DOLDEN WALLACE FOLICK LLP

CYBER RISK: CURRENT LANDSCAPE OF PERSONAL INFORMATION AND PRIVACY LIABILITY IN CANADA

Jill M. Shore & Sinziana M. Gutiu

May 2016

18th Floor – 609 Granville St.
Vancouver, BC
Canada, V7Y 1G5
Tel: 604.689.3222
Fax: 604.689.3777

308 – 3330 Richter Street
Kelowna, BC
Canada, V1W 4V5
Tel: 1.855.980.5580
Fax: 604.689.3777

850 – 355 4th Avenue SW
Calgary, AB
Canada, T2P 0J1
Tel: 1.587.480.4000
Fax: 1.587.475.2083

500 – 18 King Street East
Toronto, ON
Canada, M5C 1C4
Tel: 1.416.360.8331
Fax: 1.416.360.0146

ABSTRACT: *In the last five years, Canada has experienced increased litigation involving data breaches. Confidential personal and corporate information is at risk from a variety of threats ranging from the exploitation of big data to administrative error, workers' misconduct and criminal hackers. Affected individuals have a number of common law and statutory tools available to seek compensation in court following a breach. In order to minimize their potential exposure, organizations must become knowledgeable about the field of cyber liability, take precautionary actions to prevent breaches, and if data breaches occur, know how to appropriately mitigate the consequences through identification, containment, notification and documentation.*

The Growing Need for Client Data Protection

Data breaches in the news are becoming strikingly frequent, and the legal and financial risk to organizations that collect, store and use personal data is increasing. Canada is seeing more data breach cases being brought before the courts, creative litigation strategies being tested, and legislative amendments to privacy laws being developed.

According to a 2015 study by the Ponemon Institute LLC and IBM, lost or stolen records could cost a Canadian organization an average of $5.32 million, and an average cost per record of $250.[1] In a speech at the AAMGA on May 28, 2015, John Nelson, Lloyd's Chairman, stated that there was an increase in the cyber insurance premium global market from $850 million in 2012 to an estimated $2.5 billion in 2015, and that much of this increase occurred in the USA. A report by PWC predicted that the cyber liability market could grow to $5 billion in annual premiums by 2018 and at least $7.5 billion by 2020.[2]

Comprehensive protections for personal information are no longer an optional practice. The likelihood of a breach, potential exposure to financial loss, and possibility of legal action has become an impending reality for the average Canadian business.

Types of Client Data Breaches in Canada

Over the last five years, data breaches in Canada have generally occurred as a result of one or more of the following causes: exploitation of big data and corporate profiteering, administrative error, workers' misconduct and criminal hacking.

The exploitation of big data and corporate profiteering refers to companies that collect large amounts of personal information from their clients or third parties and use or disclose it for a profit without the prior valid consent of these individuals. Lawsuits flowing from these types of cases are typically brought as class actions.

[1] Ponemon Institute and IBM, "2015 Cost of Data Breach Study: Canada", May 2015, at p.1.
[2] PwC, "Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience", 2015 at p. 10.

Often, data breach cases arise as a result of an administrative error. An organization may disclose personal or sensitive information by accidentally sending it to the wrong address, misplacing it, or losing it. Depending on the type of administrative error, resulting lawsuits may give rise to individual claims or class actions.

Workers' misconduct cases occur when employees, former employees or contractors take or access the personal or sensitive data of colleagues, customers, or other third parties without authorization, for their own private use or profit, which may or may not involve criminal intent. Litigation flowing from workers' misconduct cases usually includes claims against the employee, as well as claims for vicarious liability against the employer for the conduct of that employee.

Cyber breaches resulting from criminal hacking (which includes phishing, ransomware etc.) occur when third parties breach an organization's computers or network and use the information illegally obtained to gain a profit, send a moral message to the organization or public, or generally cause a disruption to the affected organization or individuals. These types of cases often involve criminal conduct and make it more likely that fraud, identity theft or property damage will occur, which can result in higher damages.

A challenge for class actions that seek more than nominal damages is proving pecuniary or quantifiable damages if no fraud or identity theft has occurred. To overcome this hurdle, plaintiffs may claim waiver of tort or unjust enrichment, in an attempt to have damages assessed based on the gross revenue or net income received or saved by the organization as a result of its wrongful acts, rather than by the loss sustained by the plaintiffs. [3] Punitive damages also play an important role as the focus shifts from the harm suffered by the plaintiffs to the wrongful conduct of the organization.

Statutory Causes of Action that Protect Client Data

There are three different types of statutes in Canada that may provide a legal remedy to victims of a data breach: personal (and health) information protection statutes such as the federal *Personal Information Protection and Electronic Documents Act* SC 2000, c. 5 ("PIPEDA") and provincial laws deemed to be substantially similar; provincial Privacy Acts that provide a statutory right of action for breach of privacy in certain provinces; and starting July 1, 2017, a right to sue for damages under the federal *Canadian Anti-Spam Legislation*[4], SC 2010, c. 23 ("CASL").

[3] For an example of a case where waiver of tort was claimed, see *Tocco v. Bell Mobility* (Ontario Court, 2013).
[4] Although this act is referred to as the *Canadian Anti-Spam Law*, it's legislated title is "*An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c. 23.

PIPEDA regulates the collection, use and disclosure of personal information by private organizations without consent. After an investigation by the Office of the Privacy Commissioner of Canada has concluded, affected individuals may sue in Federal Court for damages. Generally, PIPEDA applies across Canada, unless a province has enacted legislation deemed to be substantially similar to PIPEDA. To date, only British Columbia, Alberta, and Quebec have substantially similar legislation applicable to the private sector at large, and Ontario, Newfoundland and Labrador, and New Brunswick have enacted substantially similar legislation applicable to health information. Separate information protection legislation applies to personal (and health) information held by federal and provincial governments and other public bodies.

PIPEDA was recently amended by the *Digital Privacy Act*, SC 2015, c. 32 ("DPA"), which received royal assent on June 18, 2015. The DPA requires organizations to notify, as soon as possible following a data breach, the federal Privacy Commissioner, all affected individuals, and any third parties that could mitigate the loss. Notification obligations are triggered when there is a "breach of security safeguards" that could reasonably create a "real risk" of "significant harm" to an individual. Other notable amendments include a requirement that organizations keep a record or security breach log of any and all data breaches involving personal information, and new fines and penalties up to $100,000 if an organization knowingly fails to report a data breach or fails to keep a security breach log.

British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador have enacted Privacy Acts, which provide another legislated means for plaintiffs to seek damages. The Privacy Acts create a separate statutory cause of action premised upon a breach of a right to privacy, which is not restricted to the protection of personal information. The provincial statutory claims for privacy breach require that the act leading to the breach of privacy be intentional. Proof of economic loss or other specific harm is not a pre-requisite for liability or damages.

CASL is a statute that regulates electronic communications for commercial purposes (i.e., by way of text, email, or photos). It also prohibits a wide range of commercial electronic activity including the alteration of transmission data in an electronic communication, the installation of computer programs without consent, the use of false or misleading statement online to promote a business interest or product, the collection of an electronic address obtained by way of computerized data mining, and the collection of personal information obtained from a computer system by way of a violation of Federal law, unless narrow exceptions apply. A person who breaches the statute faces potential regulatory investigation and significant "administrative monetary penalties". Starting July 1, 2017, new sections of CASL will come into force, which will create a statutory cause of action that will allow individuals affected by a violation of CASL to sue in court for compensation.

Common Law Causes of Action that Protect Client Data

Common law causes of action provide another means for individuals to seek compensation after a data breach. Outside of the Province of British Columbia[5], the tort of intrusion upon seclusion may apply. This tort, recognized by the Ontario Court of Appeal in *Jones v. Tsige* in 2012, provides a common law cause of action that permits a plaintiff to recover up to $20,000 in damages without having to demonstrate that any pecuniary loss was incurred. Liability arises only where the invasion of privacy is intentional or reckless, lacks legal justification, and would be considered offensive to the reasonable person.

The tort of public disclosure of private facts,[6] was applied in the privacy context in *Jane Doe 464533 v. D.*, a 2016 Ontario "revenge porn" case. This tort may provide a remedy where a public disclosure of a private fact has occurred, the act of the publication is highly offensive to a reasonable person, and the matter is of no legitimate concern to the public. In the *Jane Doe* case, the court awarded much higher non-pecuniary damages despite the cap set in *Jones v. Tsige* for non-pecuniary losses, due to the sensitive subject matter and psychological effects on the plaintiff.

In addition to these specific privacy related torts, individuals affected by a data breach may have valid legal claims arising from a breach of contract, negligence, breach of confidence, breach of fiduciary duty, or breach of trust on the part of the holder of the data. Claims in Canada have also been advanced alleging the tort of conversion and breach of bailment law. With respect to all of these various causes of action, if the data breach arose as a result of an employee's wrongful act a plaintiff may be able to hold the employer organization vicariously liable.[7]

Case Studies

Tucci v. People's Trust Company is a case that involves cybercriminals from the People's Republic of China who compromised the customer database of People's Trust Company ("PTC"). The case illustrates the progress of a claim from the investigation stage at the Office of the Privacy Commissioner to a class action in court. The certification of this class action was scheduled to be heard in April 2016 in British Columbia.

PTC received complaints that its clients and individuals who had completed online applications for PTC services had received phishing messages asking them to disclose

[5] In British Columbia, the courts have determined that the tort does not exist because a breach of privacy is already actionable under the British Columbia *Privacy Act*, RSBC 1996 c. 373. See *Demcak v. Vo* (BC Supreme Court, 2012), and *Ari v. ICBC*, (BC Court of Appeal, 2015).

[6] Sometimes referred to as publicity given to private life. This tort is sometimes referred to as the tort of publicity given to private life. See *Shore v. Avid Dating Life Inc. and Avid Life Media Inc.* (Ontario and Quebec Courts, 2015), and *John Doe v. Canada* (Federal Court, 2015; Federal Court of Appeal decision pending).

[7] See for example *Evans v. Bank of Nova Scotia*, (Ontario Court, 2014).

personal information including names, addresses, telephone numbers, email addresses, dates of birth, social insurance numbers and financial information. PTC retained a forensic investigator who identified the nature of the problem and extent of the data breach. PTC immediately notified the federal Office of the Privacy Commissioner, but waited about 14 days to notify affected individuals. In April 2015, the Office of the Privacy Commissioner determined that PTC did not implement adequate technological and organizational safeguards to protect the personal information of its customers.

The class action against PTC claims breach of PTC's terms of use and privacy policy, negligence in failing to keep customer information secure, breach of confidence, and intrusion upon seclusion, and relies upon the Privacy Commissioner's findings. The damages claimed are for time wasted, inconvenience, damage to credit reputation, mental distress and preventative expenses. The plaintiffs plead waiver of tort and unjust enrichment, and seek to assess damages in an amount equal to the gross revenue received by PTC, or alternatively, the net income received by PTC as a result of the fees, interest, and service charges generated on products or services it provided to the plaintiffs.

An example of a case that involved the loss of electronic property is *Belley v. TD Auto Finance Services*, a Quebec class action certified in 2015. UPS lost an unencrypted tape sent by corporate affiliates of TD Auto Finance Services ("TDAF"), which contained personal information of approximately 240,000 customers. Some of the customer information was fraudulently used by unknown third parties to purchase vehicles causing pecuniary loss to the individuals affected. The court permitted the claims in negligence against TDAF for the actions they took leading to the breach and in response to the breach. The plaintiffs plead that statements made by TDAF in their notice to customers as evidence of admissions made by TDAF that it lost the tape, was aware damages would occur to its customers as a result of the loss, and failed to adequately protect customer data.

The court also certified the plaintiffs' claim for punitive damages as a result of TDAF's failure to encrypt data, failure to inform UPS of the tape's contents, assigning a total $5 value to the tape, delaying and incompletely notifying its customers, and failing to offer any compensation to affected individuals.

Actions Organizations Can Take to Minimize the Cost of a Data Breach

Although a data breach can be extremely costly to an organization of any size, the impact of the breach can be minimized by adopting mitigation strategies early in the process. The 2015 Ponemon data breach study found certain factors can reduce the per capita cost of data breach, including having cyber liability insurance, robust incident response plans and a strong incident response team, extensive use of encryption,

employee training programs, board-level involvement, privacy officer appointments, and business continuity management.[8]

Following a breach, an organization needs to take immediate action to identify, contain, and document the breach, and notify appropriate parties, which may include law enforcement, Privacy Commissioners, and/or affected individuals. Identifying the nature and extent of the data loss, as well as containing the breach and securing the organization's networks to prevent any further loss or unauthorized access should be a top priority. In most cases, organizations should immediately contact a forensic technological support service provider to help identify the cause and scope of the breach, including the nature of the data affected, secure the organization's networks and data from further loss or intrusion (which will help minimize reputational losses and business interruption claims), and preserve electronic evidence to prove what happened and how.

Prompt identification of the cause and containment of the breach may also affect the insured's legal obligations and defences. Due diligence is a defence in proceedings before a Privacy Commissioner, and may also be a defence to any ensuing lawsuits. In other cases, the cause of the breach may confer recovery rights against other parties, such as an internet provider or computer services firm that failed to provide or maintain appropriate security measures. Organizations may need legal advice to identify which jurisdiction's laws may be triggered and what is required to comply with them, and to ensure that the organization's interests are being protected with a view to defending against any ensuing litigation or regulatory investigation.

Given the risk of litigation flowing from a data breach, and the potential for regulatory investigation, legal counsel should be retained immediately to assist with investigations, evidence preservation, documentation of the breach, and legal representation before the Privacy Commissioner and courts (as needed), as well as ensure the organization's compliance with any applicable statutory timelines.

The particular legal, accounting, technical, public relations or other consulting services an organization will require following a data breach event will depend on the circumstances of the breach and the nature of the business. Costs for such services can be substantial.

Conclusion

Personal information and privacy liability in Canada is a growing field giving rise to an increasing number of significant lawsuits. Organizations that collect, use and disclose personal information should be mindful of the requirements and risks of handling such

[8] Ponemon Institute and IBM, "2015 Cost of Data Breach Study: Canada", May 2015, at p.2.

information. While the occurrence of a data breach may not always be predictable, organizations that handle personal information must recognize their vulnerabilities and ensure that adequate preventative and post-breach systems are in place in order to reduce the financial and legal exposures if a breach occurs. The consequences of a breach are amplified if an organization's response to the breach is handled poorly. Regardless of the size of the organization, a data breach can cause immediate harm to an organization's senior management, bottom line, clients, and reputation, and the negative effects of a data breach can continue to impact the business and its clients for years to come.