Dentons 2017 Bootcamp

大成 DENTONS

Privacy and CASL

2017 Review and upcoming developments

Jawaid Panjwani
Karl Schober

November 2, 2017

Agenda

- **Privacy**
  - Preparing for Canada's upcoming data breach reporting requirements
  - Get ready for the regulator's new, stronger consent framework
- **CASL**
  - Private Right of Action – What Now?
  - Enforcement and Developments
    - Compu-Finder and Charter challenge

If time permits…

- CASL and the *Competition Act* – How your advertising is affected
- Ransomware

Privacy
Canada’s federal data breach requirements are around the corner

Notification, reporting and record-keeping obligations

- Recap
  - *Digital Privacy Act* (2015) – Established mandatory data breach reporting requirements to PIPEDA
  - Draft *Breach of Security Safeguards Regulations (2017) released*
  - If confirmed, expected to come into force early 2018

- The obligations under PIPEDA
  - Requirements based on a "real risk of significant harm" test
    - Notification to affected individuals
    - Report to the Office of the Privacy Commissioner of Canada
    - Notify any third party that the organization experiencing the breach believes is in a position to mitigate the risk of the harm
  - Maintain a record of all data breaches, regardless of "real risk of significant harm" and make these records available to the Privacy Commissioner upon request.

The (proposed) regulations – Risk of significant harm

- Assessment of “real risk of significant harm”
  - Guidance not regulation - No additional factors provided to assess risk.

- Factors that may be considered:
  - Sensitivity of personal information
  - Probability that personal information has been, or will be, misused
  - Malicious intent (e.g., malware and deliberate intrusions)
  - Length of time information potentially exposed
  - Whether information has been recovered
  - Vulnerability of victims (e.g., children)

- Alberta Breach Notification Decisions

The (proposed) regulations – Report to commissioner

- Data breach report to the Commissioner (content, form and manner)
  - Circumstances of the breach and, if known, the cause
    - Organizations not required to speculate
  - The day (or period) the breach occurred
  - Personal information that is the subject of the breach
  - Estimated number of individuals affected
  - Steps taken to reduce or mitigate harm
  - Steps taken (or that will be taken) to notify each affected individual; and
  - Contact person at the organization

- Minimum requirements – organizations may provide additional information if pertinent to Commission's understanding of the incident.

- Data breach reports can be submitted with best information available at the time. Organizations can update report at later date as information becomes available (promote timely reporting).

The (proposed) regulations – Notification to individuals

- Content of notification
  - Information about the breach (see Report to Commissioner)
  - Steps affected individual may take to reduce or mitigate harm
  - Toll-free number / email address to obtain more information about the breach; and
  - Information about organization's internal complaint process and individual's right to file complaint with Commissioner.

- Manner of notification – some flexibility
  - Direct notification
    - Email (or any other secure form of communication), letter, telephone or in-person.
    - Email: "if the affected individual has consented to receiving information from the organization in that manner"
  - Indirect notification
    - Website notice (90 days) or advertisement, but only if:
      - The giving of direct notification would cause further harm to the affected individual
      - The cost of giving direct notification is prohibitive to the organization
      - The organization does not have the contact information of the affected information (or it's out of date).

The (proposed) regulations – Notify third parties

- Determining which third-party organizations should be informed of a breach:
  - Could a third-party mitigate harm to the individual? i.e. credit monitoring agency

The (Proposed) regulations - records

- Scope and retention period for data breach record-keeping
  - **Retention Period:** Organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines the breach occurred (OPC had recommended 5 years).
  - **Scope:** Record must contain any information pertaining to the breach that enables the Commissioner to verify that the organization has reported to the Commissioner and notified affected individuals.

- No description of what constitutes a “record” – allows for broad interpretation; however, requires organizations to maintain sufficient information in a data breach record to demonstrate that they are tracking data security incidents.

The (proposed) regulations – Key take away

- No surprises
- Flexibility
  - The Regulations provide organizations with degree of flexibility to meet their statutory obligations.
- Harmonization
  - European Union (GDPR) and Alberta
  - Reduce compliance costs.
- Coming into force
  - Implementation window.

Privacy
OPC’s new, stronger contest framework

The OPC's new, stronger consent framework

Time to review and update those privacy policies

Obtaining meaningful/valid consent:

- Consent model overview (focus groups, consultations, submissions from legal, academic and business members)
- New draft Consent Guidelines shake up the standard privacy policy/statement
- Organizations must still provide complete disclosure of their privacy management practices, but must do more than a lengthy privacy document to ensure individuals understand what they are consenting to

Consent Guidelines – two new principles for organizations:

1. Emphasis on 4 key privacy elements
2. Layering and other individually-focused disclosure models

The OPC's new, stronger consent framework

1. Emphasizing 4 key elements

Organizations must disclose **4 key elements** to individuals in a clear and quick manner

1. The personal information being collected, and may be collected
2. Which third parties will receive the personal information
   - Enumerate the third parties that will receive the information
   - If not possible (too numerous to specify or changes too frequently), specify the type of third parties, and use layering
   - Third parties that use information for own purposes must be considered
3. Meaningful description of purposes
   - Describe clear purposes, vague terms such as "service improvements" should be avoided
   - Integral and non-integral purposes should be distinguished
4. Risk of harm
   - Clearly identify any known or foreseeable risk of harms that may result of information being collected, used or disclosed.

The OPC's new, stronger consent framework

2. Layering and other individually-focused disclosure models

- The struggle between obtaining valid consent and requirement to disclose an organizations privacy management practices
- Concern that standard privacy policies and terms can risk burying individuals with information
- Focus on individual's preferences
  - Provide options of how to get some or all information, and when
    - layers, just in time notices, consumer-friendly summaries, links to find out more
- Consider the business process
  - A paper application vs downloading an App

The OPC's new, stronger consent framework

- Be ready to demonstrate compliance
  - Draft Consent Guidelines highlight proactive queries should be expected
  - "Yes" or "No": Be prepared to explain why information collected is essential in providing product or service.
- How will you demonstrate you have obtained valid consent?
  - Pointing to a line buried in a privacy policy will not suffice
  - An internal review/audit of practices?
  - Check practices against new draft Consent Guidelines

A new OPC?

- Be ready for a proactive and aggressive OPC

"People are unlikely to file a complaint about something they do not know is happening, and in the age of big data and the Internet of Things, it is very difficult to know and understand what is happening to our personal information. My Office, however, is better positioned to examine these often opaque data flows and to make determinations as to their appropriateness under PIPEDA."

- OPC is not waiting for new powers
  - Complaints to the OPC will no longer be the primary tool and the OPC will be shifting itself as a proactive regulator ready to initiate investigations.

- Remember, your privacy policy is an advertisement to the OPC

CASL
Key developments

Private right of action – Suspended

- Originally scheduled to come into force on July 1, 2017

- Private Right of Action Suspended
  - June 7, 2017 – The Government of Canada announced that it was suspending the implementation of the private right of action in response to concerns raised by businesses, charities and non-profit sector.
  - Parliamentary committee is reviewing the legislation
    - Concerns about compliance – clarity required on how to comply (e.g., consent)
    - Possibility of class action suits – significant legal risks and uncertainty
    - Significant risk to daily operations.

Enforcement decision: CompuFinder (CRTC 2017-368)

- Details
  - Messages advertising educational and training services.
  - CEMs sent without consent and with unsubscribe mechanism that did not function.
  - 451 CEMs were initially identified in the investigation report. This was reduced to 317 CEMs after deficiencies found with respect to investigation report's summary tables.

- CRTC's determination
  - 317 CEMs sent without consent.
    - Messages not exempt on basis of "business-to-business" exemption.
    - CompuFinder failed to demonstrate implied consent under the "conspicuous publication exemption".
  - 87 CEMs contained a non-functioning unsubscribe mechanism.
  - CompuFinder did not take all reasonable steps to avoid violations and therefore did not establish a defence of due diligence.

- AMP
  - AMP of $1.1 million in notice of violation reduced to $200,000.
    - Number of CEMs at issue were reduced (30%).
    - Lower amount sufficient to promote CompuFinder's compliance.
    - Positive indications of self-correction.
    - CompuFinder has ability to pay, but doing so could place business at risk (bankruptcy proceedings).

Enforcement decision: Compu-Finder (CRTC 2017-368)

- Business-to-Business exemption (Establishing “Relationship”)
  - Contractual relationship with recipient organizations
    - Employee must have authority (and intent) to create a relationship on behalf of the organization.
    - Contractual relationship with one employee of an organization does not necessarily create contractual relationship with organization and a basis to send CEMs to other individuals employed by the same organization.
  - Correspondence with a business or its representatives
    - May create relationship under exemption depending on the content of the correspondence.
    - Message must also concern / refer to the activities of the organization to which the message is sent.

- Implied consent – Conspicuous publication
  - Not broad licence to contact any electronic address found online
  - Online directories
    - Conspicuous publication requires that the person to whom the message is sent publish, or cause to be published, the address in question in a directory (not a third-party on its own initiative)
    - No implied consent where terms of use of directory prohibits sending of unsolicited CEMs to addresses in the directory.

- Demonstration of due diligence
  - Onus on violator to demonstrate it was duly diligent – requires showing that it took all reasonable steps to avoid the violations in question (prevention and mitigation).
    - Routine practices, written policies, auditing mechanisms and monitoring compliance with CASL
  - Measures taken after violations committed not relevant to a potential due diligence defence.

CASL: Constitutional challenge by CompuFinder

CRTC Decision 2017-367

CompuFinder argued that CASL:

- was not validly enacted as it is not *intra vires* the federal Parliament's (Parliament) legislative powers under the *Constitution Act, 1867*.
- violates the freedom of expression guaranteed to CompuFinder by section 2(*b*) of the Charter.
- violates any of the rights of CompuFinder protected by section 11 of the Charter.
- violates the section 7 Charter protection against self-incrimination or the section 8 Charter right against unreasonable search and seizure

CASL: Constitutional challenge by CompuFinder

Provisions argued as unconstitutional

- subsection 1(1) – the definition of "commercial activity";
- subsection 1(2) – the meaning of "commercial electronic message" (CEM);
- subsection 1(3) – clarification of other electronic messages that will be considered CEMs;
- section 3 – the purpose of the Act;
- subsections 6(1), 6(5), and 6(6), as well as section 12 – provisions related to unsolicited CEM prohibitions;
- subsections 10(1), 10(9), 10(10), and 10(13) – provisions related to express consent and implied consent, including the definitions of "existing business relationship" and "existing non-business relationship";
- section 17 – notices to produce;
- sections 20, 22, and 25 – provisions related to notices of violation and AMPs;
- section 30 – clarification that a violation of CASL is not an offence;
- sections 31 and 32 – extension of liability provisions;
- the *Electronic Commerce Protection Regulations (CRTC)*, SOR/2012-36 (the CRTC regulations); and
- the *Electronic Commerce Protection Regulations*, SOR/2013-221 (the Governor in Council regulations).

CASL: Constitutional challenge by CompuFinder

Does CASL violate 2(b) - freedom of expression

- CompuFinder
  - Commercial expression of corporations is protected
  - sending of a wide range of unsolicited commercial electronic messages falls within scope
  - Section 6 of CASL (prohibiting sending unsolicited CEMs) restricts the right
- AG
  - Concedes with CompuFinder
  - But the infringement is justified

CASL: Constitutional challenge by CompuFinder

Is the violation justified under section 1?

- AG must demonstrate that:
  I. The limit on the right or freedom is prescribed by law
  II. The legislative goal is pressing and substantial
  III. A rational connection between the limit and CASL's objectives exists
  IV. The impairment of the right or freedom is minimal, and
  V. There is an overall proportionality between the salutary deleterious effects of the limiting measure

CASL: Constitutional challenge by CompuFinder

I. Is limit prescribed by law?

- CompuFinder
  - Vagueness
    - “commercial electronic message”, “electronic address”, “implied consent” , “existing business relationship” and exceptions under CASL
  - Too broad
  - No guidance to assess secondary or ancillary commercial purposes
  - Fails to adequately identify risk zones
  - Subsequent guidance by CRTC suggests lack of clarity

- AG
  - Some terms may be broad but sufficiently intelligible
  - No requirement that CASL provide enough guidance to predict, with certainty, the specific consequences of conduct
  - Subsequent guidance is part of duty to administrate

Commission

- *Simply put, if someone sends an electronic message to an electronic address and that message is of a commercial character, there is a strong possibility that the message is a CEM and may be subject to CASL*.

CASL: Constitutional challenge by CompuFinder

II. Are CASL's objectives pressing and substantial?

- CompuFinder
  - CASL's goals too broad to meet standard
  - Stats of SPAM pre-dated CASL coming into force
  - Filters are successful at addressing SPAM
- AG
  - SPAM is costly to e-commerce
  - SPAM undermines trust and confidence in online business activities
  - SPAM increases risk of viruses, etc.
- Commission
  - Agrees with AG
  - Stats and large number of complaints suggest CASL is necessary

CASL: Constitutional challenge by CompuFinder

III. Is the limit rationally connected to CASL's objective?

- CompuFinder
  - CASL fails to target the commercial activity CASL is meant to discourage
  - CASL fails to address harmful SPAM from outside Canada
- AG
  - Opt-in model keeps users from opening threatening and harmful email
  - Keeps costs with sender and not recipient
- Commission
  - Agrees with AG
  - Limits imposed in sending CEMs reasonable to prohibit unsolicited CEMs and minimize adverse effects on Canadian businesses.

CASL: Constitutional challenge by CompuFinder

IV. Is the impairment minimal?

- CompuFinder
  - "maximally impairing" due to opt-in model except in limited exceptions
  - Scope extends beyond CASL's purpose
  - U.S. and Australian models effective and impair less
  - Exemptions and exclusions are vague, narrow or both
- AG
  - Complex regulatory solution to a pressing social problem
  - Future, potential exceptions = flexibility
  - Opt-out models are less effective
- Commission
  - Several, less restrictive, reasonable alternatives exist, but not convinced would have equal effect to meet goals of CASL

CASL: Constitutional challenge by CompuFinder

V. Proportionality between salutary and deleterious effects of the limiting measure?

- CompuFinder
  - Problem is primarily linked to harmful, threatening emails, yet:
    - Significant cost to Canadian businesses
    - Chilling effect to Canadian businesses
- AG
  - Consent to send CEMs, identification and unsubscribe are minor limits on freedom
- Commission
  - This type of commercial expression falls outside the core values of freedom of expression
  - Effects to freedom do not outweigh benefits to the greater public good

CASL: Constitutional challenge by CompuFinder

Does CASL violate section 11 – Rights relating to criminal proceedings

- CompuFinder
  - CASL imposes penal consequences without constitutional protections
  - Denied fair, independent hearing
  - No presumption of innocence
- AG
  - CASL is regulatory, not criminal
  - Maximum penalties are to encourage compliance
  - Different language than *Criminal Code*
- **Commission**
  - CASL is an administrative, regulatory regime, not penal
  - $10 million AMP is only an upper limit, and high AMP's do not equal penal
  - List of factors must be taken into account
- Further, no violation of sections 7 or 8 of Charter

Enforcement decision : William Rapanos (CRTC 2017-65)

- Details
  - 58 CEMs advertising flyer design and printing.
  - Notice of violation: 10 violations; AMP of $15,000.
  - Mr. Rapanos claimed he was victim of personal vendetta or identity theft and that CRTC was unable to confirm that he registered the website that sent CEMs.
  - CRTC: Mr. Rapanos failed to provide any evidence of fraud or identity theft and did not demonstrate that he was not the owner of the website.
  - AMP amount was not lowered. Self-correction unlikely.

- Lessons
  - The CRTC will go after the “little guy”.
  - Broad use production power to obtain information.
  - The purpose of AMPs is to promote compliance and not to punish. If CRTC determines that the violator is unlikely to “self-correct”, it is unlikely to reduce the amount of the AMP.
  - Important to co-operate with a CRTC investigation in order to potentially reduce AMP.
  - Violators must provide financial documentation to prove inability to pay.

Undertaking: Couch Commerce, TCC and Mr. Halazon

- Details
  - CEMs sent by Couch Commerce to recipients without compliant unsubscribe mechanism
  - AMP: $10,000 (paid by Mr. Halazon)

- Compliance program
  - Transformational Capital Corp (TCC), which acquired the email list used by Couch Commerce, agreed on compliance program with the following elements:
    - Review of current practices;
    - Development and implementation of corporate compliance policies and procedures;
    - Training for employees;
    - Consistent disciplinary procedures; and
    - Tracking of CEM complaints and subsequent resolution, monitoring and auditing;
  - Compliance program also includes reporting mechanisms to Commission staff.

Warning letter, undertaking or a notice of violation does not close an investigation. CRTC will follow-up to ensure compliance is achieved by monitoring violators' activities and checking their compliance programs.

CASL

Representations under the *Competition Act*

CASL and the *Competition Act*

False or misleading representation provisions

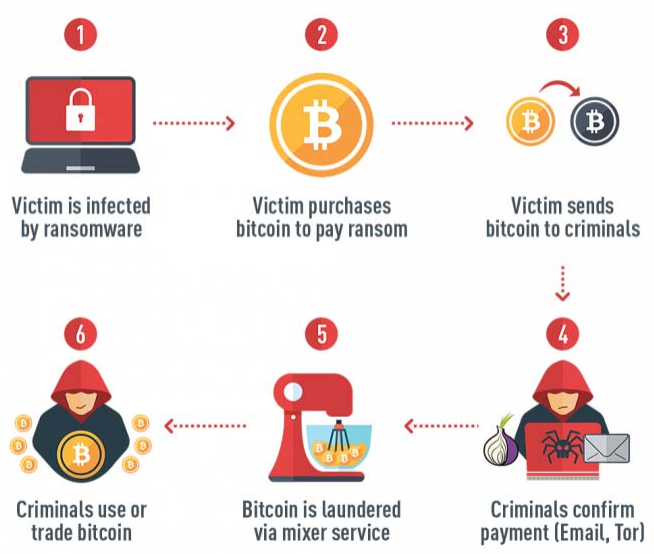
- Purpose is aimed to address disguised spammers and harmful links
- Applies to any representation in CEM
- Check all representations are not at risk of being false or misleading:
  1. Sender information
  2. Subject matter
  3. Content of CEM
  4. Locator (URL or metadata)

- Good
  - "*Our Fall offers waiting inside for you*"
- Bad
  - **Subject line:** "All inclusive Cuba package for $400.00"
  - **Content:** "With purchase of $500 roundtrip flight. Total package $900".
- Bad
  - CEM is co-sent by two companies, but information of only one is included.

Ransomware

What is Ransomware?

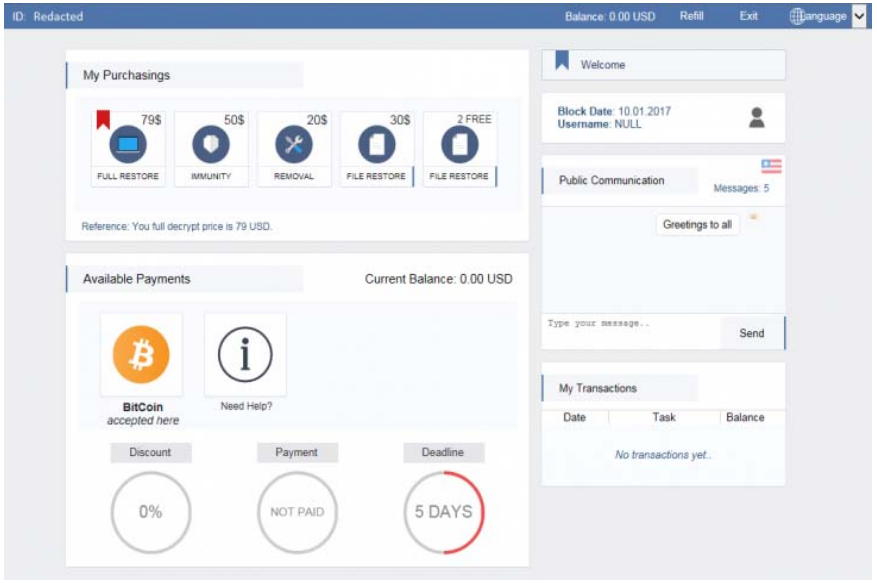
- Ransomware is malicious software that disables the functionality of a computer system in some manner until a “ransom” is paid by the victim.
  - Locker ransomware: locks or denies access to a computer or device.
  - Crypto ransomware: file and data locker that encrypts end-user data and files.
- Methods of Infection
  - Malicious email attachments and links
  - Drive-by downloads (visit compromised website with malicious code)
  - Remote Desktop Protocol attacks (i.e., hacking)
- Impact
  - Loss of sensitive or proprietary information
  - Financial loss / harm to reputation
  - Disruption of operations
- Examples: WannaCry, NotPetya, Bad Rabbit
  - Exploits (EternalBlue)



Response to Ransomware

- Canadian Cyber Incident Response Centre (CCIRC) strongly discourages paying the ransom
  - No guarantee data will be decrypted after payment
  - Promotes further criminal activity
  - Decryption does not remove malware
- Prevention
  - Back-up data
  - Update software /address vulnerabilities
  - Employee training
  - Incident response and recovery plan
- Legal considerations
  - Privacy law security standards
  - Data breach reporting and notification obligations
  - Director and officer liability
  - Risk of litigation.

Spora Ransomware Payment Interface



Thank you

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