delivery is not publicity
 - why it is important: publication is not a low threshold

Vicarious liability

- PSEU v. Ontario (Ministry of Training, Colleges and Universities), 2016 ONSC 6348 (Div Ct)
 - employee claimed intrusion upon seclusion when another employee accessed the EI records of the employee; employee claimed that employer was vicariously liable; court upheld reasonableness of decision that the employer was not vicariously liable
 - snooping happened without sanction or knowledge of the employer; not sufficiently related to conduct authorized by the employer; did not further employer's aims; was contrary to policy; did not relate to inherent friction and confrontation in the workplace
 - why it is important: the possibility of vicarious liability has been recognized but the intentionality of the tort is going to make it difficult to prove if there is a strong compliance program

International developments to watch

- A big story for the next 18 months will be the EU General Data Protection Regulation
- Many Canadian processors will come directly under the EU regulations and may even be required to have an office in the EU
- As a general concern, Canada's "adequacy" for the purposes of data transfers from the EU is likely under threat
- Always has been a limited ruling
 - Only covers personal information and entities governed by PIPEDA
 - So, doesn't cover intra-organizational transfers of employee personal data except where for federal works, undertakings or businesses
 - Arguably may not cover employee data transfers to service providers
- EU may be concerned about lack of intelligence oversight in reconsidering adequacy

30 November 2016

29

大成 DENTONS

Thank you

大成 DENTONS

Dentons Canada LLP
77 King Street West
Suite 400
Toronto, Ontario M5K 0A1
Canada

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com

© 2016 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This document is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. We are providing information to you on the basis you agree to keep it confidential. If you give us confidential information but do not instruct or retain us, we may act for another client on any matter to which that confidential information may be relevant. Please see dentons.com for Legal Notices.