ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

EYE ON PRIVACY

Volume 12, No. 1 – August 2012 Privacy Law Section

## The New Face of Privacy in the Courts: Damages, Tort Claims and Class Actions

***By Alex Cameron[1] & Jesse Harper[2] and Fasken Martineau DuMoulin LLP***

In addition to understanding the Commissioner investigations, recommendations and orders that can flow from violations of privacy, it is now increasingly critical that counsel, individuals and organizations have a clear appreciation of how violations of privacy can give rise to damage awards, tort claims and class action litigation in the courts. Canadian courts have shown an increasing willingness to protect privacy interests in these areas. The landmark decision of the Ontario Court of Appeal in *Jones v Tsige*, 2012 ONCA 32, as well as Canada's forthcoming anti-spam legislation ("CASL")[3] (which contains a private right of action and statutory damages) are expected to further encourage such recourse to the courts. Potential risks and liabilities in these respects include not only the damages that might be awarded in a given case but also the tremendous reputational, lost opportunity and out-of-pocket costs and harms to organizations that are often associated with such claims. This short paper provides a brief overview of some of the recent developments that are changing the face of privacy in Canadian courts.

### Damage Awards Under PIPEDA

Pursuant to section 14 of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[4], a complainant may, after receiving a report from the Office of the Privacy Commissioner of Canada ("OPC") or upon being notified that the investigation of the complaint has been discontinued, apply to the Federal Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the OPC report, and that arises from certain sections of the legislation. The hearing is a *de novo* review akin to an action; it is not a judicial review of the OPC findings.

Section 16 of PIPEDA sets forth some of the remedies that the Court may grant following such a hearing. Subsection 16(c) in particular provides the Federal Court the discretion to award damages to a complainant, including an amount for any humiliation suffered. Until very recently, there were no cases in which the Court exercised its power to award damages. In a number of recent cases issued since 2010,

---

1 Alex Cameron is a lawyer with Fasken Martineau, practising in the areas of civil litigation and privacy law. He has acted as counsel in several landmark privacy cases, including most recently as counsel to the defendant in *Jones v Tsige*, 2012 ONCA 32, discussed in this paper. He has received high-profile commissions from the Office of the Privacy Commissioner of Canada and works with clients from a wide range of industries where privacy issues arise. Alex is currently the Chair of the Canadian Bar Association National Privacy & Access Law Section.

2 Jesse Harper is a Student-at-Law with Fasken Martineau in Toronto.

3 *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 E-1.6 [Assented to December 15, 2010]

4 SC 2000, c 5.

however, a damages framework has begun to emerge and in several cases the Court has awarded damages for violations of PIPEDA.

The Court will look at a number of factors to determine whether a damage award is appropriate under PIPEDA and, if an award of damages is appropriate, the quantum of damages that should be awarded. In general terms, the Court will consider in each case the alleged injury to the complaint, including the impact of the breach on the health, welfare, social, business or financial position of the complainant, the nature of the breach, and the organization's conduct before and after the breach.[5] In addition, the Court has held that it may consider whether damages should be awarded to deter future breaches or to further the general objects of PIPEDA.[6]

The Court has made clear that an award of damages is not to be made lightly and should only be made "in the most egregious situations …where the breach has been one of a very serious and violating nature such as video-taping and phone-line tapping, for example."[7] For example, in a case where a fitness club was found to have breached PIPEDA by disclosing (without consent) the frequency of the complainant's gym visits to the complainant's employer, the Court refused to award damages and instead held that the club's implementation of the OPC's recommendations was sufficient.[8] The complainant claimed that the disclosure had led his employer to retaliate against him. However, the Court characterized the situation as "the result of an unfortunate misunderstanding."[9] In refusing to award damages, the Court considered it relevant that:

> (a) the disclosure of personal information was "minimal";
>
> (b) there had been no injury to the complainant sufficient to justify an award of damages;
>
> (c) the club did not benefit commercially from the breach;
>
> (d) the respondent did not act in bad faith; and
>
> (e) there was no connection between the breach and the employer's alleged retaliation against the complainant.[10]

In addition, in assessing the conduct of the organization in breach of PIPEDA, the Court has held that it may consider the organization's response and steps taken *after* it was notified of the complaint:

> …an assessment of a respondent's conduct is appropriate when a court is exercising its discretion to award damages and in considering the quantum of damages. In examining the reasonableness of conduct where there has been a breach of the Accuracy Principle, it is appropriate that the Court be guided by a number of factors including the nature of the response to the complaint, the steps taken to investigate the allegation of inaccuracy, the steps taken to correct the information collected in an organization's own records, the

---

5 See generally *Girao v Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070 at paras 46-48.

6 *Ibid*.

7 *Randall v Nubodys Fitness Centres*, 2010 FC 681 at para 49. This principle has been adopted in subsequent cases: see e.g. *Nammo v TransUnion*, 2010 FC 1284.

8 *Randall v Nubodys Fitness Centres*, *ibid* at paras 47, 59. The OPC recommended that the club modify its procedures and documentation to ensure that it obtained members' consent to the collection, use and disclosure of their personal information. The club subsequently proffered evidence that it modified its forms to properly disclose the company's privacy policies and provided the updated forms to all affected individuals.

9 *Ibid*. at para 58.

10 *Ibid* at paras 49-51. See also *Nammo v TransUnion*, *supra* note 7 at para 71 where the court reviewed these factors. With respect to the final factor, see also *Stevens v SNF Maritime*, 2010 FC 1137.

> steps taken to correct false information the organization has provided to others, the steps taken to keep the individual informed of actions taken, and the timeliness of all steps taken.[11]

In the damages analysis, the above factors may also be weighed against any contributory fault of the complainant.[12]

In applying the above factors, the quantum of damages awarded by the Court in cases under PIPEDA to date has varied according to the particular facts of each case. The first case to award damages for a breach of PIPEDA, *Nammo v TransUnion*[13], dealt with a credit reporting agency that failed to maintain accurate personal information about the complainant and consequently released an inaccurate credit report to a potential creditor of the complainant. The Court ordered TransUnion to pay $5,000 to the complainant based on the humiliation suffered (noting that the nature of TransUnion's business was a relevant consideration, as demonstrated in the paragraph below), despite the fact that no actual loss had been shown:

> I am satisfied that in the circumstances experienced by Mr. Nammo it would be the exceptional person who would not be humiliated. He had partnered with a friend to undertake a business; his role was to secure financing because he was creditworthy while his friend was not, and the loan was approved subject to the credit check, which came back indicating that Mr. Nammo had poor credit. Mr. Nammo then had to inform his partner of this result. Although he said to his partner that the information was wrong, the credit reporting service said that it would take up to 30 days to investigate, during which time the opportunity and partnership were lost. In addition, RBC officials were provided with information that led them to conclude that the applicant was not a good credit risk. The reasonable person, knowing that the assessment made of his creditworthiness must be incorrect, would be humiliated at having to face and to protest to both his prospective partner and to bank officials. The reasonable person would suffer additional humiliation when the error was not clearly corrected by informing RBC and the credit applicant that an error was made, that there was no debt owed by the applicant, and that the error had been corrected.
>
> A credit reporting agency such as TransUnion would know that false information it provides showing a person to have unpaid debts would adversely affect that person's ability to secure a loan. It would also know that in such circumstances the person seeking credit would be humiliated when his credit application was rejected. Where the credit reporting service has failed to take prompt, reasonable steps to correct the record and to therefore ameliorate the embarrassment of the individual, it should expect that it will be ordered to compensate him for the humiliation it has caused. A credit reporting agency makes a profit from trading in the personal information of others. Such business, perhaps more so than others, ought to be aware of the need for accuracy and prompt correction of inaccurate information. Such businesses should expect to be held to account when they fail to do so.[14]

---

11 *Nammo v TransUnion, supra* note 7 at para 57. In *Landry v Royal Bank*, 2011 FC 687 at paras 28-32, the Court considered it relevant in awarding damages that the employee responsible for the breach had attempted to cover up her conduct after the fact.

12 *Landry v Royal Bank, ibid.*

13 *Supra* note 7.

14 *Ibid* at paras 68-69. The court agrees with the respondent that the complainant "failed to prove any loss arising from the failure to secure the loan and, in any event, has failed to mitigate any loss he may have incurred" at para 64.

In *Landry v Royal Bank*[15], the complainant was involved in divorce proceedings in which the opposing party issued a subpoena *duces tecum* to the complainant's bank, requiring a bank employee to appear before the Superior Court with the relevant documents and information. Prior to the appearance, however, the bank employee sent the information about the complainant's personal bank accounts directly to opposing counsel without the complainant's consent. The Court noted the humiliation suffered by the claimant and awarded $4,500 in damages, but refused to award exemplary damages.[16] The Court took into account the contributory fault of the complainant, who had "contributed to her own misfortune by attempting to conceal under oath the existence of her personal accounts even though she was obliged to disclose their existence."[17]

Finally, in *Girao v Zarek Taylor Grossman Hanrahan LLP*[18], a law firm posted on its website a final report issued by the OPC (which is not a publicly available document) following the investigation of a complaint that the complainant had made against a client of the firm. The report contained personal information about the complainant, including her name, although there was some dispute about whether much of the information was already made 'public' through disclosure in ongoing legal proceedings between the complainant and the client of the firm. In the result, however, the Court held that there had been a violation of PIPEDA and awarded $1,500 for mental anguish (plus costs of $500). The Court characterized the breach as "careless" and "negligent" and noted that a lack of bad faith and economic gain of the law firm tempered the award.[19] The Court also noted that when the law firm received notice of the complaint, it acted quickly to remove the posting from its website. Consideration was also given to the statutory limit on damages for mental anguish of $10,000 under the *Personal Health Information Protection Act*[20], though PIPEDA does not prescribe such a limit.

**Invasion of Privacy at Common Law in Ontario**

On January 18, 2012, the Ontario Court of Appeal issued its landmark decision in *Jones v Tsige*[21], recognizing for the first time in Ontario the tort of 'intrusion upon seclusion', a type of 'invasion of privacy'. The decision marks the first time a Canadian appellate court has recognized the tort.

The facts in the case involved a claim against an employee of a bank who periodically viewed a co-worker's banking records at work, without authorization, over a number of years. The defendant did not publish, distribute or record the information in any way. The defendant maintained that she was involved in a financial dispute with the plaintiff's former husband and accessed the information to confirm whether he was paying child support to the plaintiff.

The plaintiff became suspicious that the defendant was accessing her account and complained to the bank. The bank investigated the matter. Upon being confronted by the bank, the plaintiff admitted her conduct and acknowledged that it was contrary to the bank's policies. The bank disciplined the defendant. The plaintiff brought an action against the defendant for invasion of privacy and breach of fiduciary duty. The plaintiff brought a motion for summary judgment on the claim and the defendant brought a cross-motion for summary judgment. It is notable that the defendant apologized to the plaintiff and made genuine attempts to make amends.

---

15 *Supra* note 12.
16 *Ibid* at para 32.
17 *Ibid* at para 29.
18 *Supra* note 5.
19 *Ibid* at paras 59-61.
20 SO 2004, C 3, s 65(3).
21 *Jones v Tsige*, 2012 ONCA 32.

In the reasons on the motions for summary judgment, Whitaker, J. canvassed the jurisprudence and concluded that there is no freestanding tort of invasion of privacy in Ontario. The principal basis for that finding was the Ontario Court of Appeal's statement in *Euteneier v. Lee* that "…there is no 'free-standing' right to dignity or privacy under the *Charter* or at common law…"[22] That statement had not been squarely addressed in any privacy-related cases decided since *Euteneier*.

In addition, the defendant argued that the legislature, not the court, was the appropriate venue for making any decision(s) about whether and how to regulate privacy, particularly given the numerous stakeholder interests, complex economic and policy ramifications, and the tremendous amount of legislative activity that had already taken place with respect to privacy in Canada. Although those arguments were not ultimately determinative, Whitaker, J. considered the existence of the numerous legislative regimes to be a relevant consideration:

> Turning back now to the various statutory provisions that govern privacy issues, most Canadian jurisdictions have statutory administrative schemes that govern and regulate privacy issues and disputes. In Ontario, it cannot be said that there is a legal vacuum that permits wrongs to go unrighted - requiring judicial intervention. […]
>
> I would also note that this is not an area of law that requires judge-made rights and obligations. Statutory schemes that govern privacy issues are, for the most part, carefully nuanced and designed to balance practical concerns and needs in an industry-specific fashion.
>
> I conclude that there is no tort of invasion of privacy in Ontario.[23]

The plaintiff appealed the decision of Whitaker, J. to the Ontario Court of Appeal. The appeal was heard September 29, 2011.

On January 18, 2012, the Court of Appeal released its decision allowing the appeal and recognizing for the first time the tort of 'intrusion upon seclusion'. The Court held that the elements of the tort of 'intrusion upon seclusion' are as follows:

> (a) the defendant's conduct must be intentional (which includes reckless conduct);
>
> (b) the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and
>
> (c) a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.[24]

The Court stated that the protection of privacy will have to be reconciled with "competing claims" such as freedom of expression. In addition, the Court stressed that the tort will arise only for "deliberate and significant invasions" and that damages "will ordinarily be measured by a modest conventional sum". Following a review of privacy-related damage awards in Ontario and other jurisdictions, the Court set forth the following framework regarding damage awards in such cases:

> …damages for intrusion upon seclusion in cases where the plaintiff has suffered no pecuniary loss should be modest but sufficient to mark the wrong that has been done. I

---

[22] *Euteneier v Lee* (2005), 77 OR (3d) 621; 260 DLR (4th) 145 at para. 63 (CA).

[23] *Jones v Tsige*, 2011 ONSC 1475, 333 DLR (4th) 566 at paras 53-57.

[24] *Supra* note 21 at para 71.

> would fix the range at up to $20,000. The factors identified in the Manitoba Privacy Act, […] provide a useful guide to assist in determining where in the range the case falls:
>
> 1. the nature, incidence and occasion of the defendant's wrongful act;
>
> 2. the effect of the wrong on the plaintiff's health, welfare, social, business or financial position;
>
> 3. any relationship, whether domestic or otherwise, between the parties;
>
> 4. any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and
>
> 5. the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.
>
> I would neither exclude nor encourage awards of aggravated and punitive damages. I would not exclude such awards as there are bound to be exceptional cases calling for exceptional remedies. However, I would not encourage such awards as, in my view, predictability and consistency are paramount values in an area where symbolic or moral damages are awarded and absent truly exceptional circumstances, plaintiffs should be held to the range I have identified.[25]

The Court's historic decision has already been the subject of considerable commentary, analysis and debate. It is widely expected that the decision will have very significant and far-reaching ramifications across Canada. Many important questions remain unanswered, particularly in respect of claims and activities which are already subject to existing legislative regimes that regulate privacy. At the time of writing, neither party had sought leave to appeal the decision to the Supreme Court of Canada.

**The Rise of Privacy Class Action Litigation**

Following many years of significant activity in the United States, privacy-related class action litigation is on the rise in Canada.[26] While many claims, including actions against Internet, entertainment and social media giants, have either settled or do not appear to have been materially advanced, there can be many adverse consequences for organizations in managing, responding to and/or settling such claims and there are signs that more claims may proceed in future. In addition to the new potential for damage awards based upon 'intrusion upon seclusion', an increase in claims may result from an Ontario court's recent certification of a privacy-related class action suit in *Rowlands v. Durham Region Health et al*.[27]

In *Rowlands v. Durham Region Health*, the plaintiffs allege that a nurse employed by the Durham Region Health Department lost a USB thumb drive containing personal and confidential health information of over 83,500 patients. The thumb drive contained unencrypted private patient information relating to H1N1 flu vaccinations received during the period of October 23 to December 15, 2009.

The class action was brought following an investigation and Order by the Ontario Information and Privacy Commissioner, which cited a number of breaches of the *Personal Health Information Protection*

---

[25] *Ibid* at paras 87-88.

[26] See e.g. Sharon Gaudin, "Facebook slapped with class-action privacy lawsuit" *Computerworld* (July 8, 2010) online: <http://www.computerworld.com/>; Rob Tripp, "Corrections to pay victims of breach of privacy" The Whig-Standard (July 2010) online: <http://www.thewhig.com/ArticleDisplay.aspx?e=2729596&archive=true>.

[27] 2011 ONSC 719.

*Act* ("PHIPA")[28] by Durham Region Health in relation to this incident. Section 65(1) of PHIPA permits a party to commence a proceeding for damages for actual harm suffered as a result of a contravention of PHIPA.

The plaintiffs in the class proceeding seek $40 million in damages. One of the main bases for damages in the lawsuit is the risk that the confidential information contained in the USB drive might be used to facilitate identity theft.[29] The action is based in, among other things, negligence and breach of the statutory duty to protect patient information.

The court granted certification of the class proceeding pursuant to section 5 of the *Class Proceedings Act*, largely with the consent of the defendants. As a result of the defendants' consent to much of what could have been at issue on the certification motion, the court's reasons in respect of the section 5 certification test are very brief and, therefore, will not likely be of much assistance to parties in future contested certification motions in this area. Notably, however, the court held that without certifying the action as a class proceeding, the class members identified would not reasonably be able to obtain access to justice.[30]

While the merits of the lawsuit have yet to be determined, the case has potentially broad implications for organizations that collect, use and disclose personal information. The circumstances that gave rise to this case are not uncommon. For example, media reports indicate that a number of organizations in the health care sector have recently been alleged to have committed privacy related data breaches.[31] Similar privacy claims have arisen in contexts outside of the healthcare sector, as mentioned above. It remains to be seen what quantum of monetary damages is possible in such cases.

In light of the certification of *Rowlands v. Durham Region Health*, the availability of damage awards pursuant to the new tort of 'intrusion upon seclusion', and reports about the frequency and magnitude of data breaches and other violations of privacy, among other factors, many organizations are carefully monitoring and assessing the impact of the rise of privacy related class action developments in Canada. This interest has been heightened by the potential for claims and damages, including statutory damages, under Canada's new anti-spam legislation, CASL.[32]

In December 2010, the Canadian government passed 'anti-spam' legislation that will affect the interests of organizations that communicate and market electronically. The legislation has a broad scope, covering the sending of commercial electronic messages, altering of transmission data, installation of computer programs, sending of false or misleading representations, and address harvesting. The potential risk of monetary loss under the new legislation is extensive. CASL provides for administrative monetary penalties up to a maximum amount of $1,000,000 for an individual and $10,000,000 for an organization.[33] In addition to these administrative monetary penalties, CASL provides a private right of action for any person "affected" by any contravention of the legislation.[34] The legislation further introduces statutory damages (for example, damages of $200 for each contravention of certain messaging requirements, not exceeding $1,000,000 for each day on which a contravention occurred) that could result in damage

---

28 *Supra* note 20.

29 *Supra* note 27 at para 1.

30 *Ibid* at para 8.

31 See e.g., North Bay Regional Health Centre, News Release, "Breach of Privacy Occurs at North Bay Regional Health Centre Affecting 5,800 Patients" (6 September 2011) online: <http://www.nbdh.on.ca/media/default-e.aspx>; Stanford Hospital and Clinics, News Release, "Electronic Files and Patients' Personal Information Discovered and Removed From Web Site: Summary and Frequently Asked Questions" (12 September 2011) online: <http://stanfordhospital.org/newsEvents/>; Florida Hospital, News Release "We Are Notifying Our Patients" (29 September 2011) online: <http://www.floridahospital.com/News.aspx>.

32 *Supra* note 3.

33 *Ibid*, s 20(4).

34 *Ibid*, s 47.

awards that far exceed any loss actually suffered by the complainant.[35] These provisions in CASL are expected to lead to claims by both individuals and businesses that are affected by violations of CASL, with a heightened risk of class action litigation.

**Conclusions**

This short paper has highlighted some of the recent developments – damage awards, tort claims and class action litigation – that are changing the face of privacy in Canadian courts, including those changes to the law that may see increased recourse to the courts and that are being closely monitored by counsel, organizations and individuals alike.

[35] *Ibid*, s 51.