Privacy Law

Privacy Law Matters

This is the first newsletter of a series entitled "Privacy Law Matters" which will provide updates on recent developments in privacy legislation and case law. This newsletter will provide an update on the enforcement of *Canada's Anti-Spam Legislation* ("CASL"), a brief summary of the new *Digital Privacy Act* ("DPA") and an update on the *Personal Health and Information Protection Act* ("PHIPA").

CASL Enforcement

In the past two years, the Canadian Radio-television and Telecommunications Commission (the "CRTC") has released the following four decisions which provide some insight into the application and enforcement of CASL.

1. *Porter Airlines*

The CRTC investigated Porter Airlines for allegations that commercial electronic messages ("CEMs") from Porter did not contain an unsubscribe mechanism or did not clearly set out the unsubscribe mechanism and Porter failed to honour unsubscribe requests within ten (10) days. Porter immediately took steps to change its practices and was cooperative throughout the investigation. Porter Airlines agreed to enter into an undertaking to resolve the matter in which it agreed to pay a fine of **$150,000** and to make amendments to its compliance program and policies. The CRTC also reminded organizations that proof of consent is required for each electronic address. General business practice or policies are not sufficient as proof of consent.

2. *Compu-Finder*

Compu-Finder was given a penalty of **$1.1 million** for sending CEMs without consent, CEMs containing an unsubscribe mechanism that did not function properly, and CEMs containing an unsubscribe mechanism that was not valid for 60 days, and failing to respond to unsubscribe requests within 10 days. Numerous complaints were filed with the CRTC against Compu-Finder. The CRTC found that Compu-Finder failed to follow CRTC guidelines once released and continued to violate basic principles of privacy law. In contrast to *Porter Airlines*, Compu-Finder was not very cooperative during the investigation or in amending its policies to demonstrate compliance.

Compu-Finder was also recently investigated for violations of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") for sending large volumes of emails to individuals without consent. Compu-Finder obtained the email addresses through telemarketing, sign-up forms and business listings and websites without advising the individuals of the purpose for which their email addresses were being collected. Compu-Finder tried to rely on the consent provisions under CASL, including the consent exemption for "business to business" communications; however, the Privacy Commissioner rejected this argument on the basis that compliance with CASL is irrelevant to the determination of whether there is compliance with PIPEDA.

3. *PlentyofFish*

PlentyofFish faced similar allegations but was given a much lower penalty of **$48,000** after it agreed to enter into an undertaking to change its practices. PlentyofFish was investigated for allegedly sending commercial emails to registered users with an unsubscribe mechanism that was not clearly set out and could not readily be performed. The emails notified users of the services offered by PlentyofFish. One of the factors that the CRTC took into account was PlentyofFish's actions in immediately updating its unsubscribe mechanism when notified of the complaints filed by Canadians. In a press release, the CRTC made the following comments:

> "This case is an important reminder to businesses that they need to review their unsubscribe mechanisms to ensure they are clearly and prominently set out and can be readily performed," said Manon Bombardier, the CRTC's chief compliance and enforcement officer, in the release."

"We appreciate that Plentyoffish Media changed its practices once it became aware of the problem."

PlentyofFish demonstrated an appreciation of CASL and efforts to become compliant which resulted in a lower penalty.

4. *Kellogg Canada Inc.*

More recently, on September 1, 2016, the CRTC announced that Kellogg Canada Inc. ("Kellog") has agreed to pay a penalty of **$60,000** as part of an undertaking regarding alleged CEMs sent by Kellogg and/or its third party service providers to recipients without consent. Kellogg also agreed to update and implement its compliance program which will include guidelines for the review and revisions of existing written policies and procedures, training programs for employees, tracking complaints with respect to CEMs and resolution and implementing auditing mechanisms to assess compliance. Kellog will also ensure that its third party service providers will comply with CASL.

Summary

When determining whether a penalty should be imposed and how much the penalty should be, the CRTC will consider:

- the nature of the violation;
- the company's history with CASL;
- whether the company benefited financially from the violation; and
- the company's ability to pay a penalty.

As demonstrated in the above noted cases, where an organization provides an undertaking to resolve the matter and shows it has made changes to its practices to become compliant with CASL, the fines are lower. On the other hand, if there is a flagrant violation of CASL and disregard for its guidelines, the fine will be higher.

It is also important to keep in mind the potential liability of directors, officers or agents of a corporation if they direct, authorize, assent to or acquiescence in or participate in the commission of a violation. The maximum monetary penalty for a CASL violation is $10,000,000 per violation. This makes it imperative for directors and officers of corporations to ensure management and/or other employees maintain an effective CASL compliance program and maintain records of all documents or information with respect to CASL compliance. If the CRTC issues a Notice to Produce requiring the corporation to prove valid consent or compliance with CASL, the necessary documents and information should be readily available.

To ensure their CASL compliance programs are effective, organizations should carefully review and revise written policies and procedures regarding compliance, implement ongoing training programs for employees, implement updated monitoring and auditing mechanisms to assess compliance, and diligently respond to all CEM complaints with the aim of resolution.

If you do not have a compliance program in place, the CRTC has published guidelines to assist businesses in doing so: Information Bulletin CRTC 2014-326.

Digital Privacy Act

The DPA came into effect on June 18, 2015. It was enacted permanently as an amendment to PIPEDA made in order to regulate cyber security and data protection.

A) Reporting Breaches

Organizations may now be required to notify affected individuals and the Privacy Commissioner of privacy breaches of security safeguards. "Breach of security safeguards" is defined in PIPEDA and generally includes what is commonly known as a data breach. This aspect of the DPA is not in force yet.

In what circumstances must an organization report a breach? Do all breaches need to be reported?

Not all privacy breaches need to be reported. An organization must report a breach if it is reasonable to believe the breach creates a "real risk of significant harm to the individual." Significant harm includes bodily harm, humiliation, damage to reputations, relationships, loss of employment, business opportunities financial loss or identity theft. When determining whether there is a "real risk" the following factors will be taken into account:

- sensitivity of information;
- probability the information has been, is being or will be misused; and,
- any other prescribed factor.

Organizations must also keep a record of all breaches involving personal information and provide a copy to the Privacy Commissioner upon request. A failure to do so can result in a fine of up to $100,000.

When must the organization report the breach?

The breach must be reported "as soon as feasible." It is not entirely clear what is meant by this phrase, and there is no guidance in the legislation with respect to the interpretation of this phrase. It is likely that future case law will provide clarity to organizations on the reporting timelines.

Public Interest Disclosure

The Privacy Commissioner has the power to make public any information that comes to his/her knowledge in the performance of his/her duties under the DPA, if he/she deems

that doing so is in the public interest. This language in the DPA has widened the discretion previously given to the Privacy Commissioner which only applied to information "relating to the personal information management practices of an organization."

B) Sliding Scale of Consent

There is now a sliding scale when assessing whether an individual provided consent to the release of his/her personal information. Consent is now based on the sophistication of individuals. Where the individual is vulnerable (for example, a minor or a senior), organizations will be held to a higher standard and as such, should implement policies and procedures to ensure that vulnerable and less sophisticated individuals have provided informed consent. To ensure they are in compliance with the DPA, some organizations may need to differentiate policies for specific demographics.

The DPA also provides a number of new exceptions to consent, including:

- for the purposes of investigations/fraud detection;
- business transactions as defined in the DPA, including the sale of a business, a merger or the lease of a company's assets, only if it is necessary to decide whether to proceed with or complete the transaction;
- witness statements in insurance claims where necessary to assess, process or settle an insurance claim;
- to identify injured, ill or deceased persons and notify a government institution, next of kin or authorized representative. If the individual is alive, he/she must be notified in writing of the disclosure;
- if there are reasonable grounds to believe an individual "has been , is or may be the victim of financial abuse;
- to establish, manage or terminate an employment relationship in a federally regulated workplace; and
- personal information produced in the course of employment, business or profession, as long as the collection, use or disclosure is consistent with the purpose for which the information was produced.

C) Impact on Organizations?

These requirements of the DPA create new costs, challenges and risks for organizations. The DPA will likely result in more enforcement actions taken against organizations. The risk of litigation and class actions has also increased as a result of the DPA. Organizations must ensure that they have internal safeguards in place to comply with the DPA or risk being fined. To ensure a record of all privacy breaches is kept and maintained, some organizations may need to make changes to the policies in place for their IT groups. With an amorphous standard of determining whether there is a breach, it will become increasingly difficult for organizations to prove they have met the standard for security safeguards.

Amendments to the Personal Health and Information Protection Act

Bill 119 was introduced on September 16, 2015, received Royal Assent on May 16, 2016, and will come into force on a date to be proclaimed. The Bill provides for the following amendments to the PHIPA:

- The definition of "use" is amended to include the "viewing" of personal health information;
- Mandatory reporting to the Privacy Commissioner of specific privacy breaches;
- Mandatory reporting to health regulatory colleges in certain circumstances;
- Notice to patients regarding the breach at the first reasonable opportunity where the information is stolen, lost, used or disclosed without authorization. The notice must include a statement that the individual is entitled to make a complaint to the Privacy Commissioner;
- Increased fines – the fines will be doubled from $50,000 to $100,000 for individuals and from $250,000 to $500,000 for organizations;
- A new section has been added to facilitate the privacy framework for an "Electronic Health Record"; and
- Removal of the requirement that prosecution offences under PHIPA be commenced within six months of when the alleged offence occurred.

What does this mean for you?

Health information custodians must familiarize themselves with the new compliance requirements and implement measures to ensure compliance with the PHIPA. Compliance measures that organizations can take include implementing policies and practices to ensure privacy breach notification requirements are met, reviewing and auditing their agents to ensure compliance, and ensuring personal health information is not collected, disclosed or used without authority whether through the Electronic Health Record or otherwise. Health information custodians should review the amendments to ensure that the Information and Privacy Commissioner, individuals and patients are notified of privacy breaches when required and ensure that the notifications include the required information.

Pallett Valo Privacy Law Practice

Privacy and data protection are very important considerations for both private and public sector organizations. At Pallett Valo LLP, our Privacy Law Group advises and supports private sector organizations to comply with their obligations under both federal and provincial laws including the: *Personal Information Protection and Electronic Documents Act* (PIPEDA), *Personal Health Information Protection Act, Freedom of Information and Protection of Privacy Act, Municipal Freedom of Information and Protection of Privacy Act, Canadian Anti-Spam Legislation* (CASL) and the *Digital Privacy Act*. We assist our clients in developing privacy policies and practices to meet strategic business needs and to ensure compliance with privacy legislation.

Pallett Valo lawyers have extensive experience in advising clients on compliance matters, negotiating, drafting and advising on privacy aspects of corporate transactions and helping clients navigate new and evolving legislation such as the *Digital Privacy Act* which focuses on cyber security and date protection.

Pallett Valo's Privacy Group provides advice on both transactional and day-to-day compliance matters for small and large organizations in a number of different industries including manufacturers, distributors, property management, data collection and technology. We provide timely, collaborative and cost effective legal services and consulting services to ensure our clients become and remain compliant with privacy laws in Canada.

Areas of Practice Include:

- Developing and implementing compliance strategies and plans
- Drafting and negotiating contractual protections with respect to data protection, privacy policies and the use of personal information and confidentiality
- Review of marketing and promotional material to identify privacy issues
- Application of Canadian privacy law to companies based in other jurisdictions
- Customized privacy questionnaires and audits
- Reviewing and recommending changes to your organization's existing policies, forms and contractual arrangements
- Educational training and seminars for senior management, board of directors or staff
- Legal representation during third party privacy audits or complaint hearings
- Ongoing advising on the collection, use, disclosure and retention of personal information
- Privacy issues in employment

Contact Members of our Privacy Law Practice:

Andy Balaura
abalaura@pallettvalo.com • (905) 273.3022 ext. 225

Manpreet Brar
mbrar@pallettvalo.com • (905) 273.3022 ext. 214

Joe Conte
jconte@pallettvalo.com • (905) 273.3022 ext. 217

Annette Pereira
apereira@pallettvalo.com • (905) 273.3022 ext. 241

PALLETT VALO LLP
Lawyers & Trade-Mark Agents