The CIO Association of Canada – Calgary Chapter

What is New in Digital Communications and Privacy? : CASL Enforcement Update, Mandatory Breach Notification and EU GDPR

September 21, 2017

Martin Kratz, Q.C.

Bennett Jones

Agenda

- Three updates – lots to cover

- **Refresher - *Canada's Anti-Spam Legislation*** (CASL)
- Review of enforcement actions

- ***Privacy Update – New Mandatory Breach Notification Rules***

- ***High Level Overview of EU's General Data Protection Regulations***

Bennett Jones

The fine print…

This presentation was prepared to provide general information on recent legal developments and topical issues relating to anti-spam and privacy legislation in Canada. Due to the general nature of this presentation, nothing herein should be relied upon as legal advice.

Bennett Jones

CASL

Three Years of Enforcement Experience

Bennett Jones

Key Electronic Communications Prohibition

- It is **prohibited to send** or cause or permit to be sent **a commercial electronic message** (CEM) to an electronic address unless:
  - the message is **exempt** under CASL;
  - ***OR***
    - the messages meets the **formality** requirements; ***AND***
    - the person to whom the message is sent **has consented** to receiving it.

Bennett Jones

Assessment of exemptions

- *Bejm v. Law Society of British Columbia*, 2015 BCSC 169
- LSBC communicated messages via email through Craigslist in respect of unauthorized legal practice – Bejm seeks to prohibit "unauthorized messages" claiming violation of CASL
- Court finds:
  - Messages not "commercial" so not a CEM
  - Exempt as Bejm engaged in commercial activity and the message consists solely of an inquiry or application related to that activity
  - Exempt sent to satisfy a legal or juridical obligation
- Exemptions interpreted broadly by the Court in this case

Bennett Jones

Formalities

- A commercial electronic message must contain:
  - the **name of the sender ,** the name under which the sender carries on business, and the name of the person on whose behalf the message is sent (if any);
  - **the mailing address, and** either:
    - a telephone number;
    - an email address; or
    - a web address; and
  - an **unsubscribe mechanism**.

Bennett Jones

Unsubscribe

- Majority of enforcement decisions have involved technical defects with unsubscribe mechanisms
  - Must be set out 'clearly and prominently'
  - Must be able to be 'readily performed'
  - Must be given effect without delay
    - within 10 days
  - Must remain in force for 60 days after message sent

- Enforcement learning – a recipient may not use the mechanism properly so must assess your process

Bennett Jones

CASL Enforcement action

- CRTC have received about a million complaints
  - Proactive investigation
  - Honey pot sites
  - International Cooperation
- Triage process
- Reporting on cases by press release / two enforcement decisions
  - Limited information available to assist in guidance for your organization's compliance program

Bennett Jones

CASL Enforcement Actions

- **Access Communications**
  - computer reseller based in Saskatchewan
    - Malware infected server sent millions of messages – unknown to owner
    - 24 million emails June 2014
    - 73 million emails July 2014
  - CRTC notified owner
  - Small business cooperates to remedy
  - **No fine**

CASL Enforcement Actions

- **Compu-Finder**
  - Sent four CEM campaigns without consent,
    - between July 2, 2014 – September 16, 2014
    - promoting training courses
    - unsubscribe mechanisms did not function properly
      - not valid for 60 days after message sent
      - No indication given effect without delay
  - Analysis shows Compu-Finder responsible for 26% of all complaints received at the time
  - **$1.1 million dollar** penalty
  - Compu-Finder disputing the Notice of Violation

Bennett Jones

CASL Enforcement Actions

- **Compu-Finder**
- OPC conducts its own investigation of Compu-Finder
  - Commissioner initiated investigation under Principle 4.3 – Consent
  - Results:
    - Collecting personal information, not just business contact information
    - Lack of appropriate consent
    - Use of addresses after July 1, 2014 using address harvesting software brings PIPEDA S. 7.1(2)(b) into play so can not claim under 'publicly available' exception

Bennett Jones

CASL Enforcement Actions

- **Compu-Finder -** OPC recommendations

1. Designate an individual responsible for compliance with the Act;
2. Develop and implement a privacy policy and procedures;
3. Publish the policy in an easily accessible and understandable form;
4. Train employees on the privacy policy and procedures;
5. Consent: revise the telemarketing script to be compliant;
6. Maintain appropriate records and evidence of express and implied consent;
7. Only market to individuals from which proper consent has been obtained;
8. Cease automated forms of collecting e-mail addresses; and
9. Commission a third party audit of its privacy practices.

CASL Enforcement Actions

- Compu-Finder key lessons
  - You need to be able to back up your responses
  - An accountability framework is key
  - Due diligence is key
  - Record keeping is key
  - Using email harvesting software removes the exemption for 'publicly available information'
  - Must be transparent about privacy practices

- **Must comply with <u>both</u> privacy obligations and CASL obligations!**

Bennett Jones

CASL Enforcement Actions

- **Plenty of Fish** (social media dating service)
  - Sent commercial electronic messages to registered users of the Plenty of Fish online dating service, on its own behalf
  - Messages contain an unsubscribe mechanism:
    - that was not set out ‘clearly and prominently’ and
    - was not able to be ‘readily performed'
  - Respond to complaint with Undertaking
    - implement a compliance program
    - brought their unsubscribe mechanism into compliance with CASL
    - **$48,000** penalty

Bennett Jones

CASL Enforcement Actions

- **Porter Airlines**
  - Sent commercial messages without an unsubscribe mechanism
  - Did not honour unsubscribe requests
    - In one case within 10 days
  - Unsubscribe issues
    - Notice of unsubscribe not prominently set out
    - Some messages had 2 unsubscribes , one of which did not work
    - Some messages had no unsubscribes
  - Unable to prove consent in all cases
  - Respond to complaint with Undertaking
    - implement a compliance program
    - brought their unsubscribe mechanism into compliance with CASL
    - **$150,000** penalty

Bennett Jones

CASL Enforcement Actions

- **Rogers Media**
  - Sent commercial messages without an adequate unsubscribe mechanism
    - Not enabled, or
    - Not able to be readily performed
  - Did not contain an electronic address valid for 60 days
  - Did not honour some unsubscribe requests within 10 days
  - Respond to complaint with Undertaking
    - implement a compliance program
    - brought their unsubscribe mechanism into compliance with CASL
    - Commit that 3rd party service providers will also comply with CASL
    - **$200,000** penalty

Bennett Jones

CASL Enforcement Actions

- **Kellogg Canada**
  - Sent CEMs during a period of October – December 2014 without consent
  - Some work carried out by 3rd party message service provider
  - Respond to complaint with Undertaking
    - implement a compliance program
    - commitment to require 3rd party message service providers to comply with CASL
    - **$60,000** penalty

  - **Note customer is responsible for the service provider's actions!**

Bennett Jones

CASL Enforcement Actions

- **Blackstone Learning Corp.**
  - Sent 9 CEM campaigns without consent
  - Compliance and enforcement decision
  - CRTC issues penalty of **$640,000**
  - Blackstone defends claiming implied consent based on conspicuous publication
  - Blackstone did not provide evidence to show:
    - where or how it discovered any of the recipient addresses,
    - when the addresses were obtained,
    - whether their publication was conspicuous,
    - whether they were accompanied by a disclaimer statement, or
    - how Blackstone determined that the messages it was sending were relevant to the roles or functions of the intended recipients
  - Penalty reduced to **$50,000**

Bennett Jones

CASL Enforcement Actions

- **William Rapanos**
- Operates service printing and distributing flyers
  - 3 message campaigns (58 complaints received by CRTC)
    - 3 violations – sending CEM to a person without consent
    - 3 violations – sending CEM without the prescribed information
      - Identifying the sender
      - Contact details
    - 1 violation – sending CEM without an unsubscribe mechanism
  - **$15,000 penalty**
  - CRTC does not buy defenses (i) it was not me but boarders using my wifi (though CEMs sent from his domain) (ii) victim of identity theft, (iii) proof must be beyond a reasonable doubt or violates Charter

Bennett Jones

CASL Enforcement Actions

- **Mr. Halazon and TCC**
  - Mr. Halazon, CEO of Couch Commerce
  - Alleged CEMs sent with unsubscribe mechanism that did not work
    - could not be readily performed,
    - requests not acted upon in 10 days
  - Couch Commerce goes bankrupt
  - CRTC pursues Mr. Halazon **personally** under S. 31 CASL
  - Undertaking
  - Mr. Halazon pays **$10,000** penalty
  - Successor company, TCC agrees to implement compliance program

Bennett Jones

CASL Enforcement Actions

- Summary Learnings to date
  - Legitimate businesses are often being pursued under CASL
  - Formalities and technical compliance are essential to avoid liability
  - Understand CASL. The legislation is complex and has contradictory provisions. A potential defendant should carefully assess the legislation.
  - Develop a compliance program. Development of a policy and actions to support the compliance efforts mean that an organization is more likely to understand the scope and limitation of the implied consent regime under CASL.
  - Must comply with both CASL and privacy law.

Bennett Jones

Privacy Update

Mandatory Breach Notification

Bennett Jones

Breach Notification

- Notification can be an important means of risk mitigation
  - Effort to communicate to customers
    - Empower customers to protect themselves
    - Can mitigate reputational impact
  - Important to provide first stage of remediation

- Mandatory in Alberta since 2010
- Soon to be mandatory nationally under PIPEDA
- Draft Regulations released

Bennett Jones

Alberta PIPA

- Mandatory to report the breach to OIPC - 2 stage process:
  - (1) would a reasonable person consider that a real risk of "***significant harm***" exists to an individual as a result of the breach?
    - Some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident.
    - The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.
    - Risk of detriment, damage, injury, humiliation, etc.
  - (2) Is there a "***real risk***" of the significant harm will occur?
    - The likelihood that the significant harm will result must be more than mere speculation or conjecture. Must be a cause and effect relationship between the incident and the possible harm.
    - E.g. circumstances such as encryption may mitigate risk.
- OIPC to advise on notification or not - based on harm assessment

Bennett Jones

PIPEDA Breach Notification

- Reporting obligation – unless prohibited by law
- Obligation of an organization to report to Federal Privacy Commissioner
  - Any breach of security safeguards
  - If reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual
- Obligation of an organization to report to individual
  - Any breach of security safeguards
  - If reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual
- Notification to contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm

Bennett Jones

PIPEDA Breach Notification

- Notification shall be given as soon as feasible after the organization determines that the breach has occurred
- Factors relevant to whether a breach of security safeguards creates a real risk of significant harm to the individual include
  - sensitivity of the personal information involved in the breach,
  - probability that the personal information has been, is being or will be misused
- Additional duty of organization to notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm

Bennett Jones

PIPEDA Breach Notification

- PIPEDA Breach Notification
- An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control
- Organization shall, on request, provide the Commissioner with access to, or a copy of, a record

- Regulations published for comment September 2, 2017

Bennett Jones

PIPEDA Breach Notification Regulations propose

- Breach of Security Safeguard Report to **OIPC** must be in writing and contain:

(a) a description of the circumstances of the breach and, if known, the cause;

(b) the day on which, or the period during which, the breach occurred;

(c) a description of the personal information that is the subject of the breach;

(d) an estimate of the number of individuals in respect of whom the breach creates a real risk of significant harm;

(e) a description of the steps that the organization has taken to reduce the risk of harm to each affected individual resulting from the breach or to mitigate that harm;

(f) a description of the steps that the organization has taken or intends to take to notify each affected individual of the breach; and

(g) the name and contact information of a person who can answer, on behalf of the organization, OIPC's questions about the breach.

Bennett Jones

PIPEDA Breach Notification Regulations propose

- Notification to **individuals** must contain:

(a) a description of the circumstances of the breach;

(b) the day on which, or period during which, the breach occurred;

(c) a description of the personal information that is the subject of the breach;

(d) a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;

(e) a description of the steps that the affected individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm;

(f) a toll-free number or email address that the affected individual can use to obtain further information about the breach; and

(g) information about the organization's internal complaint process and about the affected individual's right, under the Act, to file a complaint with the Commissioner.

Bennett Jones

PIPEDA Breach Notification Regulations propose

- Direct notification of individuals
  - Email (if person has consented to those mode of communication)
  - Letter
  - Telephone
  - In person
- Indirect notification of individuals
  - Conspicuous message on website for at least 90 days, or advertisement likely to reach them
  - Possible if giving direct notification
    - Would cause further harm
    - Cost of giving direct notification is prohibitive
    - Organization does not have current contact information

Bennett Jones

PIPEDA Breach Notification Regulations propose

- Record keeping
- Organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred.
- Expect enhanced corporate obligation with record keeping requirement
  - Expect records to be sought out in inevitable litigation over the breach

Bennett Jones

PIPEDA Breach Notification

- Will come into force once final regulations are published

General Data Protection Regulation

EU takes data protection to a new level

Bennett Jones

EU GDPR

- EU member states currently comply with EU Data Protection Directive 95/46/EC
  - Some substantial differences from current Canadian law

- New General Data Protection Regulation to be implemented by EU member states May 25, 2018
  - New liabilities
  - New rights of individuals

Bennett Jones

Who does the GDPR apply to?

- GDPR applies to 'controllers' **and** 'processors'.
  - E.g. the controller says how and why personal data is processed
  - The processor acts on the controller's behalf
  - If currently under the current regime – likely subject to GDPR
- If you are a controller, you continue to have obligations for your processor
  - Additional obligations to ensure the processor complies with GDPR
- If you are a processor, the GDPR places specific legal obligations on you
  - E.g. you are required to maintain records of personal data and processing activities
  - You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

Bennett Jones

Who does the GDPR apply to?

- The GDPR applies to processing carried out by organizations operating within the EU.
- It also applies to organizations outside the EU that offer goods or services to EU citizens.
- The GDPR does not apply to
  - Processing covered by the Law Enforcement Directive,
  - Processing for national security purposes, or
  - Processing carried out by individuals purely for household or personal activities.

Bennett Jones

Who does the GDPR apply to?

- GDPR contains new provisions to enhance protection for children's personal data
- Where services are offered directly to a child, privacy notice must be written in a clear, plain way that a child can understand
- If you offer an online service targeting children you need to obtain consent from a parent or guardian to process the data
- Parent/guardian consent for access to online services required for children 16 or younger but counties can select lower ages so long as not below 13

- Note COPPA (U.S.) remains the most developed regime for the protection of children under 12

Bennett Jones

New rights of individuals

- The right to be informed
- The right of access
- The right of rectification
- ***The right to erasure***
- ***The right to restrict processing***
- ***The right to data portability***
- ***The right to object***
- ***Rights in relation to automated decision making and profiling***

Bennett Jones

New Rights

- The right to erasure is also known as ‘the right to be forgotten’.
  - The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.
  - The right is not absolute e.g. free speech
- Under existing EU law individuals have a right to ‘block’ or suppress processing of personal data. The restriction of processing under the GDPR is similar.
  - When processing is restricted, you are permitted to store the personal data, but not further process it.
  - You can retain just enough information about the individual to ensure that the restriction is respected in future.

Bennett Jones

New Rights

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
  - Can move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
  - Must save in structured, commonly used machine readable form.
- Right to object to direct marketing and profiling
- Right to object to processing for purposes of scientific, historical research and statistics
- GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
  - Assess if any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with GDPR.

Bennett Jones

Accountability & Governance

- New principle requires organization to demonstrate that you comply with the GDPR principles
- Compliance is organization's responsibility

- Must implement technical and organizational measures to demonstrate compliance
- Must maintain relevant document on data process activities
- Special record keeping requirements

Bennett Jones

Breach Notification

- The GDPR will introduce a duty on all organizations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.
- Must report where a breach where it is likely to result in a risk to the rights and freedoms of individuals.
  - E.g. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Bennett Jones

Data Transfer Restrictions

- The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organizations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

- Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organization ensures an adequate level of protection.

- Expect "Adequacy" hearings as occurred with PIPEDA

Bennett Jones

GDPR

- Europe is a much more privacy focused society than Canada
  - Value privacy more highly than security

- Time will tell how much of the new European rights or practices might influence Canada's privacy law as it develops

Bennett Jones

We have covered a lot of ground today

QUESTIONS?

Martin P.J. Kratz, QC
kratzm@bennettjones.com

Bennett Jones