DOLDEN WALLACE FOLICK LLP

CURRENT LANDSCAPE OF PERSONAL INFORMATION AND PRIVACY LIABILITY IN CANADA

Eric A. Dolden, Jill M. Shore, Paul C. Dawson and Sinziana M. Gutiu

February 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

CONTACT LAWYER

Eric Dolden
604.891.0350
edolden@dolden.com

Jill Shore
604.891.0390
jshore@dolden.com

Gerry Gill
416.360.8331 (ext: 205)
ggill@dolden.com

Paul Dawson
604.891.0378
pdawson@dolden.com

Sinziana Gutiu
604.891.5259
sgutiu@dolden.com

Mikel Pearce
416.360.8331 (ext: 202)
mpearce@dolden.com

TABLE OF CONTENTS

© Dolden Wallace Folick LLP

I. INTRODUCTION

Personal information and privacy law is a rapidly developing area. Canada is seeing an increasing number of cases being brought to the courts, creative litigation strategies being tested, and legislative amendments awaiting implementation. 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.

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] Comprehensive security of personal information is no longer an optional practice, as 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.

Over the last year, Canada has seen litigation commenced as a result of unauthorized disclosure from increasingly diverse industries, including social media, government, banking, retail, online gaming and healthcare. We've seen unauthorized disclosures occur as a result of hacking, improper collection and access to data, administrative errors, or bad employee behaviour. Individuals whose personal data is affected by a breach have a number of common law and statutory tools available to them in order to take legal action. In turn, organizations must take precautionary action and become knowledgeable about the field of cyber liability in order to think strategically and minimize their potential exposure.

This paper will provide a summary of the current landscape of personal information and privacy liability in Canada in six parts:

- Part 1 provides a snapshot of the types of statutory claims that are available under the *Personal Information Protection and Electronic Documents Act* S.C. 2000, c. 5 ("PIPEDA") and provincial personal information acts (that have been deemed by the federal government to be "substantially similar"[2] to PIPEDA), the Privacy Acts in a few provinces, the Canadian Anti-Spam Legislation, S.C. 2010, c. 23

[1] Ponemon Institute and IBM, "2015 Cost of Data Breach Study: Canada", May 2015, at p.1.

[2] Section 26.2(b) of PIPEDA provides that if a province has enacted legislation that the federal government deems to be "substantially similar" to PIPEDA, then the organizations governed by that provincial legislation will be exempt from the application of PIPEDA respecting the collection, use and disclosure of personal information in that province, with the exception of FWUBs (see definition at p.4 of this paper).

© Dolden Wallace Folick LLP

("CASL"), as well as common law claims, such as the tort of intrusion upon seclusion, breach of contract, negligence, and others.

- Part 2 of the paper explores the process for certifying class action litigation in the context of data breaches.

- Part 3 provides a discussion about the "stacking" of various statutory and common law claims typically advanced, and describes what causes of action may be more successful and under what circumstances.

- Part 4 addresses breach notification requirements in Canada, including a discussion about the historical status of breach notification in Canada, and the notification provisions that will be enacted as a result of the new *Digital Privacy Act*, SC 2015, c. 32 (the "DPA"), which received royal assent on June 18, 2015.

- Part 5 summarizes the types of damages that have arisen under PIPEDA in the last two years, as well as damages under the common law privacy tort and CASL (starting July 1, 2017).

- Part 6 will describe the claims process, the role of counsel as a "breach coach", and the types of costs usually incurred following a data breach.

© Dolden Wallace Folick LLP

A. PART 1: CAUSES OF ACTION FOR CLAIMS IN CANADA

There are 38 separate statutes in Canada regulating the collection and use of personal information and health information, or that affect privacy rights. A complete list that applies to both private and public organizations is provided as Appendix "A" to this paper.

Statutory causes of action and the opportunity to recover damages are afforded by way of the following statues:

- PIPEDA or the equivalent substantially similar provincial acts;
- Privacy Act right of action for breach of privacy available in four provinces; or
- CASL starting July 1, 2017.

Common law causes of action are also available. The tort of intrusion upon seclusion, recognized by Canadian courts in the case *Jones v. Tsige,* 2012 ONCA 32, provides a common law cause of action that permits a plaintiff to recover up to $20,000 in damages without demonstrating that any pecuniary loss was incurred. Another privacy tort of public disclosure of private facts was recognized in Ontario in the case *Jane Doe 464533 v. D.*, 2016 ONSC 541, where much higher non-pecuniary damages were awarded despite the cap set in *Jones v. Tsige*. A claim in breach of contract may be available if there is a contract or implied term governing the protection of the personal information, such as a privacy policy or terms of use. A claim could also be made against an organization in negligence, by showing that the organization failed to adequately protect personal information, promptly notify affected individuals of the breach, or protect personal information following the breach. Some plaintiffs have brought privacy-related claims that were creatively framed in the tort of breach of confidence, breach of fiduciary duty, vicarious liability, the tort of publicity given to private life, and even violation of sections 7 (the right to life, liberty and security) and 8 (the right to a reasonable expectation of privacy) of the *Canadian Charter of Rights and Freedoms*.

This part of the paper summarizes the application of these various causes of action and how the courts in Canada are responding to data breach litigation.

© Dolden Wallace Folick LLP

1. Claims Under PIPEDA or "Substantially Similar" Provincial Acts

The federal government has constitutionally mandated legislative power over personal information in the possession or control of federal government entities, and over federally regulated entities (entities that are considered to be federal works, undertakings or businesses ("FWUB")), located anywhere in Canada. Provincial governments have constitutionally mandated legislative power over personal information in the possession or control of provincial government entities and over provincially regulated entities (all commercial activities within a province, excluding inter-provincial or international activities, or FWUBs).

The federal PIPEDA applies to personal information held by private sector organizations in some but not all provinces. It applies in the provinces and territories as follows:

- to organizations in industries such as telecommunications, broadcasting, inter-provincial or international transportation (*i.e.*, trucking, railways, and aviation), banking, military, nuclear energy, maritime navigation and shipping, which are subject to federal legislative jurisdiction;

- to organizations in the Yukon, Northwest Territories and Nunavut, which are considered to be FWUBs;

- to employee information of FWUBs; and

- to personal information (excluding employee information) collected, used or disclosed in the course of commercial activities by provincially regulated private organizations, in those provinces which do not have their own provincial personal information protection legislation applicable to the private sector in a format that has been deemed to be substantially similar to the federal PIPEDA (*e.g.*, in Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, PEI, Newfoundland, and the territories). Manitoba has passed its own privacy and personal information statute, but it has not yet come into effect.

© Dolden Wallace Folick LLP

The terms "organization", "personal information" and "commercial activities" are defined very broadly, which gives PIPEDA a wide reaching scope of application. However, PIPEDA does not apply to:

- employee information of provincially regulated private organizations in any province, even if PIPEDA applies to commercial activities of such private organizations;

- commercial activities of provincially regulated private sector organizations in the provinces of Alberta, British Columbia, and Quebec, which have their own provincial personal information protection legislation that has been deemed by regulation to be substantially similar to PIPEDA;

- health information custodians operating in the private sector in Ontario (subject to *Personal Health Information Act*, 2004 S.O. 2004, c. 3.), New Brunswick (subject to *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05), and Newfoundland and Labrador (subject to *Personal Health Information Act*, S.N.L. 2008, c. P-7.01), because they have also been deemed by regulation to be substantially similar to PIPEDA;

- any federal government institution to which the federal *Privacy Act* applies;

- information collected, used or disclosed for personal or domestic (family and home) purposes; and

- information collected by organizations for exclusively journalistic, artistic or literary purposes.

Federally (and in most Provinces) PIPEDA and its Provincial analogues are enforced by Privacy Commissioners, empowered to receive complaints, investigate potential non-compliance (e.g., data breaches), and to issue remedial Orders. If a Commissioner finds that an organization has failed to protect information as required by the statute, the Commissioner may issue remedial Orders, including the imposition of fines or penalties. If a Commissioner makes ruling on an organization's statutory compliance, the legislation permits individuals affected to sue in court for damages.

© Dolden Wallace Folick LLP

The provincial personal information protection Acts govern the collection, use and disclosure of personal information by private organizations (including businesses, charities, unincorporated associations, trusts, trade unions and labour organizations, and not-for-profit associations) within the enacting province. The provincial Acts typically do not apply to the collection, use or disclosure of personal information for personal or domestic (home or family) purposes.

Personal information is defined in these Acts in a manner that is substantially similar to the Acts that apply to protect personal information in the possession or control of public bodies. Personal information typically exempts business contact information, or work product information.

Most provincial personal information Acts empower the provincial Privacy Commissioner to hear complaints, make investigations, conduct inquiries, issue orders, enter into compliance agreements, and appeal orders to the courts.

The BC and Alberta Acts create a statutory cause of action for damages resulting from a breach of the Act found by the Commissioner, or resulting from an offence committed under the Act, if an individual has suffered actual loss or injury as a result of the breach or offence. These Acts do not provide for a right of appeal of a Commissioner's decision, but judicial review is available to the local courts.

The availability of a statutory cause of action under PIPEDA or the substantially similar legislation is triggered after the Privacy Commissioner has issued a report or order against the organization, or the complaint has been discontinued. The provincial Acts provide the Commissioner with the power to make orders, and establish offences under the Act for failing to comply with the order of a Commissioner. None of the Acts provide for a right to seek damages directly from the Commissioner for breach of privacy. However, the Quebec Act provides the Commissioner with broad powers to make remedial orders. Complainants may try to seek damages under this provision, or by seeking remedies in court after an order has been issued by the appropriate Commissioner.

An action under PIPEDA must be filed in Federal Court within one year of the report or notification issued by the Federal Privacy Commissioner (prior to the enactment of the DPA the timeline was 45 days). Alberta's personal information statute provides a deadline of 45 days after the Commissioner's order, whereas the window is only 30 days in British Columbia. If a claimant brings an action pursuant to PIPEDA, the claimant must demonstrate that the appropriate Commissioner issued a report or finding against the organization, that a breach occurred (the action is not a review of the

© Dolden Wallace Folick LLP

report but a *de novo* claim), that there is a nexus of damages arising from the breach, and where no specific damages can be shown, that it is appropriate to award damages.

Manitoba has not appointed a Privacy Commissioner, so its recent privacy legislation, once in effect, will allow affected individuals to commence action in the courts directly, without any prior resort to an administrative process or remedy.

The statutory cause of action under PIPEDA and equivalent Provincial statutes is premised specifically upon the loss, misuse, or unauthorized access to personal information held by an organization. A defense is available under PIPEDA if the organization can establish that it exercised due diligence to prevent the breach.

The following cases illustrate the types of situations that can lead to litigation under PIPEDA:

- *Speevak v. Canadian Imperial Bank of Commerce*, 2010 ONSC 1128 – Class action certification granted for the purpose of settlement. The defendant bank had inadvertently but repeatedly faxed customer information to a private fax machine in the United States. The Privacy Commissioner concluded that the bank had breached PIPEDA by failing to properly safeguard the information. No cases of identity theft appeared to have resulted from the breach, but the bank agreed to compensate anyone who did suffer a loss; it also paid $100,000 to a registered charity and $42,500 to class counsel for its fees, plus unspecified costs.

- *Chitrakar v. Bell TV*, 2013 FC 1103 – Plaintiff brought claim against Bell for emotional pain, anguish, anxiety, humiliation, and punitive damages as a result of Bell conducting an unauthorized "hard check" on the plaintiff's credit prior to installing satellite service, which the plaintiff claimed negatively affected his credit score. The court found that Bell breached PIPEDA and awarded the plaintiff $10,000 in damages, $1,000 in costs and $10,000 in exemplary damages for Bells' disregard of the plaintiff's privacy rights, failure to offer compensation, lack of engagement with the complaint, and failure to appear in Court.

- *Henry v. Bell Mobility*, 2014 FC 555 – Bell Mobility revealed the plaintiff's mobile telephone account to an unauthorized third party who impersonated the plaintiff, and also changed the PIN Number and the spelling of the plaintiff's name on the account. Bell corrected the error, apologized and conceded that it had breached PIPEDA. The plaintiff claimed $49,500 based on the decision in

© Dolden Wallace Folick LLP

Chitrakar, however the Court distinguished the cooperative response from Bell in this case, and only awarded the plaintiff $2,500.

- *Rowlands v. Durham Region Health*, 2012 ONSC 3948 - the plaintiff pursued damages under the Ontario health legislation that is substantially similar to PIPEDA. The Court approved a settlement arising from a nurse's loss in 2009 of an unencrypted USB stick containing data on 83,524 flu shot recipients. By 2012, there was still no evidence that any identity theft had occurred. The defendants agreed to reimburse any claims presented before August 2, 2016, and paid $500,000 to class counsel to cover costs.

2. Statutory Claim for Damages under Provincial Privacy Acts

The statutory cause of action under PIPEDA and equivalent provincial statutes is based specifically on the loss, misuse, or unauthorized access to personal information held by an organization. However, the *Privacy Acts* in several Provinces (British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador) have created a separate statutory cause of action premised upon a breach of a right to privacy, which is not restricted to personal information.

The statutory cause of action requires that the act leading to the breach of privacy be intentional, and proof of economic loss or other specific harm is *not* a pre-requisite for liability or damages.

British Columbia's *Privacy Act*, R.S.B.C. 1996, c. 373, provides an example of the operative provisions, and lists eavesdropping and surveillance as factors that create a *prima facie* presumption that the tort was committed:

> ***Violation of privacy actionable***
>
> ***1*** *(1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.*
>
> *(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.*
>
> *(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.*

© Dolden Wallace Folick LLP

(4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

Whether this cause of action may overlap with PIPEDA and similar statutory causes of action is an issue that is currently debated, as explained in more detail in Part 3 of this paper. Certain factual scenarios might give rise to claims under both the personal information and privacy statutory regimes, (*e.g.*, where an employee accesses private customer information without authority), but it can arise in situations not covered under the personal information statutes (*e.g.*, where an employee is alleged to have spied on customers in a business' restroom).

The case examples below illustrate how courts have interpreted the Privacy Act right of action:

- *Douez v. Facebook, Inc.*, 2014 BCSC 953, 2015 BCCA 279 - the Court approved certification of a class action on behalf of all Facebook users resident in British Columbia whose name, portrait, or both had been used by Facebook in a "sponsored story" without the user's consent. Section 3(2) of the BC *Privacy Act* makes it a tort, actionable without proof of damage, to use a person's name or portrait for advertising or promotional services without that person's consent. However, the Court of Appeal overturned the decision and dismissed the case on the basis that British Columbia did not have jurisdiction to hear the matter based on the forum selection clause in the plaintiff's contract with Facebook.
- *Ladas v. Apple Inc.*, 2014 BCSC 1821– Plaintiff brought a class action alleging that Apple devices using an iOS4 system recorded and stored unencrypted locational information without consent. The privacy claims were for breach of the provincial Privacy Acts, negligence, and breach of the privacy tort. The Court found that the pleadings disclosed a reasonable claim under the provincial Privacy Acts. However the class action was not certified as the plaintiff failed to establish an identifiable class and common issue. But see *Albilia c. Apple Inc.*, 2013 QCCS 2805, where the Court certified what appears to be a highly speculative action on behalf of consumers in Québec who had downloaded applications from Apple that allegedly shared private information with third parties.

- *Watts v. Klaemt,* 2007 BCSC 662 – the defendant recorded the plaintiff's telephone conversations with her daughter and son in law after being intimidated by the plaintiff's son in law. He reported the contents of the conversations to the plaintiff's employer (the plaintiff had disclosed confidential Ministry information to her daughter and son in law) and she was terminated for breach of trust. The Court found that this amounted to a violation of the plaintiff's rights under the

© Dolden Wallace Folick LLP

Privacy Act, and she was awarded general damages in the amount of $30,000, out of pocket expenses $1,000 and punitive damages in the amount of $5,000.

3. Common Law Invasion of Privacy Torts

In Provinces that have *not* adopted statutes equivalent to the *Privacy Acts* of British Columbia, *et al.*, the courts have developed a similar common law cause of action for invasion of privacy, known as the tort of intrusion upon seclusion, and the recently recognized tort of public disclosure of private facts.

First recognized by Ontario's Court of Appeal in *Jones v. Tsige*, 2012 ONCA 32, the test for liability is whether the invasion of privacy was intentional or reckless, lacked legal justification, and would be considered offensive to the reasonable person. It will typically relate to particularly personal subjects, such as medical information, financial matters, sexual orientation, diaries, private correspondence, etc. As previously mentioned, damages up to $20,000 are available despite lack of proof of actual harm.

In *Jones, supra,* a bank employee searched the private banking records of her colleague (who was also her common-law partner's ex wife) 174 times over the course of four years. The Court of Appeal recognized the new tort and given the lack of any pecuniary loss, awarded the plaintiff $10,000. The Court also provided a list of factors to be considered in awarding damages to act as a guide in future cases.

In *Evans v. Bank of Nova Scotia*, 2014 ONSC 2135, the Ontario Superior Court of Justice certified a class action based on the tort of intrusion upon seclusion. Customers of the Bank sued the bank and its employee as a result of the employee's disclosure of their personal information to his girlfriend, who then disseminated it for fraudulent and improper purposes, causing several customers to become victims of identity theft or fraud. The bank admitted the wrongful conduct took place and the plaintiff sought to hold the bank vicariously liable for the tortious and deliberate actions of its employee. The bank sought leave from the Divisional Court to appeal the class certification, but leave to appeal was denied.

Another privacy tort, the tort of public disclosure of embarrassing private facts, was recognized by the Ontario Superior Court of Justice in the context of "revenge porn" in *Jane Doe 464533 v. D.*, 2016 ONSC 541. The elements for this tort are the public disclosure of a private fact, and for the matter publicized or the act of the publication to be highly offensive to a reasonable person and not of legitimate concern to the public. In that case, an intimate video of a woman was posted by her ex-boyfriend on a public website the day he received it, after convincing her to send him the video on the promise that he would keep it private. The court found the defendant (who did not file

© Dolden Wallace Folick LLP

an appearance) liable for breach of confidence, intentional infliction of mental distress, and the tort of public disclosure of private facts, and awarded the plaintiff $141,000 (including costs).

4. Claims for Breach of Contract

When a data breach occurs, an action in breach of contract may be available as a result of the organization's promise not to collect, use or disclose personal information outside of the purposes consented to by its customers. This promise may be expressly made in a contract, or can be implied in certain circumstances. Whether or not this cause of action is available to a plaintiff involves an analysis of the provisions dealing with privacy or consent for services in a terms of use contract, privacy policy or other similar agreement. A claim in breach of contract does not require the plaintiff to demonstrate it has suffered actual loss in order to be entitled to damages.

In *Eliot Shore v. Avid Life Media Inc. and Avid Dating Life Inc.*, CV-15-22622CP (ONSC), a class action was commenced in breach of contract, breach of the Ontario *Consumer Protection Act*, negligence, intrusion upon seclusion, breach of privacy and publicity given to private life, against the online dating site Ashley Madison, for $760 million in damages. This high-profile case arose as a result of a data breach committed by one or more hackers called the Impact Team, who stole and publicly released personal information (including payment information and the messaging history) of Ashley Madison users. The site was marketed towards people who are married or in committed relationships, and was premised on the anonymity and privacy of its users in its privacy policy and terms of service. The claim alleges that the users' contract with Avid Dating Life Inc. included an express or implied term that it would prevent the unauthorized collection, retention and disclosure of users' personal information, which was breached as a result of the Impact Team's hack and public disclosure. Further, users had the option of paying extra to have their personal information deleted, which in a number of cases, the website failed to do.

In *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 (ONSC), the Court approved a certification and settlement of a class action arising from the 2011 hacking of Sony's "PlayStation Network" and related gaming services. Details of up to 4.5 million accounts held by Canadian gamers were compromised, and the network was temporarily shut down as a response to the attacks. Multiple class actions were commenced in Canada and the USA. Among other claims, the plaintiff argued that the defendant breached its contract with the users by allowing their personal information to be compromised, and depriving them of access to the network. Under the terms of the settlement, class members were entitled to be paid out in cash the balance of any affected PSN accounts; gamers were granted certain "online game and service benefits";

© Dolden Wallace Folick LLP

and Sony agreed to reimburse members who could demonstrate they actually suffered any identity theft, including expenses of up to $2,500 per claim. Class counsel fees were approved at $265,000, and Sony agreed to pay for a notice program that reached as many as 3.5 million account holders' email addresses.

Certification was refused in *St-Arnaud c. Facebook Inc.*, 2011 QCCS 1506, in which the class alleged they had been exposed to the disclosure of personal information as a result of changes Facebook made to its terms of use and policies. The Court concluded that because class members had clicked to accept the changes, they had no cause of action.

In *Albayate v Bank of Montreal*, 2015 BCSC 695, the plaintiff claimed breach of privacy, negligence, and breach of contract. The BC Supreme Court found that the Bank of Montreal had breached its contract with the plaintiff when it changed her address in their system without her knowledge or consent, causing her bank statements to be sent to her ex-husband's address, and incorrect contact information being provided to two credit reporting bureaus. The bank was not liable for breach of privacy as there was no unauthorized disclosure because her husband returned the unopened envelopes to her. She claimed $600,000 in damages and costs, but was only awarded $2,000 as she did not establish that she suffered any actual damages as a result of the bank's error.

A class action was filed in *Bennett v. Lenovo (Canada) Inc.*, CV-15-00523714-00CP, seeking $10,000,000 in damages (plus $5,000,000 in punitive damages) for the tort of intrusion upon seclusion, breach of contract and breach of the Ontario *Consumer Protection Act*. Lenovo preinstalled malicious "Superfish Software" on certain models of its retail laptops, allowing criminals to intercept user's secure connection, resulting in thousands of customers' personal and financial information becoming compromised. The plaintiff argued that Lenovo breached implied terms in its contract for sale with the class members, namely that the computers would be free of defects and not include malicious software that exposed the buyers to significant security risks, and that if dangerous software was installed on the computers, Lenovo would provide adequate warnings to class members before they decided to purchase the computers.

5. Claims in Negligence

A claim in negligence for a data breach may be commenced when the organization responsible for protecting the personal information failed to comply with a legal duty of care to protect the information, notify or respond to the breach, and caused the plaintiff to incur damages as a result. There is a general duty on organizations to protect personal information collected by them for a commercial purpose where it is reasonably foreseeable that harm could result from a data breach.

© Dolden Wallace Folick LLP

A plaintiff would have to show that the organization breached the standard of care required to protect the personal information and to respond to the breach. The appropriate standard of care for an organization to meet in the circumstances can be determined by standard practices in the respective industry, as well as past court decisions, or decisions of the Privacy Commissioner. One of the most challenging aspects of making out a claim in negligence is demonstrating that there has been a quantifiable loss.

Mazzona c. DaimlerChrysler Financial Services of Canada, 2012 QCCS 958, was a case arising from the defendant's loss of an unencrypted tape during shipment through UPS from the USA parent company to its Quebec subsidiary containing the names, addresses, phone numbers, birth dates, credit information and SIN number of approximately 240,000 customers. The plaintiff admitted she had not suffered any identity theft, and the Court concluded that mere anxiety about the *possibility* of theft was not injury and did not amount to compensable damages.

In *Belley v. TD Auto Finance Services*, 2015 QCCS 168, the Quebec Superior court certified a class action involving the same incident as in *Mazzona*. However, the plaintiff had suffered fraud and identity theft as a result of the loss, so the Court permitted the claims in negligence leading to breach and in response to the breach. The Court granted punitive damages for malicious, oppressive and high-handed conduct, which included a failure to encrypt data, failure to inform UPS of the contents and assigning a total $5 value to the tape, delayed and incomplete notification to its customers, and failing to offer any compensation to affected individuals.

In *Condon v. Canada*, 2015 FCA 159, 2014 FC 250, the Federal Court certified a class proceeding on behalf of 583,000 students whose financial and student loan data, stored on an unencrypted hard drive, was lost by a civil servant. The Court certified claims for breach of contract and for "intrusion upon seclusion", but refused to certify claims in negligence and breach of confidence because there was no evidence that any class member had suffered an actual loss. The Federal Court of Appeal sent the matter back to the trial level for determination, stating that the plaintiff had pled that they suffered damages, which was sufficient for the purposes of certification.

6. Additional Common Law and Charter Claims

Additional claims in tort, such as breach of confidence, breach of fiduciary duty and vicarious liability, and publicity given to private life, as well as claims alleging violation of the *Charter of Rights and Freedoms* s.8 and s.7 claims (when the state is involved), have been brought by plaintiffs with varied success.

© Dolden Wallace Folick LLP

Commencing an action for breach of confidence requires that the plaintiff's information be privately held by an organization for a specific purpose to be treated confidentially, and be disclosed without consent. Similar to a claim in negligence, demonstrating damages is an essential element in the claim. In *Condon, supra,* the Court did not certify a claim in breach of confidence because the plaintiffs could not demonstrate that they suffered any injury or loss.

If the data breach arose as a result of an employee's wrongful act or omission during the course of employment, a plaintiff may be able to allege vicarious liability against the employer organization. Further, if the organization is a public institution that can be said to have a fiduciary duty to the public or to those whose personal information it holds, a plaintiff may claim breach of fiduciary duty and breach of trust. *Evans, supra* and *Hopkins, supra*, are both examples where the Courts found that the pleadings alleging vicarious liability, and breach of a fiduciary duty disclosed a reasonable cause of action and granted certification. In *Broutzas/Taylor v. Rouge Valley Health System*, CV-14-507026-00CP hospital employees accessed and sold personal information about new moms to Registered Education Savings Plan ("RESP") companies without authorization. The plaintiffs are seeking damages in the amount of $412 million, alleging (among claims for breach of contract and negligence), vicarious liability on the part of the hospital and the RESP companies.

The claim of publicity given to private life was recently certified by the Federal Court in *John Doe & Suzie Jones v. Her Majesty the Queen,* 2015 FC 916. Although this case is currently under appeal, the Court noted that "*the area of privacy rights, either by statute, contract or tort, is developing rapidly. It is a new area and its development or limitation should not be decided at this stage of the litigation*".[3] The facts of this case are provided below and in Part 3 of this paper.

A claim for breach of s. 7 and 8 of the *Charter of Rights and Freedoms* may be available if the organization is a public body, and the plaintiff had a reasonable expectation of privacy. Section 7 of the Charter protects life, liberty and security of the person, and s.8 protects a person's right to be free of unreasonable search and seizure. In *John Doe & Suzie Jones, supra*, the plaintiffs argued that by disclosing their names, addresses and interest in the medical marijuana program, Health Canada violated their right to life, liberty and security, and their reasonable expectation of privacy. Although the Court certified this claim as well, it cautioned that the statement of claim would likely require amendments. Other creatively pleaded causes of action include breach of warranty, which is most often seen in product liability cases and arises out of breach of warrantees

[3] *John Doe & Suzie Jones v. Her Majesty the Queen*, 2015 FC 916, at para. 40. A Notice of Appeal was filed by the Government of Canada on April 6, 2015, and the certification decision is now under appeal.

© Dolden Wallace Folick LLP

in the contract, and the tort of conspiracy to commit an unlawful act, which is usually alleged in cases involving fraud.

7. CASL Private Right of Action (as of July 1, 2017)

CASL prohibits a wide range of commercial electronic activity, but provides exceptions for such activity within narrow circumstances. A person who contravenes the prohibitions in the statute faces investigation by the Canadian Radio and Telecommunications Commission ("CRTC"), which can impose "administrative monetary penalties" for "violations". CASL prohibits the sending of "commercial electronic messages" ("CEMs"), unless the recipient has consented to receive the message. CEMs must also meet certain formatting and functional standards, include the identification of the sender, the sender's contact information, and an "unsubscribe" mechanism through which recipients may decline further communications. A person who fails to cooperate with the investigations of the CRTC commits an "offence" and may be liable to a fine.

Insureds who engage in commercial electronic activity must be able to justify each and every CEM they send – including the basis for asserting "consent", or they may face regulatory investigation, administrative penalties, and starting in 2017, civil liability by way of a private cause of action.

On July 1, 2017, sections 47–51 of CASL will come into force and create a statutory cause of action that will allow individuals affected by a violation of CASL to sue in court for compensation.

As of that date, persons who believe they have been affected by an act or omission may sue for damages if the act or omission constitutes a contravention of any of sections 6 to 9 of CASL (sending CEMs, altering transmission data in a CEM, and installing computer program, without the required consent), or s. 5 of PIPEDA (collecting, using or disclosing personal information for purposes that a reasonable person would consider appropriate) relating to the collection or use in s. 7.1(2) and (3) of PIPEDA (use or collection without knowledge or consent) or relating to conduct reviewable under 74.011 of the *Competition Act* (sending or causing to be sent a false or misleading representation in an electronic message).

As with the administrative penalties that the CRTC may impose, a court imposing a compliance award must take into account the nature of the violation, profits made from the violation, ability to pay, etc.

© Dolden Wallace Folick LLP

The private right of action is subject to an important limitation – a court may not consider an application for compensatory damages pursuant to s. 51(1)(b) if the CRTC has issued a Notice of Violation, or has entered an undertaking (s. 48(1)). This prevents the imposition of both administrative fines *and* compliance awards for the same conduct. Further, there is a three year limitation period to bring an application for compensatory damages under CASL from the day "the subject matter of the proceeding became known to the applicant". This means that once the private right of action comes into force on June 1, 2017, claims may be brought for violations that occurred after July 1st, 2014 onwards. CASL also provides a defense that the person exercised due diligence to prevent the contravention.

B. PART 2: THE CLASS ACTION TREND IN CYBER LITIGATION

Because data breaches tend to involve mass records relating to large numbers of affected individuals, and the harm caused to each person may be individually difficult to prove or small in dollar terms, court proceedings for breach events in Canada are often brought as class actions.

The Federal Government has not passed a class action statute, but virtually all of the Provinces have done so. The Federal Court Rules permit a limited form of group representative proceeding, but the mechanism is not widely used. Almost all class actions are therefore filed in Provincial Supreme (Superior) Courts. Class actions involving data breaches do not rely on PIPEDA – which, as noted above, would require filing in Federal Court – but may rely upon Provincial personal information statutes, or upon statutory or common law privacy rights. They may also rely upon the privacy-related causes of action canvassed in the sections above. As illustrated in the cases in Part 1 of this paper, several data breach and privacy-related class actions have been commenced in Canada in recent years, with diverse results.

Class actions require certification by a court, and specific thresholds must be met before the action can be commenced. The procedure in class actions in general terms is as follows:

- A "Representative Plaintiff" works with class counsel to define the contours of the class on whose behalf the action is brought, and to define the common issues to be resolved.

- Class counsel brings a "certification motion" before the Court, seeking to have the action certified as a class action.

© Dolden Wallace Folick LLP

- If the Court is satisfied that the proposed action meets the conditions set out in the jurisdiction's *Class Proceedings Act*, which typically requires evidence that there is an issue to be tried; that the proposed class definition and common issues are workable; that a class proceeding would be the most appropriate way to resolve those issues; and that the proposed plaintiff can adequately represent the class; then the Court will grant the certification.

- The parties will then negotiate (or the Court will order) a litigation plan setting out how the matter will be tried. Typically a "common issues" phase is tried first, and a process for resolving any remaining "individual issues" will be established (usually by a claims manager, umpire, or through arbitration, rather than a full individual trial before the Court).

- If at any point in the process the parties negotiate a settlement, they must return to the Court and seek its approval.

Privacy class actions are not always certified, and if certified, do not result in especially large settlements. Class members are able to recover nominal damages individually, which can become significant if the class is large enough. In addition, defence costs can sometimes be substantial. Very few Canadian class actions of any kind are ultimately tried on their merits, and privacy-related actions are no exception. A minority of proposed actions fail at the certification stage if the Court concludes that the issues raised in the proceeding cannot suitably be resolved on a class-wide basis. The legislation in some provinces may provide for cost awards against unsuccessful claimants.[4] More cases are certified "for the purposes of settlement", or settle after the certification is granted.

A key issue in class action certification is determining whether the class action raises common issues among all class members. The issues must be substantial and the class proceeding must be the preferable method for resolution of those common issues.

Unlike class action requirements in the USA, Canadian class action statutes do not require that common issues predominate over the individual issues. However, in certain provinces, the court may weigh common vs. individual issues as a factor in determining whether there is a preferable alternate method of addressing the claims.

[4] See Ontario's *Class Proceedings Act, 1992*, SO 1992, c. 6. Saskatchewan's *Class Actions Act, 2001*, c.C-12.01, also provides for cost awards, but at a lower scale.

© Dolden Wallace Folick LLP

C. PART 3: STACKING COMMON LAW AND STATUTORY CLAIMS

When applicable, stacking of multiple common law and statutory claims in an action can provide an avenue for plaintiffs to overcome one or more of the potential barriers to a claim. Such barriers can include monetary thresholds for damages, the need for a plaintiff to demonstrate it suffered actual damages, and that the defendant's actions were intentional or reckless.

When there is a potential breach of PIPEDA or its provincial substantially similar legislation, a plaintiff will make a complaint to the appropriate Commissioner while at the same time commencing an action in court in one of the other privacy-related causes of action. Once the Commissioner's decision is issued, the pleadings are typically amended to include a breach of PIPEDA (or the equivalent provincial act). The Commissioner's decision can be used during certification to justify that there is a triable issue, and the evidence and findings in the report can be used to prepare the plaintiff's case and determine the appropriate standard of care.

There is an ongoing debate in Canada, which varies by jurisdiction, as to whether the provincial Privacy Acts preclude the ability to also bring a claim for the tort of intrusion upon seclusion. In British Columbia and Alberta, superior courts have held that the tort of invasion of privacy is not available in light of the exclusive statutory tort created by the Privacy Act. However, a number of the British Columbia cases that stand for this principle are currently under appeal and remain to be decided.

The Manitoba *Privacy Act* explicitly states that "any cause of action created by the Act is not in derogation of existing causes of action available to a claimant." The Manitoba Court of Appeal in *Grant v. Winnipeg Regional Health Authority et al.*, 2015 MBCA 44 held that the wording of the Manitoba Privacy Act permitted a plaintiff to also claim the tort of intrusion upon seclusion. In that case, a man died in a Manitoba hospital, and the hospital, in its public statement to the media, negligently disclosed confidential patient information about the deceased.

In *Hopkins v. Kay*, 2015 ONCA 112, the Ontario Court of Appeal held that the Ontario *Personal Health Information Protection Act* ("PHIPA") was not an exhaustive code that precluded the application of the common law privacy tort, and that permitting actions based on the tort would not undermine or circumvent the PHIPA scheme. The court found that the elements of the common law cause of action were not more advantageous than PHIPA, and that PHIPA did not, like the BC and Alberta Privacy Acts, provide a general statutory cause of action for general breach of privacy. The Supreme Court of Canada dismissed the appeal (cited as *Peterborough Regional Health Centre, et al. v. Heike Hesse and Erkenraadje Wensvoort*), meaning that health custodians

© Dolden Wallace Folick LLP

can be sued for privacy breaches as well PHIPA, if a claim is available following the decision of the Privacy Commissioner.

In *John Doe, supra,* the Federal Court certified an action where Health Canada's medical marijuana access program made an administrative error in its mail-out and sent letters to its members with the program name on the envelope's return address. The plaintiff claimed for breach of warranty, breach of contract, negligence, breach of confidence, tort of intrusion upon seclusion, tort of publicity given to private life, and breach of the *Charter of Rights and Freedoms* s.7 and s.8. By stacking the various claims, the plaintiff was able to overcome the lack of pecuniary damages required for some of the claims due to the low evidentiary threshold of certification. The Court certified all causes of action alleged, and suggested amendments to the Notice of Claim.

D. PART 4: BREACH NOTICE REQUIREMENTS IN CANADA

1. Historical Situation

Private sector personal information protection Acts require organizations to comply with minimum personal information protection measures. All of them impose on the organizations a duty to protect personal information within their possession or control. Although the "duty to protect" sections are all worded differently, they typically require that personal information must be protected by security safeguards appropriate to the sensitivity of the information, to protect against loss or theft, and unauthorized access, disclosure, or use.

Historically, most provincial health Acts have imposed a duty to protect personal health information. The provincial health information Acts apply to the collection, use and disclosure of personal health information held by "health information custodians" within the enacting provinces. Health information custodians are typically defined to include, among others, health care practitioners (doctors, dentists, physiotherapists, etc.), home care service providers, hospitals, independent health facilities, retirement and long term care homes, pharmacies, and ambulance services. Most of these Acts (all but British Columbia) impose on custodians a duty to protect against unauthorized use or disclosure of personal health information in its possession or control. Most empower the provincial Privacy Commissioner to hear complaints, make investigations, conduct inquiries and issue orders, similar to the other provincial personal information protection Acts, and to appeal orders to the courts. These Acts also create offences for certain breaches of the Acts, which are punishable by monetary penalties.

© Dolden Wallace Folick LLP

The Ontario *Personal Health Information Protection Act*, *2004*, S.O. 2004, c. 3 (the "Ontario PHIPA"), the Newfoundland and Labrador *Personal Health Information Act,* S.N.L. 2008, c. P-7.01, and the Nova Scotia *Personal Health Information Act,* S.N.S. 2010, c. 41 contain a duty to notify the individual affected at the first reasonable opportunity, if personal health information is stolen, lost or accessed by unauthorized persons. The Ontario PHIPA also creates a statutory cause of action for damages resulting from a breach of the Act found by the Commissioner, or resulting from an offence committed under the Act. Amendments to the Alberta *Health Information Act*, R.S.A. 2000, c. H-5, which passed on May 14, 2014, once in force, will add mandatory notice provisions and create new offences and penalties for health-related data breaches involving personal information.

The Saskatchewan *Health Information Protection Act*, SS 1999, c. H-0.021, empowers the court to make any order it considers appropriate if it has found that a breach of the act has occurred. Complainants could try to seek damages under this section.

The Alberta PIPA has some unique provisions that were added by amendment to that Act in May 2010, which set out minimum standards for mandatory notification requirements in the event of security breaches that pose a real risk of significant harm (organizations must notify the Commissioner, and upon receipt of such notice, the Commissioner may require the organization to give notice to affected individuals). The purpose of the notification requirements is to avoid or mitigate harm to individuals that might result from the breach.

With the exception of the Alberta PIPA and the new amendments to PIPEDA made in the DPA (discussed below), none of the other general personal information protection Acts currently contain an express duty to notify. Manitoba's *Personal Information Protection and Identity Theft Prevention Act*, SM 2013, c. 17, s. 34(2), (the "Manitoba PIPITPA") will, if it comes into force, require organizations to notify individuals "*as soon as practicable*" about the theft or loss of, or unauthorized access to, their personal information. As of July, 2015, this statute has not yet come into effect.

Like the personal information protection Acts that apply to the public sector, these Acts establish a Commissioner with similar powers to hear and investigate complaints, initiate their own complaints and audits, and write reports of their conclusions and make orders following an investigation. Many of these Acts give the complainant a right to apply to court for a hearing following an investigation.

© Dolden Wallace Folick LLP

2. The *Digital Privacy Act* ("DPA")

The Federal Government's DPA received Royal Assent on June 18, 2015. This legislation provides a number of amendments PIPEDA, including new mandatory breach notification provisions. These new provisions are not presently in force and are still subject to further consultation with businesses and other stakeholders. Two previous government Bills (Bill C-29, 2010 and Bill C-12, 2011) failed to pass before the close of the respective Parliamentary sessions, and a substantially similar Bill introduced by an opposition Member of Parliament was defeated by the government in January, 2014 (Bill C-475).

Sections 10.1 to 10.3 of the DPA will require mandatory data breach notification to both the Privacy Commissioner and to affected individuals of any breach of security safeguards involving personal information, "*if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual*". The definition of "significant harm" includes, but is not limited to, bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. Determining whether there is a "real risk" of significant harm will involve a consideration of a number of open factors, including the sensitivity of the personal information affected by the data breach, and the probability that the personal information has or will be misused.

Notification must be provided as soon as feasible, and the contents of the notification must include sufficient information to allow individuals notified to understand the significance of the breach and be able to take steps to reduce or mitigate their risk of harm. Additional prescribed information, to be enacted by regulation, must also be included.

Organizations must also keep and maintain a log of *every* breach of security safeguards involving personal information, which could be overly onerous given the cost to organizations of documenting and investigating breaches. The Commissioner may request to review the log, and a failure to comply can be deemed to be an offence under PIPEDA.

The breach notification amendments to PIPEDA are anticipated to dramatically increase the cost to Canadian businesses resulting from data breaches, triggering more demand for cyber insurance to cover these costs, and a likelihood that more first party claims will arise.

© Dolden Wallace Folick LLP

Other notable DPA amendments to PIPEDA include:

- Shortened definition of "personal information" from "*information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization*" to "*information about an identifiable individual*";

- Requirement that consent is only valid if in the circumstances it is reasonable to expect that the consenting individual would understand the nature, purpose and consequences of the collection, use or disclosure of personal information;

- Exceptions from consent for information contained in witness statement for insurance claim administration purposes, and for business transactions if prescribed statutory requirements are met;

- Exempted business contact information collected, used or disclosed "*solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession*";

- An extension from 45 days to one year from the date of the federal Commissioner's report to file an action in the Federal Court;

- Added power for Commissioner to enter into compliance agreement with organizations to enforce negotiated settlements; and

- Changes to offences and penalties for failure to comply with PIPEDA, including requirement to show intentional breach of Act, failure to notify, and failure to maintain a breach log.

The provinces that have substantially similar legislation to PIPEDA will likely have to implement similar amendments to their current Acts in order to maintain substantially similar status to PIPEDA.

3. Case Study: *Zuckerman c. Target Corporation*[5]

A recent Quebec case, although dismissed on the basis of lack of jurisdiction, foreshadows an interesting argument based on admissions in breach notices that might be revisited in future class actions.

[5]*Zuckerman c. Target Corporation*, 2015 QCCS 1285.

© Dolden Wallace Folick LLP

The plaintiff, Mr. Zuckerman, shopped in the USA Target stores using his Bank of America credit card. Between November 27, 2013 and December 15, 2013, Target's customer information data network was hacked, affecting the payment card information of millions of its customers in the USA.

Mr. Zuckerman received two notification emails from Target Canada (who was not added as a defendant in the action). The first informed customers that the payment information of its USA customers had been stolen, and that it was likely that contact information (name, email, mailing address and phone number) of some Canadian customers may have also been taken. The second letter provided further apologies as well as a free credit monitoring services for a year, and stated that the compromised contact information was "*generally publicly available information, so the primary risk is increased exposure to consumer scams, such as phishing, web scams and social engineering*".[6]

Mr. Zuckerman argued that Target (through Target Canada) admitted that Mr. Zuckerman had suffered a loss as a result of the breach, by offering free credit monitoring, apologizing and stating that there was a primary risk of increased exposure to scams. Mr. Zuckerman's claim in negligence was that Target had improper security measures and protocols in place, failed to prevent the breach despite prior warnings and ongoing breaches, offered inadequate credit monitoring for an insufficient period of time with less insurance available to Canadian vs. USA customers, and failed to promptly and accurately notify its Canadian customers thereby leaving them vulnerable to attack.

The Court found that there was no evidence that Mr. Zuckerman had suffered any actual damages, and ultimately dismissed the claim on the basis that the Quebec Court did not have jurisdiction to hear the action.

E. PART 5: DAMAGES

Individual damages in data breach and privacy cases tend to be nominal unless an actual loss can be demonstrated. The Court in *Jones*, *supra*, awarded only $10,000 to the successful plaintiff without evidence of loss. Likewise, damages under a successful claim for breach of PIPEDA can give rise to damages in the range of $1,000 to $5,000, while damages under the Privacy Acts can result in slightly higher damages, between $5,000 and $35,000 under the BC Privacy Act.

[6] *Ibid,* at para 8.

© Dolden Wallace Folick LLP

In *Chitrakar v. Bell TV*, *supra*, an award of $21,000 (including $10,000 in punitive damages) under PIPEDA was widely considered to be large. The high award appears to be a result of the court's finding that Bell's behaviour in disregarding the personal information of the plaintiff was reprehensible.

The Federal Court in *Townsend v Sun Life Financial*, 2012 FC 550, emphasized three rationales for awarding damages under PIPEDA: compensation, deterrence and vindication. Some of the factors to consider include the seriousness of the breach, including the impact of the breach on the health, welfare, or financial position of the plaintiff, the conduct before and after the breach of the defendant, and any benefits to the defendant as a result of the breach.

In *Henry v. Bell Mobility*, *supra,* the court only awarded the plaintiff $2,500 plus interest for breaching PIPEDA as Bell had "taken responsibility for the breach", "put in place stapes to better train CSRs", did not benefit in any way from the breach, and acknowledged that the plaintiff was entitled to some damages as a result of the breach.

In cases involving the tort of intrusion upon seclusion involving non-pecuniary loss, the damages are symbolic and cannot exceed $20,000. In *Jones v. Tsige, supra*, the court left open the potential for aggravated and punitive damages in appropriate cases, and provided a number of factors to be considered in awarding damages, similar to those in *Townsend, supra.* The factors include the relationship between the parties, distress, annoyance or embarrassment suffered by the plaintiff as a result of the breach, and the parties' conduct following the breach, including any apologies made by the defendant.

However, in *Jane Doe 464533 v. D.*, *supra*, the court awarded $100,000 plus $41,000 in costs, ($100,000 are the maximum damages available under the Ontario Simplified Procedure that the action was commenced under), based on the new tort of public disclosure of private facts, breach of confidence and intentional infliction of mental distress. The court took note of the cap for non-pecuniary damages set in *Jones v. Tsige, supra,* but found that given the nature of "revenge porn" as a wrong, and its significant and ongoing impact on the plaintiff, an analogy to the damages awarded in claims arising from physical sexual battery, "with its attendant psychological impact and consequences", was more appropriate.

In *Mazzona c. DaimlerChrysler Financial Services of Canada*, 2012 QCCS 958, the court reiterated that the law does not recognize upset, disgust, anxiety, agitation or other similar mental states as a form of injury, unless it is serious, prolonged and rises above the ordinary annoyances, anxieties and fears that people living in society have come to accept.

© Dolden Wallace Folick LLP

In claims where the plaintiff has not suffered actual pecuniary loss, interesting arguments are advanced alleging waiver of tort, disgorgement of profits, restitution, moral damages for humiliation and embarrassment, general damages for anxiety, annoyance, upset and loss of time and effort in dealing with the effects of the breach, and special damages for expenses incurred.

A US case suggests that the legal scope of "injury" may be subject to future reconsideration in certain contexts. In *Remijas v. Neiman Marcus Group, LLC,* No. 14-3122 (7th Cir. 2015), a decision of the U.S. Court of Appeals for the Seventh Circuit, found that "injury" meant more than immediate charges as a result of a hacker data breach. The Court stated that the customers of the defendant, Neiman Marcus, faced an objectively reasonable likelihood that identity theft or credit card fraud would occur, and that requiring the affected customers to wait for the threatened harm to materialize in order to sue would only dilute their ability to establish causation. It remains to be seen whether this line of reasoning will be applied in the Canadian context in future cases to argue that requiring proof of actual damages (at least in the hacker context) could be prejudicial to individuals affected by the breach.

The private cause of action under CASL starting July 1, 2017, has been discussed in Part 1 of this paper. The scale of compensation under this new statutory right of damages appears to be significant. It includes actual loss, damage or expenses incurred by the complainant, *as well as* amounts intended to "*promote compliance*" (ss. 51(1)(b) and 51(2)). Such "compliance awards" are calculated based on the nature of the violation. For example, sending unauthorized CEMs, in breach of s. 6, will bring a maximum of $200 for each contravention, up to $1,000,000 for each day on which the contravention occurred, whereas diversion of electronic messages (s. 7) or installation of unauthorized software (s. 8) brings a maximum of $1,000,000 for each day on which the contravention occurs.

In the Porter Air decision issued by the CRTC on June 29, 2015, the company entered into an undertaking and agreed to pay $150,000. Porter Air was alleged to have sent commercial emails with inadequate unsubscribe information, and with an unclear unsubscribe mechanism. Porter Air's CEMs failed to provide all required information, failed to honour unsubscribe requests within 10 days, and Porter Air was unable to provide proof of consent to send CEMs.

On March 25, 2015, Plenty of Fish agreed to enter into an undertaking and paid $48,000 after the CRTC investigated complaints that the company had sent CEMs to its own members with an unclear and delayed unsubscribe mechanism.

© Dolden Wallace Folick LLP

In Compu-Finder, the CRTC issued a Notice of Violation on March 5, 2015 with a penalty of $1.1 million for CEMs about a training course being sent without consent, and with a non-functioning unsubscribe mechanism.

Subject to future decisions regarding the quantum for compensatory damages pursuant to the CASL statutory cause of action, the three CASL violation cases that have been investigated by the CRTC to date suggest that agreeing to an undertaking may be a more cost-effective way of dealing with an alleged violation of CASL.

F. PART 6: THE CLAIMS PROCESS AND THE BREACH COACH

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 that certain factors can reduce the per capita cost of data breach, including having robust incident response plans, acquiring insurance protection and using a strong incident response team.[7]

This section of the paper outlines the role of a "breach coach", and the types of services a firm like ours can provide:

- Section 1 outlines several important issues to be considered when a data breach is discovered: *identification and containment, notification and statutory compliance*, and *documentation*.

- In Section 2, we describe the types of costs that insureds might incur in the event of a data breach, including forensic computer analysis and notification about the data breach to affected individuals.

1. Issues to Consider as First Response

Many insureds, when they first report a data breach to their insurer, will not be familiar with their obligations under Canadian privacy legislation, or know what they need to do to protect themselves and their customers. A breach coach can assist insureds to act quickly on several fronts at once – *identification, containment*, *notification* and *documentation*.

[7] *Supra*, note 1 at p. 2. Other factors mentioned were extensive use of encryption, employee training programs, board-level involvement, CISO appointments, and business continuity management.

© Dolden Wallace Folick LLP

a. Identification and Containment

As seen from the case examples in Part 1 of this paper, data breach may arise in many different forms, including the accidental erasure of customer's personal information, an employee's unauthorized access of confidential information, the loss of an unsecured USB drive or laptop computer, or even as a result of malicious hacking or malware attacks. Identifying the nature and extent of data loss, mechanism of loss, and securing the insured's networks to prevent any further loss or unauthorized access will thus be a top priority. Insureds should immediately contact the forensic technological support service provider appointed by its insurer under the program (or as recommended by their breach coach), who will work with the insured to identify the cause and scope of the breach, including the nature of the data affected. They will also help the insured secure its networks and data from further loss or intrusion, thereby minimizing reputational losses and business interruption claims.

A breach coach will coordinate these functions to ensure that first responders are tracing all steps and preserving all evidence in the event of future anticipated litigation, as well as vetting all communications by the affected organization to minimize further potential harm or liability, and to preserve privilege over communications.

Prompt identification of the cause of the breach may also affect the insured's legal obligations and defences. For example, due diligence is a defence in proceedings before a Privacy Commissioner, and may also be a defence to any ensuing lawsuits, *i.e.*, if the breach arose from a sophisticated external hacker or disgruntled employee whose conduct could neither be foreseen nor guarded against with reasonable network security systems. In other cases, the cause of the breach may confer recovery rights against other parties, *e.g.*, a third party internet provider or computer repair firm that failed to provide or maintain appropriate security measures.

b. Notification and Statutory Compliance

As noted above, the discovery of a data breach can trigger legal obligations pursuant to Canadian personal information legislation, which can vary by subject matter and jurisdiction. A breach coach will assist to identify which jurisdiction's laws may be triggered and what is required to comply with them, while at the same time protecting the organization's interest. To help insureds navigate these complexities, a breach coach such as our firm can assist across Canada with pre-breach risk assessment, post-event notification to Provincial or Federal Privacy Commissioners, customer relations management, breach notification to customers or clients, and with preparations to defend any ensuing litigation.

© Dolden Wallace Folick LLP

The initial role of a breach coach will be to provide advice on the applicable legislative imperatives. A breach coach will assist the insured throughout the response process to determine whether a report to local law enforcement would be advisable, and work with the insured to retain appropriate resources, including technical support, public relations advice, or credit monitoring services.

c. Documentation

From the first discovery of breach, and as containment efforts are implemented, Insureds should document all aspects of the breach, and the steps taken to resolve it. If there is a risk of third party claims resulting from the breach, defence counsel should be retained immediately to assist with investigations and documentation, for several reasons:

- Details as to when and how a breach was discovered may affect the commencement of statutory timelines for notifying regulators or other affected persons about the breach.

- The nature of the data affected by the breach will shape the insured's response and obligations; for example, in some Provinces personal health information is subject to specific legislation, distinct from other types of personal records.

- Information about potentially affected customers or clients should be compiled in order to facilitate their notification about the breach.

- Regulators notified about a data breach may choose to investigate the circumstances of the breach, including the insured's practices and procedures for handling data, before and after the breach occurred. As discussed further below, providing a comprehensive and cooperative response to such investigations may reduce the risk of adverse regulatory findings or subsequent civil litigation.

If the insured chooses, a breach coach can also assist as defence counsel in proceedings involving the Privacy Commissioner or any third party proceedings (either by the insurer's appointment upon exercising a duty to defend, or at the insured's election). The role of "defence counsel" is to assist the insured by helping to draft responses to the appropriate Privacy Commissioner, attending any hearings and making submissions on the insured's behalf, seek to manage the consequences of the breach (*e.g.*, limiting the scope of any notice program), and laying the groundwork for the defence of any further claims or actions that might follow. Early consultation with a breach coach can help

© Dolden Wallace Folick LLP

reduce litigation costs and potentially an insured's exposure to fines or damages by improving the insured's threat response to the data breach.

2. First Party Claims and Costs

Within the existing legislative framework, data breach claims typically follow a consistent pattern: discovery of a breach, followed by a *possible* complaint to a Privacy Commissioner by an affected individual, which *could* lead to a regulatory proceeding before the Commissioner and/or a civil action before the Courts.

The particular legal, accounting, technical, or other consulting services an insured will require will depend on the circumstances of the data breach or privacy event at issue. They can be substantial: in one recent case, a manufacturer whose customer database of 120,000 records was hacked incurred $185,000 in computer forensics, $326,000 in legal costs, $200,000 to mail notice of the breach to its customers – all *before* incurring a further $450,000 to defend against resulting regulatory proceedings and a class action.

Underwriters' first notice of a data breach will typically be given by the insured – ideally, very soon after the breach has occurred – before any third party has made any Claim against the insured. Even in the absence of a claim the insured may begin to incur recoverable costs immediately. These can include fees paid to lawyers, accountants, technical consultants, etc.:

- for computer forensic analysis of the insured's computers to determine the cause and extent of the breach;
- to document steps taken by first responders to ensure preservation of evidence;
- to interview witnesses regarding data security and loss to prepare for potential investigations or litigation;
- to review any contractual indemnification that might be available to the insured from its contractors or suppliers;
- to determine if the insured must notify affected individuals or regulatory agencies about the breach;
- to comply with any applicable privacy or personal information statutes;
- to notify affected individuals or regulatory agencies about the breach;

© Dolden Wallace Folick LLP

- to seek legal advice with respect to all of these steps to minimize further risk of liability arising from the response;

- for a public relations campaign to counter or minimize negative publicity from the event or to protect the insured's business reputation; or

- to procure credit monitoring services for individuals affected by the breach.

Notice costs can be particularly serious. Most jurisdictions in the United States require organizations who suffer data breaches to notify affected individuals directly, within very short timeframes (*e.g.*, 30-45 days). As mentioned in Part 4 of this paper, only a few Canadian Provinces have included mandatory notice provisions in their legislation:

- The Alberta PIPA, at s. 34.1, and at ss. 19, 19.1 of its regulations, requires organizations to notify the Commissioner of any "*loss of or unauthorized access to or disclosure of*" personal information, if a "*reasonable person*" would consider there to be a "*real risk of significant harm*" from the breach. Notice must be given "*without delay*". The Commissioner may then require the organization to notify all individuals who may be at risk from the breach (s. 37.1).

- Manitoba's PIPITPA will require an organization to notify individuals "*as soon as reasonably practicable*" if any personal information about that individual is stolen, lost or accessed without authority. However, as of July 2015, this statute has not yet come into effect.

- Legislation in Ontario, Newfoundland and Labrador, and New Brunswick pertaining to personal *health* information requires custodians of that information to notify affected individuals about any loss, theft, or unauthorized access "*at the first reasonable opportunity*".

- Finally, the Federal Government has enacted the DPA which amends PIPEDA to require mandatory data breach notification, to both the Privacy Commissioner and to affected individuals, of any breach of security safeguards involving personal information, "*if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual*".

While other Provinces do not automatically require insureds to notify either affected individuals or the Privacy Commissioner about a data breach event, notice costs often arise in any event. Some insureds will automatically notify customers about breaches

© Dolden Wallace Folick LLP

that have disclosed financial information, either because the insureds wish to protect their reputation and goodwill, or because they are compelled to do so by agreement with credit card companies.

Commissioners who investigate after receiving a complaint have a statutory discretion to impose remedial Orders, which commonly includes ordering insureds to notify customers. This can occur at any time before or during the Commissioners investigation, or as part of the Commissioner's directions following a formal inquiry. The Commissioner will typically require that the notice be given in a form he or she approves or directs. Further, the obligation to protect data continues after the breach. The duty to notify may arise out of this duty and require notice to be given.

First party privacy breach costs recoverable under cyber policies do not usually include wages of the insured's personnel, the costs of complying with any injunctive or non-monetary relief, financing costs, taxes, or fines, sanctions, or other penalties. Nor does the term "privacy breach costs" usually include the costs of recovering or reconstructing lost data, or upgrading systems. Privacy breach costs must be incurred within a specific time period, usually 12 months, after the breach is first reported.

The types of loss contained within the definition in the cyber policy for privacy breach costs do not usually represent "property", and the cyber policy is not, strictly speaking, property insurance. However, it is first-party coverage, and therefore subject to many provisions of the respective Provincial Insurance Acts.

In British Columbia, Alberta, and Manitoba, an insured may not bring an action against an insurer until at least 60 days after the insured has filed a proof of loss, and a two year limitation period applies before the insured may commence an action under the Policy, commencing from the date the cause of action arose. In several Provinces, an insurer is required by regulation to notify insureds about any limitation periods applicable to an insured's right of action against an insurer, within 5 days of denying a claim or within 10 days of the anniversary of the loss, and such periods do not begin to run until such notice is given.

In some cases, coverage issues may arise. A few examples of coverage issues that are typical to cyber insurance claims include:

- Cyber policies typically only provide reimbursement coverage; they do not require the insurance company to appoint or instruct counsel or other professionals on the insured's behalf.

© Dolden Wallace Folick LLP

- Privacy breach costs are within the Policy's limits, not in addition to them, so amounts the insured incurs for such costs erode the indemnity that might otherwise be available to respond to claims under other insuring agreements.

- Furthermore, the insured is typically responsible for all privacy breach costs incurred up to the amount of the self-insured retention stated in the declarations.

It should be noted that cyber policies typically cover loss. The definition of "Loss" usually carves out and does not include:

- any amount for which the insureds are absolved from payment by any covenant, agreement or court order;

- taxes, fines, or penalties (unless expressly covered);

- the cost to comply with any injunctive or other non-monetary relief;

- loss of income, fees or profits by the insured;

- return by the insured of fees, commissions, or royalties received by it; or

- matters uninsurable under the law pursuant to which the terms of the Policy are construed.

A cyber policy can also contain many other limitations of liability. It may not cover either "bodily injury" or "property damage". Claims arising from privacy wrongful acts, are usually covered under cyber policies, as are defence costs incurred in regulatory proceedings.

G. CONCLUSION

This paper has provided a summary of the current landscape of personal information and privacy liability in Canada, and has touched on six key topics. It explored the types of statutory and common law claims available to commence a lawsuit, the recent trend of class actions in privacy litigation, the benefits and limitations of stacking claims in privacy actions, the status of breach notification historically and under the DPA, the ranges of damages that can be anticipated for some causes of action, as well as a discussion of the role of the breach coach, claims process and costs.

© Dolden Wallace Folick LLP

Personal information and privacy liability in Canada is a growing field made up of a combination of caselaw, regulations and legal processes. Organizations that collect, use and disclose personal information must be mindful of the requirements and risks of handling such information. Data breaches are far-reaching, and a poorly handled data breach can have significant effects regardless of the size of the organization. A data breach can cause immediate harm to an organization's senior management, bottom line, clients, and good will. The negative effects of a data breach can continue to impact the business and its clients for years to come.

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 consequences if a breach occurs. Our firm has a wealth of experience and knowledge in this area, and our dedicated team of lawyers is available to assist. Should you require assistance with a data breach, please do not hesitate to contact us.

© Dolden Wallace Folick LLP

APPENDIX "A"

LIST OF PERSONAL INFORMATION AND PRIVACY STATUTES IN CANADA

a. Personal Information Protection Laws that Apply to Government and Public Bodies:

Federal	*Privacy Act*, RSC 1987, c. P-21.
Alberta	*Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25
British Columbia	*Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165
Manitoba	*Freedom of Information and Protection of Privacy Act*, CCSM, c. F175
New Brunswick	*Right to Information and Protection of Privacy Act*, SNB 2009, c. R-10.6
Newfoundland	*Access to Information and Protection of Privacy Act*, 2015, SNL 2015, c A-1.2
Northwest Territories	*Access to Information and Protection of Privacy Act*, SNWT 1994, c. 20
Nova Scotia	*Freedom of Information and Protection of Privacy Act*, SNS 1993, c. 5
Nova Scotia	*Part XX of the Municipal Government Act*, SNS 1998, c. M-26
Nova Scotia	*Personal Information International Disclosure Protection Act*, SNS 2006, c. 3
Nunavut	*Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c. 20
Ontario	*Freedom of Information and Protection of Privacy Act*, RSO 1990, c. F. 31
Ontario	*Municipal Freedom of Information and Protection of Privacy Act*,RSO 1990, c. M.56
Prince Edward Island	*Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c. F-15.01

© Dolden Wallace Folick LLP

Quebec	*An Act respecting access to documents held by public bodies and the Protection of personal information*, CQLR, c. A-2.1
Saskatchewan	*The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. F-22.01
Saskatchewan	*The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. L-27.1
Yukon	*Access to Information and Protection of Privacy Act*, RSY 2002, c. 1

b. Personal Information Protection Laws that Apply to Private Sector Organizations:

Federal	*Personal Information Protection and Electronic Documents Act*, SC 2000, c.5
Federal	*Digital Privacy Act*, SC 2015, c. 32 (Bill S-4) [*partly not yet in force*]
Federal	*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 [*referred to as the "Canadian Anti-Spam Law", or "CASL"*]
Alberta	*Personal Information Protection Act*, SA 2003, c. P-6.5
British Columbia	*Personal Information Protection Act*, SBC 2003, c. 63
Manitoba	*Personal Information Protection and Identity Theft Prevention Act*, SM 2013, c. 17, s. 34(2) [*not yet in force*]
Quebec	*An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR, c. P-39.1

© Dolden Wallace Folick LLP

c. Provincial Personal Health Information Laws:

Alberta	*Health Information Act*, RSA 2000, c. H-5
British Columbia	*E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c. 38
Manitoba	*Personal Health Information Act*, CCSM, c. P33.5
New Brunswick	*Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05
Nova Scotia	*Personal Health Information Act*, SNS 2010, c. 41
Newfoundland & Labrador	*Personal Health Information Act*, SNL 2008, c. P-7.01
Ontario	*Personal Health Information Protection Act, 2004*, SO 2004, c. 3
Québec	*An Act Respecting the Sharing of Certain Health Information*, CQLR C. P-9.0001
Saskatchewan	*Health Information Protection Act*, SS 1999, c. H-0.021
Yukon	*Health Information Privacy and Management Act*, SY 2013, c. 16 [*not yet in force*]

d. Provincial Laws Creating Cause of Action for Breach of Privacy:

British Columbia	*Privacy Act*, RSBC 1996, c. 373
Manitoba	*Privacy Act*, CCSM, c. P125
Newfoundland & Labrador	*Privacy Act*, RSNL 1990, c. P-22
Saskatchewan	*Privacy Act*, RSS 1978, c. P-24

© Dolden Wallace Folick LLP

© Dolden Wallace Folick LLP