OIAA PROVINCIAL CONFERENCE

Cyber Liability

Date: February 4, 2015
Location: Metro Toronto Convention Centre

Prepared by:

Catherine A. Korte, Partner, McCague Borlack LLP

Laurie Murphy, Partner, McCague Borlack LLP

Cyber and Privacy Risks:

Catherine Korte and Laurie Murphy

Introduction

With the increasing interconnectivity of businesses to date, information is now exposed to a broad number of threats. Businesses need to ensure there is protection of information in order to prevent loss, unauthorized access or misuse. Businesses must have in place a process of assessing threats and risks to information and the procedures and controls to preserve the information. There are three guiding principles:

1. Confidentiality. Access to data must be limited to authorized parties.

2. Integrity. The data must be authentic and complete.

3. Availability. The data must be accessible, as needed, by those who are authorized to access it.

Class action litigation arising out of cyber and privacy risks is increasing in Canada. The cases involve a broad range of privacy and cyber risks including lost portable electronic storage devices, uploads to an unsecure website, improper disposal of computer equipment, unauthorized access and dissemination by rogue employees, cybercrime and business practices. More breaches, increased breach notifications, widespread media reports and growing concern about privacy rights have all likely contributed to the increase in class action proceedings. In addition, the recent recognition of a new tort for invasion of privacy by the Ontario Court of Appeal in 2012 has resulted in certification of privacy class actions based on the new tort. This paper will discuss examples of Canadian cyber and privacy cases which have been certified as class actions, cases that have settled, and cases that have been recently commenced as proposed class actions.

I. CERTIFICATION / RULE 21 MOTION DECISIONS

Evans* v. *The Bank of Nova Scotia (unauthorized access/dissemination)

In a decision released on June 6, 2014 in *Evans* v. *The Bank of Nova Scotia*,[1] the Ontario Superior Court of Justice certified a class action against The Bank of Nova Scotia and its employee in a case arising out of the employee's deliberate breach of customers' privacy rights. In this case, the employee, a Mortgage Administration Officer, admitted to accessing and printing customer profiles for individuals who had applied for mortgages and providing this confidential personal and financial information to his girlfriend, who then disseminated it to third parties for fraudulent and improper purposes. The bank identified 643 customers whose files were accessed by the employee and 138 customers had advised the bank that they had been the victims of identity theft or fraud. In this case, the bank offered a complimentary subscription to a credit monitoring and identity theft protection service to the 643 customers notified and compensated the 138 customers for their pecuniary losses.

As against the bank, the plaintiffs alleged breach of contract, negligence, the tort of intrusion upon seclusion, breach of fiduciary duty and of the duty of good faith, waiver of tort, and vicarious liability for its employee's conduct. Addressing the first requirement for certification, the court determined that the statement of claim disclosed causes of action in negligence, waiver of tort, breach of contract, as well as vicarious liability for the employee's tort of intrusion upon seclusion and breach of the duty of good faith. The test is whether it is 'plain and obvious' that the plaintiffs' claims would be unsuccessful against the bank and it does not involve a consideration of the merits of the case.

Notably, this was another class action[2] to be certified based on the new tort of "intrusion upon seclusion" which was first recognized by the Ontario Court of Appeal in *Jones* v. *Tsige*.[3] In *Jones*, the Court of Appeal set out the three elements required to establish the tort of intrusion upon seclusion:

---

[1] 2014 ONSC 2135 (CanLII).
[2] The other was *Condon* v. *Canada*, note 4.
[3] 2012 ONCA 32 (CanLII).

a) The defendant's conduct must be intentional (which could include recklessness);
b) The defendant must have invaded the plaintiff's private affairs or concerns without lawful justification; and
c) A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.

Proof of harm to a recognized economic interest is not an element of the cause of action. The court also stated that the damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum in the range of up to $20,000. In *Jones*, the court awarded $10,000 to the individual plaintiff (where records were accessed by one person and not disseminated).

In considering the relevant factors in determining vicarious liability on an employer, the court in *Evans* found that "the Bank created the opportunity for [the employee] to abuse his power by allowing him to have unsupervised access to customers' private information without installing any monitoring system" and "there is a significant connection between the risk created by the employer in this situation and the wrongful conduct of the employee."

The court also found that the plaintiffs who have suffered real pecuniary damages (for which the bank admitted responsibility) may be entitled to additional damages for emotional suffering, hardship and inconvenience. The court stated: "[t]his is a unique situation, where their personal financial records were distributed to third party criminals and where such confidential information has been used to steal their identity and commit fraud and has negatively affected their credit ratings." The court rejected the bank's argument that the plaintiffs' claim for damages for emotional distress would fail because they had not pleaded that they suffered a recognized psychiatric or psychological harm.

With respect to the claim for waiver of tort (recovery of disgorgement of profits as an alternative to a tort remedy), the court stated that it was "possible to infer that the Bank earned additional profits from its alleged wrongful conduct of failing to incur the costs necessary to ensure adequate supervision of its employees in order to protect customers' confidential information." The bank had argued that there was no causal connection between the wrongful conduct and the bank's profits.

***Condon* v. *Canada* - Student Loans** (lost hard drive)

On March 17, 2014, the Federal Court certified a class action against the federal government involving the loss of an external hard drive containing the personal information of 583,000 student loan program participants.[4] The unencrypted hard drive went missing from a filing cabinet in a Human Resources and Skills Development Canada office in Quebec. The information on the hard drive included names, dates of birth, addresses, student loan balances and social insurance numbers. In their statement of claim, the plaintiffs claimed damages for breach of contract, breach of warranty, the tort of intrusion upon seclusion, negligence, breach of confidence and violation of Quebec law. The court summarized the damages sought by the plaintiffs as falling into two categories: i) compensation for wasted-time, inconvenience, frustration and anxiety resulting from the data loss; and ii) increased risk of identity theft in the future. The plaintiffs also claimed punitive damages due to the delay in notification.

In this case, the court determined that the claim for the new tort of intrusion upon seclusion. recognized in *Jones* v. *Tsige*,[5] disclosed a reasonable cause of action and allowed this claim to proceed. The court also allowed the claim for breach of contract and warranty to proceed. However, the court held that it was plain and obvious that the claims based on negligence and breach of confidence would fail due to the lack of compensable damages.

The *Condon* case is a good example of the damages issues that arise in these types of cases, both here at the certification stage and later at a trial on the merits, where there are little or no damages. With respect to the breach of contract and warranty claim, the plaintiffs acknowledged that their claims were for very small sums but they submitted that nominal damages have long been awarded by Canadian courts in order to recognize a breach of contract, even if it does not have a clear economic impact, or if that impact cannot easily be assessed. The defendant argued that the plaintiffs had not properly alleged a basis in fact for damages and that nominal damages should never be awarded in a class action as only plaintiffs' counsel, not the plaintiffs, would stand to benefit financially from the outcome. While the court noted that the defendant advanced

[4] *Condon* v. *Canada*, 2014 FC 250 (CanLII) ("*Condon*").
[5] *Supra*, note 3.

"an interesting and strong argument on this point", it held that the plaintiffs' position, although novel in the context of a class proceeding is supported by sufficient authorities that it should be considered on the merit of the action. It also held that the court would be better positioned to rule on the issue of any disproportionate advantages in favour of the plaintiffs' counsel when it hears it on the merit.

With respect to the claim for negligence and breach of confidence, for which damages is an essential element, the court found that the pleadings and a summary review of the evidence revealed that the plaintiffs had not suffered compensable damages. The plaintiffs were not victims of fraud or identity theft and the evidence did not support a claim for increased risk of identity theft in the future. The plaintiffs had spent at most four hours over the phone seeking status updates from the Minister. The court followed the reasoning in the case of *Mazzonna* v. *DaimlerChrysler* where it was held that the potential for future damages for the plaintiff who had not yet been victim of identity theft or unsuccessful attempts to defraud "falls squarely within the field of 'speculation' and 'unverified hypotheses' and ought not to be considered in assessing whether there is a *prima facie* existence of damages".[6] The court also referred to the case law holding that damages are rarely awarded for "mild disruption" alone, but normally in conjunction with other more traditional heads of damages, which are not available in this case. It also noted that damages cannot be awarded for merely speculative injuries. It has been reported that the decision is under appeal.

***Hopkins* v. *Kay* – Peterborough Regional Health Centre** (alleged unauthorized access)

Another Ontario case, *Hopkins* v. *Kay*,[7] is a proposed class action involving an alleged breach of patients' privacy interests arising from improper access to their personal health records by hospital employees. The plaintiffs allege that approximately 280 patient records of the Peterborough Regional Health Centre were intentionally and wrongfully accessed by the hospital and seven hospital employees. The statement of claim as originally issued plead various causes of action including breach of the *Personal Health Information Act* ("PHIPA"), breach of a

[6] *Condon*, para. 75, quoting *Mazzonna* v. *DaimlerChrysler Financial Services Canada Inc*., 2012 QCCS 958 (CanLII) ("*Mazzonna*").
[7] 2014 ONSC 321 (CanLII) ("*Hopkins*").

confidentiality agreement, breach of contract, negligence, misfeasance and mismanagement, breach of trust and breach of fiduciary duty. The statement of claim was later amended to include only the tort of intrusion upon seclusion based on the allegation that the defendants wrongfully and intentionally accessed private medical information without the consent of the patient and disseminated it to third parties. The plaintiffs claim general damages including psychological damages and punitive and aggravated damages.

On January 31, 2014, the Ontario Superior Court of Justice dismissed the hospital's motion for an order to strike the claim as disclosing no cause of action and for an order that the court has no jurisdiction over the subject matter of the claim. The court rejected the hospital's argument that PHIPA, with its own administrative and enforcement scheme for the protection of personal health information, constituted a complete code which precluded the plaintiffs' common law claim for breach of privacy. The court also rejected the hospital's argument that the case of *Jones* v. *Tsige*, recognizing the new tort of breach of privacy, was not applicable as it dealt with Federal privacy legislation and should be confined to its facts. A notice of appeal to the Court of Appeal has been filed by the hospital.[8] The appeal is reportedly scheduled to be heard on December 15, 2014. This is an important decision on patients' privacy rights and remedies as a claim under PHIPA is limited to damages for actual harm up to $10,000.

II. SETTLED CLASS ACTIONS

***Wong* v. *TJX Companies, Inc*. – TJX/Winners/HomeSense** (cyber-attack)

This case arose from a cyber-attack on the computer systems of the TJX group of companies in December 2006 and was reportedly one of the largest computer security breaches in the United States. In *Wong* v. *TJX Companies, Inc*.,[9] the Ontario Superior Court of Justice granted an order dismissing the Ontario action in the context of the global settlement which involved class proceedings in the United States, Puerto Rico and six jurisdictions in Canada. The benefits under the settlement to the Canadian class members were essentially identical to the benefits

[8] *Hopkins* v. *Kay*, 2014 ONCA 514.
[9] 2008 CanLII 3421 (ON SC).

available to the class members in the other proceedings. Those benefits were credit monitoring, identity theft insurance and reimbursement for the replacement costs of drivers' licenses that were replaced during a defined time (where compromised), up to two vouchers for $30 each for class members who incurred out-of-pocket costs and/or lost time as a result of the intrusion (depending on documentation), a one time 15% off sales event and access to an ombudsman for a defined time period to answer questions in respect of card cancellations and credit theft.

Speevak* v. *Canadian Imperial Bank of Commerce (incorrect fax transmission)

In 2010, the Ontario Superior Court of Justice certified and approved a settlement in *Speevak* v. *Canadian Imperial Bank of Commerce*,[10] in an action commenced in 2005 involving the inadvertent disclosure of customers' personal information to third party businesses. The statement of claim asserted causes of action for breach of contract, breach of a duty of care and breach of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). There was no evidence that the disclosure of the confidential information resulted in identity theft or any direct financial loss to any class member. The terms of the settlement included a claims process whereby a class member would submit a claim form and had the option to accept an offer from CIBC or have the claim assessed by an independent arbitrator. The right to claim for identity theft was preserved. CIBC was to pay $100,000 to a registered charity. With respect to costs, CIBC was to pay the costs of the arbitration process (and class members' arbitration-related legal fees if arbitration award is higher than amount of CIBC's initial offer). CIBC was to pay class counsel $42,500 plus G.S.T. to the date of the mediation in 2007 and partial indemnity costs thereafter. CIBC could terminate the settlement and contest certification if more than five class members exercised their right to opt out of the proceeding.

***Jackson* v. *Canada* – Correctional Services** (lost address list)

The Ontario case of *Jackson* v. *Canada (Attorney General)*[11] involved a proposed class action brought by Correctional Services Canada employees at a federal prison in Kingston arising from

[10] 2010 ONSC 1128 (CanLII).
[11] 2006 CanLII 32311 (ON CA), allowing appeal from 2005 CanLII 23107 (ON SC).

circumstances in which an employee address list fell into the hands of the inmate population. The list, which included names, addresses, phone numbers and names of spouses, was later recovered and certain names and addresses had been highlighted. Following a motion to strike the claim and an appeal, the plaintiffs' claims in negligence, breach of privacy rights, breach of fiduciary duty and breach of the plaintiffs' rights under section 7 of the *Charter* were allowed to proceed. It has been reported that the action, commenced in 2004 and originally seeking $15 million, settled in 2010 on the basis that each of the more than 360 plaintiffs would receive at least $1,000 and could make a claim and receive up to $10,000 if they could establish they suffered serious psychological harm. The settlement also provided for the payment of the plaintiffs' legal costs estimated at over $140,000 and no admission of liability. It was also reported that the defendant agreed to review privacy protection at other facilities and provide their review and recommendations to the Privacy Commissioner for comment.

Rowlands* v. *Durham Region Health (lost device)

In 2011, the Ontario Superior Court of Justice certified a class action in this case concerning the loss of a digital memory USB key by a nurse employed by the Durham Regional Health Department.[12] Adding to the costs of the class action proceeding, both parties obtained expert evidence for the certification motion. While Durham Region largely consented, the court found that the proposed class action met all of the criteria for certification. The court held that without certifying the action as a class proceeding the class members would not reasonably be able to obtain access to justice. The USB key contained the unencrypted personal and confidential information of 83,524 individuals who received H1N1 shots. The plaintiffs' claims included negligence, breach of fiduciary duty, breach of confidence, breach of privacy and breach of statutory duty under the *Personal Health Information Protection Act* and punitive damages.

In 2012, the court approved a settlement whereby class members who consequently suffered economic loss could make a claim within a specified claim period and, if not satisfied with the

[12] 2011 ONSC 719 (CanLII); see also 2011 ONSC 2171 (CanLII) amending statement of claim and certification order.

Region's steps to mitigate any harm, could pursue the claim before a Claims Adjudicator.[13] The settlement also provided for the payment of costs to class counsel in the additional amount of $500,000 inclusive of taxes and disbursements, plus 25% of actual claims paid by the defendant in the future. In approving the settlement, the court considered the fact that no class member had claimed financial damage and the chance of success on the merits were quite low, relying in part on a similar case which was dismissed for failing to prove damages,[14] and the risks and costs of both the Region's intended motion for summary judgment and an ultimate trial. The court made a point of emphasizing that this case "would look far different if information from the lost USB key had been abused by a wrongdoer".

Maksimovic* v. *Sony of Canada Ltd. (cyber-attack)

In 2013, the Ontario Superior Court of Justice approved a settlement in this certified class action stemming from a cyber-attack on its online networks, including Sony PlayStation Network, which led to class actions in Canada and the United States.[15] Notice of the motion for court approval was sent to 3.5 million Canadian accountholders. As part of a "Welcome Back" package to accountholders, Sony provided benefits of free content and free or discounted subscriptions to online services. In addition, the settlement included reimbursement of account credit balances, online game and service benefits, reimbursement of up to $2,500 per claim for out-of-pocket expenses for class members who could demonstrate that they suffered identity theft, and class counsel fees of $265,000. The court noted that the settlement reflected the state of the law, including possible damages awards, for breach of privacy/intrusion upon seclusion and loss/denial of service claims.

III. RECENTLY ISSUED PROPOSED CLASS ACTIONS

Peoples Trust Proposed Class Action (cybercrime)

[13] 2012 ONSC 3948 (CanLII).
[14] *Mazzonna*, *supra*, note 6.
[15] 2013 CanLII 41305 (ON SC).

On November 18, 2013, a proposed national class action was commenced against Peoples Trust Company, an online banking firm arising from a privacy breach in which confidential personal information stored in an online application database was compromised by cybercriminals.[16] Peoples Trust notified 12,000 to 13,000 individuals who may have been affected after discovering the breach when its customers complained of phishing attempts. The action claims $13 million in damages.

Rouge Valley Proposed Class Action (alleged theft by rogue employee)

In June 2014, it was reported that the personal information of new mothers at Rouge Valley Health System was allegedly sold by two former employees to companies selling Registered Education Saving Plans.[17] Approximately 8,300 patients may be affected. A proposed class action has now been commenced seeking damages in the amount of $412 million which includes damages for breach of contract, breach of warranty, breach of confidence, intrusion upon seclusion, negligence, and conspiracy in the amount of $332 and punitive damages in the amount of $80 million plus undetermined expenses relating to costs incurred to prevent identity theft, as well as mental distress, frustration and anxiety.[18] Further reports indicate that 6,150 additional patients at Rouge Valley's Ajax and Pickering campus may be affected.[19] It has been reported that this case is on hold until the Court of Appeal ruling on whether the case of *Kay* v. *Hopkins* can go ahead.[20]

Montford Hospital Proposed Class Action (lost device)

On May 10, 2013, it was reported that a $40 million class action was commenced against the Ottawa's Montford Hospital arising from a lost USB key (memory stick) containing the

---

[16] Press Release at https://www.peoplestrustprivacyclassaction.com/press

[17] Joel Eastwood, "Privacy Commissioner contacting other hospitals after Rouge Valley data leak", Toronto Star, June 4, 2014.

[18] Joel Eastwood, "Rouge Valley faces $400M class-action lawsuit over privacy breach", Toronto Star, June 25, 2014.

[19] Joel Eastwood, "Rouge Valley hospital privacy breach affects 6,000 more patients", Toronto Star, August 27, 2014.

[20] Joel Eastwood, "Peterborough lawsuit to set precedent for Ontario patient privacy rights", Toronto Star, September 3, 2014; *Hopkins*, *supra* note 7.

confidential personal information of 25,000 patients. The unsecure USB key contained patient names, a summary of services received at the hospital and a code representing the health care provider. The class members allege breach of contract, negligence, breach of privacy and violations of hospital by-laws and the *Personal Health Information Protection Act*. They allege that the hospital was negligent in failing to ensure that the device was password protected and in failing to disclose the loss of personal information in a timely manner. The action claims damages to compensate patients for the costs related to preventing identity theft, mental distress and inconvenience, frustration and anxiety caused by the incident. The USB key was recovered and it is not known whether the information was accessed by any third parties.

***IIROC* Proposed Class Action** (lost device)

On April 30, 2013, the Investment Industry Regulatory Organization of Canada (IIROC) was served with a motion to authorize a class action in Quebec relating to the accidental loss of a portable device that contained personal information relating to clients of a number of investment firms.[21] It has been reported that the portable device, believed to be a notebook computer containing the personal information of about 52,000 clients, was password protected but not encrypted contrary to IIROC's policies which require two levels of security.[22] The class action lawsuit seeks $1,000 plus interest on behalf of each class member ($52 million based on 52,000 potential claimants) in relation to damages for stress, inconvenience and measures rendered necessary as a result of the loss of personal information. IIROC did not expect a ruling on this motion until late 2014.

The IIROC proposed class action is an example of the potential costs of a security breach on an organization. In its Annual Report 2012-2013, IIROC reported that the total costs for this incident were projected to be $5,208,000 which included credit alerts, credit monitoring and support costs provided to affected clients, professional services, a dedicated call center and other anticipated expenses.[23] At the time, IIROC also reported that it had received no reports of

[21] IIROC Annual Report 2012-2013, p. 40 ("IIROC AR").
[22] Barbara Shecter, "Lost IIROC device containing personal information of investors was not encrypted", Financial Post, April 19, 2013.
[23] IIROC AR, *supra*, note 21, pp. 39 and 64.

identity theft or fraud resulting from the loss of the portable device and "accordingly it is not possible to estimate the total amount of potential damages or range of possible loss, if any, resulting from settlements or other remedies in connection with this matter".[24]

MacEachern v. Ford Motor Company Proposed Class Action (posting to unsecure website)

A proposed class action was filed in Ontario in January 2013 against Ford Motor Company of Canada Limited and an identified vendor corporation after Ford notified employees that their personal information had been inadvertently posted to an unsecured website.[25] It has been reported that the names, addresses, phone numbers, birth dates and Ford seniority dates of 10,000 current and former Ford employees "were included in a data upload to a file on an external information technology vendor website". The statement of claim reportedly seeks $13 million in damages as well as an interim order for payment of credit monitoring services for the employees affected. The claim alleges that the defendants were negligent for letting the information become public and failing to destroy the personal information of former employees (one of the representative plaintiffs apparently retired in 2004). According to reports, Ford indicated that the information was immediately removed from the relatively obscure website upon discovery[26] (however there was no information provided on how long it was posted) and that there is no evidence there has been any misuse of the information.[27]

Business Practices Class Actions

On May 30, 2014, the British Columbia Supreme Court certified the action in *Douez* v. *Facebook*,[28] a class proceeding alleging that Facebook used the names and images of Facebook users, without their consent, for advertising in Sponsored Stories contrary to the provisions of British Columbia's *Privacy Act*. The size of the class was estimated to be over 1.8 million

[24] IIROC AR, *supra*, note 21, p. 40.
[25] Ellen van Wageningen, "Lawsuit filed over web posting Ford employees' private information", The Windsor Star, February 1, 2013.
[26] Ibid.
[27] "Class action lawsuit filed against Ford Motor Company", CTV Windsor, February 1, 2013.
[28] 2014 BCSC 953 (CanLII).

people. There is also a risk of class actions arising from the private right of action (to come into force on July 1, 2017) under Canada's Anti-Spam Legislation[29] (CASL) for non-compliance.

Conclusion

Privacy and security breaches and ensuing class actions can lead to significant legal, financial and reputational costs. The potential damages in a class action are significant considering the number of individuals affected by a single data breach. While some of the cases in Canada to date have resulted in minimal harm to class members and have settled for relatively nominal amounts, a number of other cases involve evidence of identity theft, fraud and other financial harm and, together with claims based on the new tort of intrusion upon seclusion, could result in a significantly increased risk of damages to larger groups.

The law in this area is still developing. The cases are still at early stages of litigation, where claims are permitted to proceed where it is not plain and obvious that they would fail, and have not been determined on the merits. However the current cases, including two appeals from certification decisions that are scheduled to be heard by an appellate court later this year, will provide additional guidance for future privacy and cyber risk claims.

[29] An Act to promote the efficiency and the 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, S.C. 2010, c. 23.