CANADIAN PRIVACY CLASS ACTIONS AT THE CROSSROADS

Lisa Talbot, Molly Reynolds, and Eliot Che

Abstract: Canadian privacy law, particularly as it relates to class proceedings, is in its infancy. But this jurisprudential void is beginning to fill as an abundance of privacy class actions proceed through Canadian courts. These class actions are emerging as a result of new technologies and business practices, as well as jurisprudence developing in the United States. This article canvasses the growth of privacy class action litigation in Canada, focusing on the three sources of privacy class actions — claims challenging business practices, claims arising from accidental breaches, and claims relating to targeted conduct — and issues around harm and damages in light of recent American precedents and Canadian statutory reforms.

CANADIAN PRIVACY CLASS ACTIONS AT THE CROSSROADS

Lisa Talbot, Molly Reynolds, and Eliot Che*

A. INTRODUCTION

Canadian privacy class actions are on the rise, emerging from a wealth of new technologies, novel business practices, and an ever-growing body of jurisprudence south of the border. As privacy class actions find their place in Canadian law, the question is no longer whether or when they will take hold but rather where they are going. This article canvasses the developing jurisprudence surrounding privacy class action litigation in Canada, including the circumstances in which privacy claims arise, issues around harm and damages, and the potential for ongoing influence from American precedents.

B. SOURCES OF PRIVACY CLASS ACTIONS

Privacy class actions largely fall into three categories: (1) claims that challenge a corporation's business practices, (2) claims that arise from accidental breaches, and (3) claims relating to intentional, targeted conduct.

The legal and strategic considerations involved in each category of claims will likely differ. For example, the targeted hacking of a company's server can be costly to an organization's reputation and bottom line. However, such harm may not affect the organization's underlying business model. On the other hand, a challenge to an organization's business practices could affect the viability of the business as a whole.

---

* Lisa Talbot, Molly Reynolds, and Eliot Che are lawyers at Torys LLP. Lisa practises civil litigation with a focus on privacy, employment, and class actions. She heads the firm's Privacy Practice and co-heads the firm's Pensions and Employment Litigation Practice. Molly practises civil litigation with a focus on corporate and commercial, privacy and anti-spam, administrative law, e-discovery, and class actions. Eliot practises civil litigation with a focus on corporate and commercial, privacy, intellectual property and technology, administrative law, and class actions. The authors thank Ryan Roberts for his assistance with this article.

Inadvertent or intentional conduct by employees may lead to claims of vicarious liability against their employers. Although these categories are discussed separately below, organizations that collect, use, or disclose sensitive customer information in the ordinary course should develop comprehensive privacy policies, practices, and infrastructure that aim to prevent and defend against both the risks associated with business practice challenges and mishap- and crime-based breaches.

C. CLASS ACTIONS CHALLENGING BUSINESS PRACTICES

Canadian privacy class actions challenging business models and practices relating to the handling of personal information have seen mixed results. Class action jurisprudence challenging corporate privacy practices is still limited: although courts are increasingly willing to find that privacy claims meet the low bar for certification, few proceedings to date have been decided on their merits.[1]

Online services or products that actively encourage users to provide, use, and share personal information — notably social media companies — are particularly exposed to this type of claim. Litigants have claimed that a company's use or disclosure of personal information has exposed them to harms such as identity theft, harassment, embarrassment, and mental distress.[2] Legal claims have been brought on the basis of a reasonable expectation that businesses will protect customers' personal information, a company's alleged contravention of its own privacy policy, the alleged collection, use, or disclosure of personal information without consent, and assertions that a company diverted users' private data to third parties for profit. A selection of recent cases in these last two areas is discussed below.

1) Claims Based on Use or Disclosure of Personal Information without Consent

In 2011, Internet subscribers in *Union des consommateurs c Bell Canada*[3] unsuccessfully proposed a class action in Quebec against Bell Canada in relation to Bell's alleged practice of bandwidth throttling (the slowing of Internet speeds for certain uses). The claim challenged the use of a technol-

1 See, for example, *Albilia v Apple Inc*, 2013 QCCS 2805.
2 See, for example, *Silvestri v Facebook, Inc*, C10-00429 (ND Cal 2010).
3 2011 QCCS 1118.

ogy called "deep packet inspection" to collect the content of data transmitted by subscribers using Bell's Internet service. The Quebec Superior Court found that deep packet inspection was used only for traffic management rather than to inspect the contents of the data and thereby declined to authorize the class action, which had been framed on privacy grounds.

More recently, in 2015, the British Columbia Court of Appeal reversed a lower court's decision to certify the class in *Douez v Facebook, Inc*.[4] Douez had challenged Facebook's practice of promoting and earning revenue from "Sponsored Stories." The plaintiff claimed that Facebook had used the names and profile images of users in advertisements sent to the users' contacts without their knowledge or consent and contrary to British Columbia's privacy legislation. The terms of use for the social media site stated that any disputes must be settled in California whereas British Columbia privacy legislation provided that an action under the *Privacy Act* must be heard and determined by the courts of British Columbia. The motion judge dismissed Facebook's claim that the court lacked jurisdiction, stating that online terms of use for foreign-run social media services do not override the protections of British Columbia's *Privacy Act*.

The Court of Appeal, deciding the case on conflict of law principles rather than on privacy principles, disagreed with the motion judge, holding that the forum selection clause should be enforced. Relying on the principle of territoriality, the Court of Appeal held that British Columbia law applies only in British Columbia and does not affect the law of other jurisdictions subject to specific recognition by a foreign court or legislature,[5] and there was no such recognition of British Columbia law in California in this case. Therefore, the court held that Douez was free to pursue her claim in California.

2) Claims Alleging Personal Information Diverted to Third Parties for Profit

In 2013, the Quebec Superior Court authorized a class action alleging that Apple Inc collected iPhone and iPad users' personal information and disclosed that information to third parties without customer consent.[6] The court limited the class to affected residents of Quebec, given the petitioner's reliance on the Quebec *Charter of Human Rights and Freedoms* and

4 2015 BCCA 279, rev'g 2014 BCSC 953.
5 *Ibid* at para 73.
6 *Albilia v Apple Inc*, 2013 QCCS 2805.

Civil Code of Québec. The plaintiff did not seek damages for the breach of privacy itself and did not claim misuse of the collected personal information. However, the plaintiff alleged that the class members' devices were substantially devalued, both in sale value and available resources (such as battery life and data storage), by Apple's collection and disclosure of data to third parties without knowledge or consent. The case remains pending before the Superior Court.

In 2014, a class action was launched in the Ontario Superior Court alleging that Facebook illicitly intercepted and scanned users' private messages without their knowledge or consent for the purpose of tracking website links in the messages to inflate its web presence and attract advertising revenue (e.g., if a user shared a website link in a private message, this would be reflected as a "like" by the user on that website address).[7] The proposed class action, which has not yet been certified, alleges that Facebook's Data Use Policy did not disclose that private messages would be used in this manner; rather, the policy stated that the private messages would be private. Facebook ceased the practice in October 2012 without public announcement. Nonetheless, the suit contends that the proposed class should include all Canadian-resident Facebook users who sent or received private messages containing website links up to the date on which the practice was discontinued.

As the largest social media network with over 1.44 billion monthly active users,[8] it is not surprising that Facebook has been the target of multiple class actions in Canada and abroad. Following the trend of Canadian tagalong class actions seen in other areas of litigation, the Sponsored Stories challenge began as a class action in the United States. In 2013, the District Court for the Northern District of California approved a US$20 million settlement to be distributed among American class members, resulting in recovery of approximately US$15 per class member who filed a claim.[9]

In another recent example, a US class action was commenced against iPhone app developers (such as Path, Twitter, and Electronic Arts), alleging that they engaged in intrusion upon seclusion and violated privacy by uploading users' address books and calendar information to company servers without knowledge or consent. In a 2014 decision, the Ninth Circuit allowed the claim to proceed, stating that "the court does not believe

7 *Latham v Facebook* (9 April 2014), Toronto CV-14-501879 (Ont SCJ).

8 Facebook Inc, "Company Info" (31 March 2015), online: Facebook Newsroom http://newsroom.fb.com/company-info/.

9 *Fraley v Facebook Inc*, 966 F Supp 2d 939 (ND Cal 2013).

that the surreptitious theft of personal contact information . . . has come to be qualified as 'routine commercial behavior.'"[10] It would not be surprising to see a similar claim commenced in Canada, or other jurisdictions worldwide, especially given the gradual expansion of the tort of intrusion upon seclusion in Canadian common law.

D. CLASS ACTIONS ARISING FROM MISHAPS

From misplacing a hard drive to the inadvertent transmission of customer information, accidental privacy breaches and consequent class actions often result from mishaps by employees or contractors.[11] For example, in 2008, a class of plaintiffs alleged that they had provided DaimlerChrysler Financial Services Canada with confidential personal information that was stored on a data tape and later lost in transit when the tape was shipped to a credit reporting agency via the United Parcel Service.[12] A class action was then proposed in the Quebec Superior Court in respect of the alleged privacy breach. In January 2015, the court authorized the class, holding, among other things, that the facts alleged provided an arguable case that the mishandling of the delivery and the consequences of the loss of the data tape constituted an illicit and intentional violation of the right to respect for one's private life as protected by the Quebec *Charter of Human Rights and Freedoms*.[13]

Similarly, and as discussed by Barry Glaspell and Daniel Girlando in the following article in this issue,[14] the Ontario Superior Court certified a $40 million class action in 2011 after a public health nurse lost an unencrypted USB flash drive containing confidential information about 83,524 individuals who had been vaccinated against the H1N1 flu virus.[15] The court approved a settlement in 2012 in which each class member was to be compensated for demonstrable economic harm as determined by an adjudicator.[16]

---

10 *Opperman v Path, Inc*, 2014 US Dist LEXIS 67225 (ND Cal).

11 See, for example, *MacEachern v Ford Motor Company of Canada, Ltd and John Doe Corporation* (31 January 2013), CV-13-18955-CP (Ont SCJ); *Doe v AOL, LLC*, 2010 US Dist LEXIS 14639 (ND Cal).

12 *Waters v DaimlerChrysler Financial Services Canada Inc*, 2009 SKQB 263.

13 *Belley v TD Auto Finance Services Inc*, 2015 QCCS 168.

14 Barry Glaspell & Daniel Girlando, "The Rise of Personal Health Information Class Actions" 47, in this issue.

15 *Rowlands v Durham Region Health*, 2011 ONSC 719.

16 *Rowlands v Durham Region Health*, 2012 ONSC 3948.

In December 2012, a USB flash drive containing the personal information of over 5,000 individuals was misplaced by an employee of Human Resources and Skills Development Canada (HRSDC). The personal information included each person's birthplace, social insurance number, medical information, occupation, level of education, and local Service Canada processing centre. During the Privacy Commissioner of Canada's probe of the matter, the commissioner discovered that HRSDC had also misplaced an unencrypted external hard drive containing the personal information of approximately 583,000 student loan borrowers. The personal information included each borrower's name, birthdate, address, student loan balance, and social insurance number, as well as information about some students' family members.

As a result of the mishap, several class actions were commenced in provinces across Canada. Most were eventually consolidated into a single proposed class action before the Federal Court in *Condon v Canada*.[17] The court certified the class in March 2014. The claim in *Condon* alleges that the federal government is liable for the tort of intrusion upon seclusion by failing to adequately protect personal information in its possession. The plaintiffs claim that the government failed to comply with both the appropriate policies relating to encryption and physical security and the treasury secretariat and privacy commissioner's recommendation that any loss of sensitive data be disclosed as soon as possible. In certifying the class proceeding, the court noted that frustration and anxiety might meet the threshold of "distress" required for a successful privacy breach claim. However, the court held that there was no evidence to indicate that the individuals affected by the loss of personal data were at increased risk of identity theft. The plaintiffs had not availed themselves of any credit-monitoring services, and reports from credit reporting agencies did not indicate any increase in criminal activities involving the plaintiffs' personal information. Therefore, the plaintiffs' claim for compensable damages was dismissed, leaving them to pursue nominal damages for any breach.

However, contrary to the trend of ever-lowering thresholds for certification in Quebec and elsewhere in Canada, the Quebec Superior Court declined to authorize a class action against the Investment Industry Regulatory Organization of Canada (IIROC) in August 2014.[18] After IIROC reported that it had lost a USB flash drive containing the personal

17 2014 FC 250 [*Condon*].

18 *Sofio c Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2014 QCCS 4061 [*IIROC*].

information of approximately 50,000 individuals with accounts at over thirty brokerage firms, a class action was filed claiming $1,000 for each individual. In refusing to authorize the class, the court found insufficient evidence of any real damages sustained by the representative plaintiff.

Privacy class actions have also been triggered by the improper disposal of personal information. In 2014, a Missouri health clinic deposited personal medical billing records in a dumpster. Those records later blew out of the dumpster into the surrounding neighbourhood, and a class proceeding was commenced. In November 2014, the clinic and 1,532 patients reached a settlement agreement for US$400,000.[19]

Businesses should have in place policies concerning the handling of customer information. While it goes without saying that hard copies of documents should be properly destroyed before disposal, organizations transporting confidential information on portable electronic storage devices should also implement appropriate encryption safeguards. The Office of the Privacy Commissioner of Canada has issued guidelines for organizations responding to privacy breaches,[20] and government agencies such as Employment and Social Development Canada (ESDC, formerly HRSDC) have introduced new policies to prevent subsequent breaches. Consistent with many private sector companies, ESDC's security policy now bans the use of portable hard drives and prohibits unapproved USB flash drives from being connected to the computer network.[21]

E. CLASS ACTIONS ARISING FROM CRIME

Privacy breaches may also result from intentional activity, such as the theft of portable devices containing confidential personal information[22]

19 *Shorts v Midwest Women's Healthcare Specialists, LLC* [Settlement Agreement] (25 November 2014), Jackson County 1416-cv13362 (Mo Cir Ct), online: https://secure.dahladmin.com/MWHS/content/documents/Settlement.pdf.

20 Office of the Privacy Commissioner of Canada, "Guidelines: Key Steps for Organizations in Responding to Privacy Breaches" (August 2007), online: www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf.

21 See Jim Bronskill, "Federal Agency Loses Personal Data on More Than 500,000 Student Loan Borrowers" *Globe and Mail* (12 January 2013), online: www.theglobeandmail.com/news/politics/federal-agency-loses-personal-data-on-more-than-500000-student-loan-borrowers/article7288222/.

22 See, for example, *Ruiz v Gap, Inc*, 2010 WL 2170993 (9th Cir) [*Ruiz*]; *McLoughlin v People's United Bank Inc and Bank of New York Mellon, Inc*, 2009 US Dist Lexis 78065 (D Conn) [*McLoughlin*]; *In Re Department of Veterans' Affairs (VA) Data Theft Litigation*, 653 F Supp 2d 58 (D DC 2009); *Bordoff v Gestion d'actifs CIBC Inc/CIBC Asset Management Inc*, 2010 QCCS 4841.

and the disclosure of customers' email addresses to third parties who later send spam.[23] Many recent privacy class actions have arisen from intrusions into the computer systems of high-profile retailers such as The Home Depot, Target, and Sony Online Entertainment.[24] Additionally, recent jurisprudence south of the border suggests that there may be a necessary distinction between circumstantial breaches and breaches resulting from targeted hacking.

1) Circumstantial Breaches

As demonstrated by the cases described above regarding accidental data loss, a breach may be circumstantial where there is no evidence of who, if anyone, had access to the lost information, what use, if any, was made of the information, and whether any harm suffered by the plaintiffs can be linked to the mishap. In *Larose c Banque Nationale du Canada*, the Quebec Superior Court authorized a class action after the bank had had three laptops stolen in Montreal, one of which contained personal information of approximately 225,000 mortgagors.[25] The court emphasized the plaintiff's evidence of actual identity theft and noted that under Quebec law, a mere fear of identity theft or fraud is not a sufficient harm on which to ground a claim for damages.

2) Targeted Hacking

The evidentiary hurdles inherent in circumstantial breach claims may be easier to overcome in cases arising out of targeted hacking, at least at the certification stage. A number of privacy class actions have recently been commenced and certified, settled, or dismissed after hackers targeted the computer servers and systems of large retailers and commercial service providers.

In September 2014, two proposed class actions were commenced against The Home Depot, one in Ontario and the other in Quebec. The company's computer systems had suffered a security breach compromising payment information such as names, credit card numbers, expira-

23 See *In Re TD Ameritrade Accountholder Litigation* (1 May 2009), C-07-2852-VRW (ND Cal); *Cherny v Emigrant Bank*, 604 F Supp 2d 605 (SD NY 2009).

24 See *Maksimovic v Sony of Canada Ltd*, 2013 ONSC 4604 [*Sony*]; *Theriault v The Home Depot, Inc* (22 September 2014), Montreal 500-06-000711-149 (Que Sup Ct) [*Theriault*]; *Lozanski v The Home Depot, Inc* (22 September 2014), Toronto CV-14-512624-00CP (Ont SCJ) [*Lozanski*]; *Zuckerman v Target Corporation* (13 March 2014), Montreal 500-06-000686-143 (Que Sup Ct) [*Target* 1].

25 2010 QCCS 5385 [*Larose*].

tion dates, verification value codes, and purchase information, as well as email addresses. The breach affected customers in Canada and the United States who had used credit and debit cards in-store from approximately April 2014 onward. The proposed class action in Ontario claims over $1 billion in general, special, punitive, and aggravated damages, in addition to an order that the company fund a court-supervised credit-monitoring program (although, as an increasingly common component of breach response plans, The Home Depot has offered Equifax credit monitoring free for one year to all customers who claimed — without requiring evidence — to be affected). The statement of claim indicates that the proposed representative plaintiff suffered actual damages when he attempted to make a credit card purchase and learned that $8,000 in unauthorized purchases had already been charged to the account.[26] The Quebec claim does not indicate that the class suffered actual harm but alleges that the petitioner faces an imminent and certainly impending threat of future harm due to an increased threat of identity theft and fraud.[27]

In March 2015, the Superior Court dismissed a proposed class action commenced against Target Corporation in Quebec.[28] The company's point-of-sale computer network, which processes retail transactions, had been breached affecting the personal information of between 70 and 110 million individuals and payment information of about 40 million individuals, including approximately 700,000 Canadians as a result of their purchases while in the United States.[29] The compromised information included names, phone numbers, mailing addresses, email addresses, credit and debit card numbers, encrypted PINs, expiration dates, and magnetic stripe information. The claim did not allege that actual damage had been suffered apart from "fear, inconvenience, expenses, and/or

26 *Lozanski*, above note 24. See also The Home Depot, "Customer Update on Data Breach," online: The Home Depot https://corporate.homedepot.com/mediacenter/pages/statement1.aspx.

27 *Theriault*, above note 24.

28 *Zuckerman v Target Corporation*, 2015 QCCS 1285 [*Target* 2].

29 See *Target* 1, above note 24. See also Target Corporation, "Data Breach FAQ," online: A Bullseye View https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888. A $10 million settlement in the privacy class action filed against Target in the United States has received preliminary approval, with a final hearing taking place November 2015. The proposed settlement would pay affected customers up to $10,000 each for demonstrated damages: Hiroko Tabuchi, "$10 Million Settlement in Target Data Breach Gets Preliminary Approval" *New York Times* (19 March 2015), online: www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html.

loss of time due to the loss of their personal and/or financial information, which has made [class members] potential targets for fraud and/or identity theft."[30]

In granting Target's motion to dismiss the class proceeding, the court noted that the breach had been restricted to Target's activities in the United States and had not involved activities in Quebec. Target's motion to dismiss the action was thereby granted on the basis of *forum non conveniens*. The court also noted that the prejudice allegedly sustained by the plaintiff did not constitute compensable damages in this particular context.[31] Citing the Supreme Court of Canada, the Quebec court held that

> [w]ith the advent of computers and the Internet, the ever increasing use of technology in business transactions, online or in store, the use of electronic devices to effect a payment with a credit or debit card and the proliferation of people who unfortunately use the technology and Internet in their attempt to defraud others, the "*inconveniences*" described by Zuckerman fall in the category of "*ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept.*"[32]

In 2013, Sony settled a class action commenced after its gaming network had suffered a targeted hacking breach.[33] The breach exposed approximately 77 million user records (including those of 1 million Canadian users) including customers' credit and debit card information, names, mailing addresses, email addresses, birthdates, usernames, passwords, security questions, usage history, and other related information. While the class action had claimed over $1 billion in combined damages, the Ontario Superior Court eventually approved a settlement of $1 million for Canadian users. The settlement provided class members with one free game or a discount on future Sony subscription services for three months. In approving the settlement, the court noted that there had been no improper use of customers' personal information resulting

30 *Target* 1, above note 24 at para 74.

31 *Target* 2, above note 28 at paras 25–29 and 34–35.

32 *Ibid* at para 42 [emphasis in original].

33 See *Sony*, above note 24. See also Sebastian Moss, "Sony Settles Class Action Lawsuit: Over $1 Million in Free Games, Themes and PS+ Discounts Available for Canadians" *PlayStationLifeStyle.net* (18 April 2013), online: PlayStationLifeStyle.net www.playstationlifestyle.net/2013/04/18/sony-settles-class-action-lawsuit-over-1-million-in-free-games-themes-and-ps-discounts-available-for-canadians/.

in identity theft and that there was no evidence any credit card payment information had been accessed.

The aforementioned class actions indicate that both class counsel and Canadian courts recognize the difficulties inherent in proving damages from data breaches. The cases are also indicative of the litigation risks companies face even when data breaches are caused by third parties' actions. Negligence in developing and maintaining adequate security measures is often alleged in data breach litigation. Other actions have alleged the breach of an express or implied contractual term with respect to safeguarding personal information in the agreement between the business and consumer. The focus of the claim may also be on the subsequent delay in notifying customers and appropriate authorities, thereby preventing the possible mitigation of harm resulting from the breach.

In Re Heartland Payment Systems, Inc arose from one of the largest data breaches ever reported.[34] Hackers used malware to breach Heartland's computer network in 2007 exposing approximately 130 million credit and debit card numbers, along with corresponding personal information. The United States–based payment processor was then subject to seventeen consumer class actions and ten credit company and bank class actions. The claimants alleged that Heartland had failed to detect the security breach until alerted by credit card companies, had delayed notifying customers, and had not offered affected individuals credit-monitoring services or other relief. The hackers were eventually convicted on criminal fraud charges. Heartland later settled with the major credit card companies for US$100 million and with consumers for US$4 million.

The number and scope of proposed privacy class actions continue to expand in Canada. Outside of the data breach context discussed in this article, intentional misuse of corporate and customer information by employees is continuing to prompt litigation against both the perpetrators and their employers.[35] Similarly, privacy class actions in the health care context are on the rise.[36]

F. WHAT CONSTITUTES REAL DAMAGE?

Particularly with respect to privacy class actions arising from crime or mishap, not every breach will result in monetary relief: a breach does not necessarily lead to compensable harm. Whereas the plaintiffs in *Larose*

34 (12 April 2012), Houston 4:09-MD-2046 (SD Tex).

35 See, for example, *Evans v The Bank of Nova Scotia*, 2014 ONSC 2135.

36 See Glaspell & Girlando, above note 14.

demonstrated a link between the laptop theft and actual harm, in *IIROC* no actual harm was alleged from the loss of the USB flash drive. Accordingly, the court declined to authorize the *IIROC* action.

1) Developments in US Jurisprudence regarding Actual Harm

Historically, a number of American class actions were unsuccessful because of an inability to prove actual harm or "injury-in-fact," including "certainly impending" harm.[37] The Supreme Court of the United States, in *Clapper v Amnesty International USA*,[38] recently affirmed the standard for determining whether an injury-in-fact, which provides a party with standing before the court, occurred. In this case about government wiretapping of communications involving individuals located outside the United States, the plaintiff human rights and media organizations claimed "an objectively reasonable likelihood" that their communications would be acquired by the government at some point in the future. The Supreme Court held that the standard requires that the threat of harm be certainly impending — "'[a]llegations of possible future injury' are not sufficient."[39] Thus the Court found that the plaintiffs' fears were "highly speculative" and based on a "highly attenuated" chain of events that did not result in a certainly impending injury.[40]

However, a recent order by the District Court for the Northern District of California suggests a novel approach to the requirement of demonstrable harm. *In Re Adobe Systems, Inc Privacy Litigation* arose out of an intrusion into Adobe's computer network that resulted in a data breach.[41] In July 2013, hackers gained access to Adobe's servers, spending several weeks undetected collecting the personal information of customers (and the source code for some of Adobe's products). The intrusion compromised information that included customer names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and email addresses. Further, Adobe disclosed that hackers had been able to use Adobe's own systems to decrypt customers' credit card numbers stored

37 See *Clapper v Amnesty International USA*, 133 S Ct 1138 (2013) [*Clapper*]. See also *Ruiz*, above note 22; *Allison v Aetna, Inc*, 2010 WL 3719243 (ED Pa); *McLoughlin*, above note 22; *Randolph v ING Life Insurance and Annuity Co*, 973 A 2d 702 at 710 (DC Ct App 2009).

38 *Clapper*, above note 37.

39 *Ibid* at 1141.

40 *Ibid* at 1148.

41 (4 September 2014), San Jose 13-CV-05226-LHK (ND Cal) [*Adobe*].

in an encrypted form. The court noted that independent researchers had determined that Adobe's security infrastructure was deeply flawed and did not meet industry standards.

The court distinguished *Clapper* from *Adobe* on the facts. The plaintiffs' claim in *Clapper* had depended on the future occurrence of a series of independent choices by the federal government and a court specializing in foreign intelligence, and the plaintiffs had not been able to demonstrate with any certainty that their particular communications would be intercepted: "the overall chain of inferences was 'too speculative' to constitute a cognizable injury."[42] In contrast, the court in *Adobe* found no need to speculate as to whether the plaintiffs' data on Adobe's servers had been stolen and what information had been taken. The plaintiffs alleged that hackers had deliberately targeted Adobe's servers and used Adobe's own systems to decrypt customers' credit card information, leading to an "immediate and very real" risk that the data would be misused. The court found the allegations sufficient to establish the injury-in-fact required for standing, asking, "why would hackers target and steal personal customer data if not to misuse it?"[43] The court noted that "to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact."[44]

2) Damages in Canadian Privacy Litigation

It is not yet clear whether the reasoning in *Adobe* will make its way north of the border, but it would not be surprising to see plaintiffs in proposed privacy class actions urging the adoption of a similar approach to allegations that stem from targeted hacking. However, such an approach would likely not alter the common law addressing circumstantial breaches, or breaches arising from mishaps. In fact, the court in *Adobe* specifically reviewed such types of cases. For example, if data tapes, among other articles, are stolen from a car, injury-in-fact requires that the thief recognize the tapes for what they are, obtain the equipment necessary to load the tapes, break the encryption, acquire the software necessary to read the data, and then misuse the data. This scenario mirrors the "highly attenuated" chain of events rejected in *Clapper*, and it

42 *Ibid* at 13.
43 *Ibid* at 17.
44 *Ibid* at 15.

is unlikely that victims of such a theft would have standing to sue under American law.

Therefore, the approach to actual harm may depend on the factual circumstances surrounding the breach. As it stands today, Canadian courts are moving in the direction of awarding modest "moral" damages when demonstrable economic damages are absent. For example, in an action before the Federal Court, an individual sued RBC Royal Bank for unauthorized disclosure of her personal financial information. During divorce proceedings between the plaintiff's husband and his ex-wife, the ex-wife subpoenaed records relating to all of the husband's accounts at the bank, including records relating to a credit card held jointly between the plaintiff and her husband. In producing the records, RBC breached the plaintiff's privacy resulting in "humiliation."[45] The court ordered RBC to pay the plaintiff $2,500 in moral damages.

In the leading case on the tort of intrusion upon seclusion, *Jones v Tsige*, a bank employee accessed the plaintiff's financial information without authorization 174 times over four years. The Ontario Court of Appeal noted that the plaintiff had suffered no economic damages, but nonetheless awarded her $10,000 in moral damages to "vindicate rights or symbolize recognition of their infringement."[46] The court found the intrusion to be highly offensive to a reasonable person and that it had caused distress, humiliation, or anguish. The ruling suggested that damages awards in such cases should be modest and within a conventional range congruent with "consistency, predictability and fairness." The court fixed the range at up to $20,000.[47]

3) Statutory Reforms Affecting Privacy Class Actions

Jurisprudence across the continent continues to mature, and privacy claims continue to be regularly pursued. It remains to be seen whether moral damages awards will find a stronger foothold or whether Canadian courts will distinguish between circumstantial and targeted breaches in the assessment of harm. However, proposed amendments to federal privacy legislation may influence judicial approaches to determining whether the risk of actual harm is sufficient to push a claim forward.

---

45 *Biron v RBC Royal Bank*, 2012 FC 1095 at para 43.

46 2012 ONCA 32 at para 75.

47 *Ibid* at paras 75 and 87–88.

The *Digital Privacy Act*[48] amends the federal *Personal Information Protection and Electronic Documents Act*[49] to require public and regulatory notification for breaches that create a "real risk of significant harm" to an individual. The amendment broadly defines "significant harm" to include bodily harm, humiliation, damage to reputation or relationships, loss of employment or business opportunities, financial loss, negative effects on one's credit record, identity theft, and damage to or loss of property. Notably, the presence of a "real risk" is to be determined by reference to the probability that the personal information has been or will be misused, the sensitivity of the personal information, and other factors that may be prescribed by regulation. These considerations are notably similar to those taken into account by courts at the certification stage of privacy class actions.

Privacy class action claims can almost certainly be expected to follow disclosure of a breach, even where no damage appears to have occurred. As the law develops, plaintiffs' counsel will be better positioned to determine what types of harm are sufficient to commence individual or class actions. With the *Digital Privacy Act* now enacted, lawyers may urge courts to adopt the prescribed statutory factors in considering whether a claim pleads a "real risk of significant harm" sufficient to certify a class action arising from a privacy breach.

G. LOOKING BEYOND THE CROSSROADS

Canadian privacy law, particularly as it relates to class proceedings, is in its infancy. However, this jurisprudential void is beginning to fill as an abundance of privacy class actions proceed through Canadian courts. While US law has long recognized invasions of privacy as tortious, Canada is only now moving in that direction, with only a few provinces following the American approach.[50]

Canada also continues to develop its statutory causes of action related to misuses of technology. Data breach privacy class actions in the United States are largely predicated on statutes such as the *Electronic*

48 SC 2015, c 32.

49 SC 2000, c 5 [*PIPEDA*].

50 See, for example, Michael Power, *The Law of Privacy* (Markham, ON: LexisNexis, 2013) at 202–3; Barbara McIsaac, Rick Shields, & Kris Klein, *The Law of Privacy in Canada* (Toronto: Carswell, 2000) (loose-leaf June 2015 supplement) at § 1.5.2.2; Allen M Linden and Bruce P Feldthusen, *Canadian Tort Law*, 9th ed (Markham, ON: LexisNexis, 2011) at 59.

Communications Privacy Act and the *Computer Fraud and Abuse Act*.[51] Although there is some provincial legislation amenable to similar actions — including the British Columbia *Privacy Act*[52] in certain limited circumstances as demonstrated by *Douez v Facebook, Inc* — the statutory patchwork is far from comprehensive. Canada's anti-spam legislation (CASL) is new, having come into effect only in 2014, and the private right of action it affords will not be available until 2017.[53]

Also in contrast to the United States, Canada has a sophisticated federal regulatory regime governing privacy under *PIPEDA*, which provides a relatively simple administrative process for complaints and remedies. Where *PIPEDA* applies, there may be an argument that class actions are simply not needed, are certainly not preferable, and should therefore not be certified. That being said, *PIPEDA* does not prohibit private action by individuals, and CASL explicitly authorizes such claims.

Although privacy class actions have indeed crossed the starting line in Canada, there remains much ground to travel. Issues of circumstantial breach, hacking, actual harm, and moral damages, as they approach the intersection of legislative change and the influence of American class action precedent, promise to generate further debate in the courts of Canadian law and public policy.

---

51 *Electronic Communications Privacy Act of 1986*, Pub L 99–508; *Computer Fraud and Abuse Act*, 18 USC § 1030.

52 RSBC 1996, c 373.

53 *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.