CANADIAN PRIVACY LAW REVIEW

Volume 11 • Number 1 December 2013

In This Issue:

Damages under *PIPEDA*: A Purposive Approach and a New High Water Mark

Neil Wilson
Stevensons LLP

The Federal Court's recent decision in *Chitrakar v. Bell* TV [*Chitrakar*][1] is a new high water mark for damages for breaches of privacy under the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*].[2] The $20,000 award may be a sign of increased damages to come under the *PIPEDA* regime and invites consideration of how damages are assessed under this unique and accessible system for addressing privacy breaches.

PIPEDA Applications in a Nutshell

PIPEDA aims to protect Canadians' personal information through the articulation of several "Principles" to be followed by organizations using personal information in the course of commercial activities.[3] The Principles include consent, accuracy, and openness, and each Principle contains subsections imposing related obligations that organizations are required to meet.

A complainant who feels a Principle has been breached may make a complaint to the Privacy Commissioner.[4] Upon receiving a complaint, the Commissioner must conduct an investigation and prepare a report containing findings and recommendations within one year from the date the complaint was made[5] unless the investigation is discontinued based on certain limited grounds.[6] The Commissioner has significant investigatory powers, including the power to issue summonses, require the production of records, and enter premises.[7]

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $255.00 (print or PDF)
$395.00 (print & PDF)

Once the Commissioner either issues a report or discontinues the investigation, the complainant may apply to the Federal Court for a hearing with respect to the complaint.[8] The hearing before the Federal Court is not in the nature of a judicial review or appeal but is a hearing *de novo* with no deference to the Commissioner's report. The court reaches its own conclusions regarding the respondent's conduct and breaches of *PIPEDA*.[9] However, as a practical matter, the Commissioner's report may serve as the groundwork for the court's inquiry.[10]

Upon an application under *PIPEDA*, the court is empowered to award damages to a complainant, including "damages for any humiliation that the complainant has suffered".[11]

Chitrakar v. Bell TV: A Quantum Leap in Damages

In *Chitrakar*, the applicant launched a complaint regarding, among other things, an unauthorized credit check conducted by Bell. After complaining directly to Bell and receiving what the court described as the "royal runaround",[12] Chitrakar filed a complaint with the Privacy Commissioner, followed by an application to the Federal Court. Bell did not respond to the application.

Justice Phelan determined that Bell had violated Chitrakar's privacy rights under *PIPEDA* and branded Bell's conduct "reprehensible".[13] Damages of $20,000 were awarded, comprising $10,000 in general damages and $10,000 in exemplary damages—the first time exemplary or punitive damages have been awarded under *PIPEDA*.

The award in *Chitrakar* is notable as both the largest damages award to date under *PIPEDA* and an affirmation of an approach to damages under *PIPEDA* that prioritizes the public purposes underlying the Act over a strictly compensatory approach to damages and insistence on strict proof of tangible losses.

The amount of the award in *Chitrakar* is a quantum leap forward. The handful of previous damages awards under *PIPEDA* have been modest: $4,500 and $2,500 for disclosure of financial information by banks in family law proceedings,[14] $1,500 for accidental publication of personal information on a law firm's website,[15] and $5,000 for the delivery of an inaccurate credit report by a credit reporting company.[16]

What distinguishes *Chitrakar* from the earlier cases is Bell's response to the privacy breach. Justice Phelan was clearly troubled by Bell's apparent apathy towards their errors, including the failure to respond to the court application. Conversely, earlier cases involved carelessness or inadvertence rather than disregard for privacy rights. However, what all of the cases have in common is a willingness to recognize the appropriateness of compensation for violations of privacy rights through a flexible approach to proof of damages informed by the purposes of *PIPEDA*.

A Purposive Approach to Damages

Damages awards under *PIPEDA* are unique. They fulfill a broad public purpose beyond the more strictly individual and compensatory purpose of damages in modern tort law. *PIPEDA* damages serve to advance organizational and societal respect for the Principles outlined in the legislation by providing a meaningful remedy for their breach. Jurisprudence has sought to reinforce the seriousness of such breaches through a flexible approach to damages which recognizes that breaches of privacy rights may be compensated even absent clear evidence of a direct loss.

Indeed, none of the damages awards under *PIPEDA* have been linked to a direct pecuniary loss. Damages have been awarded under the inherently subjective head of humiliation.[17] The cases have, quite properly, taken into account the prophylactic potential of damages awards in furthering *PIPEDA*'s general objectives and values, deterring future breaches, and "sending the message" that organizations must handle personal information prudently.[18] At least one decision has awarded damages in the absence of any actual damages suffered by the applicant.[19] None of the decisions have been based on what could be considered "hard evidence" of damages.

As one commentator has observed:

> … it would appear that the need for vindication or deterrence apparently outweighed the lack of proof of damages, the lack of direct causation between the damages or losses claimed by the applicants and the privacy breach in question, and even the applicant's own role in the circumstances leading to the claimed damages.[20]

This flexible approach to damages is supported on a number of levels. First, given *PIPEDA*'s clear public functions, analogies to cases decided under Canada's premier codification of rights, the Charter, are appropriate and have been drawn in a number of the cases awarding damages under *PIPEDA*.[21] These cases have cited as instructive the Supreme Court's approach to Charter damages in *Vancouver v. Ward* [*Ward*], which recognizes deterrence and vindication as valid objectives of public law damages.[22] Importantly, the court in *Ward* affirmed that, particularly in the constitutional context, absence of personal loss does not preclude damages where an award is clearly supported by the objectives of vindication or deterrence.[23] *PIPEDA*, like the *Privacy Act*,[24] has been recognized as quasi-constitutional legislation to be interpreted in light of its special purposes.[25]

Second, an approach to damages that gives primacy to vindicating *PIPEDA*'s Principles, even in the absence of tangible damages, is consistent with the statute's public purpose, particularly in the context of breaches of rights that are worthy of sanction but cause damages which are difficult to measure empirically and susceptible to being shrugged off. As the Supreme Court observed in *Ward*: "a resilient claimant whose intangible interests are harmed should not be precluded from recovering damages simply because she cannot prove a substantial psychological injury".[26] This approach is also supported by *PIPEDA*'s language itself, which specifically empowers the Federal Court to award damages for "any humiliation that the complainant has suffered".[27]

Finally, a purposive approach does not mean that any trifling privacy breach will be compensated with damages. Rather, such an approach fixes

damages through a contextual assessment of the potential effect of the award on organizational behaviour. *Girao* outlines factors that may be relevant to this exercise:

> [1.] Whether awarding damages would further the general objects of *PIPEDA* and uphold the values it embodies;
>
> [2.] Whether damages should be awarded to deter future breaches;
>
> [3.] The seriousness or egregiousness of the breach;
>
> [4.] The impact of the breach on the health, welfare, social, business or financial position of the applicant;
>
> [5.] The conduct of the respondent before and after the breach;
>
> [6.] Whether the respondent benefited from the breach;
>
> [7.] The nature of the information at stake;
>
> [8.] The nature of the relationship between the parties;
>
> [9.] Prior breaches by the respondent indicating a lack of respect for privacy interests.[28]

Only one of these nine factors, the impact of the breach on the position of the applicant, is directly concerned with compensating the applicant for the damage caused by the wrongful conduct of the respondent. The balance of the factors fulfils the objectives of vindication and deterrence. *PIPEDA* damages thus need not be either compensatory or punitive. They are what has been referred to as symbolic or moral damages awarded, in the words of Professor Stephen M. Waddams, "to vindicate rights or symbolize recognition of their infringement".[29]

Damages and Access to Justice

PIPEDA's structure also provides access to justice for breaches of privacy in a way in which common law remedies, such as the tort of intrusion upon seclusion recently recognized by the Ontario Court of Appeal in *Jones v. Tsige*, do not.

The complaint procedure under *PIPEDA* is simple and is accomplished through the completion of a complaint form that can be filled out online.[30] Once a complaint is made, the Commissioner investigates and produces a report within one year. This mechanism in practice accomplishes many of the same purposes as documentary and oral discovery in civil proceedings at no cost to the complainant. While the Commissioner's report does not bind the court,[31] it may be tendered as evidence and accepted as an accurate reflection of events, thereby laying the factual groundwork and obviating the need to call extensive *viva voce* evidence to prove liability.[32] Finally, the application to Federal Court itself must be "heard and determined without delay and in a summary way".[33]

This legally unburdened process provides the accessibility that has eluded typical civil litigation. It also explains the success self-represented litigants have had in obtaining *PIPEDA* damages—all of the cases where damages have been awarded have been pursued by self-represented litigants.[34]

The Future of *PIPEDA* Damages

Legislative change may further enhance accessibility. Amendments to provide for statutory damages administered by the Federal Court have been proposed by the Privacy Commissioner.[35] Such a model would provide complainants with the option of selecting set damages upon proof of liability without any need to prove damages, similar to the regime currently in force under the *Copyright Act*.[36] This change would further simplify the Federal Court hearing process by streamlining damages—arguably the most difficult issue the court has had to grapple with in applications under s. 16 of *PIPEDA*.

Absent legislative change, a salutary jurisprudential development would be the articulation of a range of benchmark damages. Such a development is likely, given that, other than *Chitrakar*, awards have all fallen within a modest range of a few thousand dollars. A similar scale approach to damages has taken hold in the Federal Court's jurisprudence

on trade-mark violations, avoiding the need for lengthy damages inquiries in another class of cases where damage calculations can be cumbersome and approximate.[37] This approach is also consistent with *Jones v. Tsige*, where the court advocated the use of a modest conventional range of damages to maintain consistency, predictability, and fairness.[38] Of course, it would always be open to an applicant to prove additional damages or to seek to establish conduct warranting an award of punitive damages.

Appellate clarification of *PIPEDA* damages may also be forthcoming. A damages award under *PIPEDA* has yet to be appealed; when an appeal is made, we may expect the Federal Court of Appeal to outline the appropriate approach to both quantification of and entitlement to damages, given the sometimes stark trial-level divergence on these issues. For example, one Federal Court authority held that an award of damages under *PIPEDA* "should only be made in the most egregious situations"[39] while another ruled that "there is no reason to require that the violation be egregious before damages will be awarded."[40]

Looking forward, there is every indication that damages awards under *PIPEDA* will rise in both quantum and frequency. Given the ubiquity of the collection and use of personal information for commercial purposes, and growing public awareness of privacy rights, the volume of applications is likely to rise. Higher awards are also likely—we have thus far not seen a case where any significant economic or psychological damages have been proved, though the potential for such damages is enormous. Professional representation for applicants has yet to take hold, and if and when it does, it is reasonable to expect the court will see a more sophisticated marshalling of evidence of damages with the attendant expert reports on loss.

All of these considerations signal the ascendancy of the Federal Court application process as an effective tool for fulfilling *PIPEDA*'s objectives and providing access to a streamlined system for resolving privacy disputes. In an age in which privacy, technology, and law collide more than ever, it stands to be an adjudicative mechanism of ever-increasing importance.

---

1 *Chitrakar*, [2013] F.C.J. No. 1196, 2013 FC 1103.
2 *PIPEDA*, S.C. 2000, c. 5.
3 *Ibid*., s. 4 and Schedule 1.
4 *Ibid*., s. 11.
5 *Ibid*., s. 13.
6 *Ibid*., s. 12.2.
7 *Ibid*., s. 12.1. The limits of the Commissioner's investigative powers were considered by the Supreme Court in *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, [2008] S.C.J. No. 45, 2008 SCC 44, where it was held that the Commissioner could not access documents covered by solicitor-client privilege, even for the purpose of establishing whether the privilege was properly claimed.
8 *Ibid*., s. 14.
9 *Englander v. Telus Communications Inc.*, [2004] F.C.J. No. 1935, 2004 FCA 387 at paras. 47–48; *Johnson v. Bell Canada*, [2008] F.C.J. No. 1368, 2008 FC 1086 at para. 20; *Girao v. Zarek Taylor Grossman, Hanrahan LLP*, [2011] F.C.J. No. 1310, 2011 FC 1070 at para. 23 [*Girao*].
10 *Chitrakar*, *supra* note 1 at para. 17; *Landry v. Royal Bank of Canada*, [2011] F.C.J. No. 880, 2011 FC 687 at para. 13 [*Landry*].
11 *PIPEDA*, s. 16(c).
12 *Chitrakar*, *supra* note 1 at para. 11.
13 *Ibid*. at para. 18.
14 *Landry*, *supra* note 10; *Biron v. RBC Royal Bank*, [2012] F.C.J. No. 1183, 2012 FC 1095.
15 *Girao*, *supra* note 9.
16 *Nammo v. TransUnion of Canada Inc.*, [2010] F.C.J. No. 1510, 2010 FC 1284.
17 *Biron*, *supra* note 14 at para. 43; *Nammo*, *ibid*. at paras. 67–69, 79; *Landry*, *supra* note 10 at para. 32.
18 *Nammo*, *supra* note 16 at para. 76; *Girao*, *supra* note 9 at para. 50.
19 *Girao*, *ibid*. at para. 55, where Justice Mosley awarded damages, even upon finding absent evidence of damages and a finding that the record did not establish any humiliation as a result of the breach.
20 David Elder, "Panning for Gold in the Mud: The Availability of Privacy Damages under *PIPEDA*", Can. Priv. L.R. 9, no. 1 (December 2011): 6.
21 *Nammo*, *supra* note 16 at paras. 72–74; *Chitrakar*, *supra* note 1 at para. 26; *Girao*, *supra* note 9 at paras. 43–45.
22 *Ward*, [2010] S.C.J. No. 27, 2010 SCC 27, at paras. 25, 27, 30–31, 50–52, 71–72.
23 *Ibid*. at para. 30.
24 R.S.C. 1985, c. P-21.
25 *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] S.C.J. No. 55, 2002 SCC 53; *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. No. 1043, 2004 FC 852 at para. 100; *Nammo*, *supra* note 16 at paras. 74–75.

[26] *Ward*, *supra* note 22 at para. 27.
[27] *Chitrakar*, *supra* note 1 at para. 2.
[28] *Girao*, *supra* note 9 at paras. 46–48.
[29] *Jones v. Tsige*, [2012] O.J. No. 148, 2012 ONCA 32 at para. 75, citing Professor Stephen M. Waddams, *The Law of Damages*, looseleaf (Toronto: Canada Law Book, 2011).
[30] <http://www.priv.gc.ca/complaint-plainte/pipeda_e.asp>.
[31] *Biron*, *supra* note 14.
[32] *Chitrakar*, *supra* note 1 at para. 17. As noted above, the Federal Court hearing is a hearing *de novo*, and accordingly, the Commissioner's Report will not be granted deference and may be challenged or contradicted as other documentary evidence: *Englander*, *supra* note 9 at para. 48.
[33] *PIPEDA*, *supra* note 2, s. 17(1).
[34] *Landry*, *supra* note 10; *Biron*, *supra* note 14; *Girao*, *supra* note 9, *Nammo*, *supra* note 16; and *Chitrakar*, supra note 1.
[35] Office of the Privacy Commissioner of Canada, *The Case for Reforming the* Personal Information Protection and Electronic Documents Act, May 2013, <http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp>.
[36] Under the *Copyright Act*, applicants have the option either to pursue statutory damages or to prove their actual damages. See *Copyright Act*, R.S.C. 1985, c. C-42, s. 38.1.
[37] *Louis Vuitton Malletier S.A. v. Singga Enterprises (Canada) Inc.*, [2011] F.C.J. No. 908, 2011 FC 776 at paras. 129–132; *D. & A.'s Pet Food 'n More Ltd. v. Seiveright (c.o.b. Pets 'n' More)*, [2006] F.C.J. No. 243, 2006 FC 175 at paras. 8–9.
[38] *Jones v. Tsige* at paras. 71 and 75, citing Professor Stephen M. Waddams, *supra* note 29.
[39] *Randall v. Nubodys Fitness Centres*, [2010] F.C.J. No. 823, 2010 FC 681 at para. 55.
[40] *Chitrakar*, *supra* note 1 at para. 24.

I Spy with My Little GPS Eye …

Michelle McCann
Associate
Stewart McKelvey

Using GPS to monitor off-site employees has once again been approved by the British Columbia Office of the Information & Privacy Commissioner.

Earlier this year, we wrote a blog post on time theft by employees,[1] noting that in British Columbia, using GPS and engine status data from the company's vehicle to effectively manage elevator inspectors working off-site was not an invasion of their privacy in the 2012 *Schindler Elevator* decision.[2]

Two new decisions have recently been released in British Columbia—*Kone Inc*.[3] and *Thyssenkrupp Elevator*,[4]—which reached the same conclusion.

In *Thyssenkrupp Elevator*, like in *Schindler Elevator*, the GPS device was installed in the company-owned vehicle and was used to track the movements and productivity of employees throughout the day. The Adjudicator confirmed that using GPS in this way was not a breach of employee privacy.

However, because the employees had not been given appropriate notice on how the GPS system would be used, Thyssenkrupp was ordered to suspend its use for a period of ten weeks to ensure all employees were given proper notice.

In *Kone Inc*., the GPS devices were contained in company cell phones that elevator mechanics used. Employees argued this was more intrusive than using GPS data from the company vehicle because it tracked all of the movements of the employee. Such tracking, they argued, constituted an invasion of privacy under British Columbia's legislation.

The Adjudicator disagreed, finding that the use of GPS tracking through cell phone data was a fair substitute for supervision where in-person supervision was not practical. He said information collected by the employer was not particularly "sensitive" because it concerned the location of employees during working hours.

The Adjudicator found that the following facts suggested the employee's privacy was not violated:

- The mechanic had the ability to put the phone on "off duty" status and was expected to do so during break times, lunch times, and non-working hours. When the phone was on "off duty" status, no information was fed back to the main office.

- Due to the wide geographic working location of the mechanics, Kone Inc. had valid safety concerns, and the ability to track employees was a safety feature. Part of that safety feature included alerting the employer when a phone has been stationary for more than 30 minutes.
- In addition to acting as a time clock for employees, the data was collected for other legitimate purposes, such as client billing. The GPS recorded the time at different jobs in the same way employees previously recorded time manually.
- Questioning the employees, based on the location information provided by the GPS, was "nothing remarkable". Where employees are not where they are supposed to be during working hours, do not follow company rules, or struggle with productivity, it is not an uncommon workplace response for management to question the employee.

In both cases, the Adjudicators recommended that the employers create a specific policy (setting out the purpose for which GPS information would be collected, used, or disclosed) rather than rely on broad safety and managerial policies to justify the use of GPS tracking.

What This Means to You

If an employer has a legitimate business reason for collecting GPS information on employees working off-site, it may not be a breach of an employee's privacy to do so.

While these cases specifically interpret British Columbia's privacy legislation, the underlying theme in *Schindler Elevator*, *ThyssenKrupp Elevator* and *Kone Inc.* suggests that GPS monitoring to establish where an employee is during working hours and how much time he or she is spending on a job is akin to in-person supervision and is more practical where the employer has multiple remote employees.

If you are considering setting up a GPS tracking system that will be used as a monitoring tool for off-site employees, it is important to remember that these cases included several specific facts that led to the Adjudicators' findings:

- The information collected on employees was limited.
- Employees were not monitored during off-duty times.
- Employees were off-site close to 100 per cent of their working time.
- The GPS devices were in company-owned equipment that the employee did not pay for.
- The information was also collected for purposes other than employee supervision or management.
- Information about how the GPS data would be used was required to be communicated to employees in advance.
- The Adjudicators encouraged employers to develop specific written policies surrounding the use of GPS data.
- Notice of implementation of the GPS system, given before the system is introduced, is an important consideration.

---

1 Michelle McCann, "Tick Tock, Hickory Dock! Monitoring Employees for Time", *Stewart McKelvey Blog*, May 28, 2013, <http://www.stewartmckelveyblogs.com/HRLaw/tick-tock-hickory-dock-monitoring-employees-for-time-theft/>.

2 *Order P12-01; Schindler Elevator Corporation (Re)*, 2012 BCIPC 25.

3 *Order P13-01; Kone Inc. (Re)*, [2013] B.C.I.P.C.D. No. 23.

4 *Order P13-02; Thyssenkrupp Elevator (Canada) Ltd. (Re)*, [2013] B.C.I.P.C.D. No. 24.

INVITATION TO OUR READERS
Do you have an article that you think would be appropriate for *Canadian Privacy Law Review* and that you would like to submit?

Do you have any suggestions for topics you would like to see featured in future issues of *Canadian Privacy Law Review*?

If so, please feel free to contact Professor Michael A. Geist.
mgeist@uottawa.ca
or
cplr@lexisnexis.ca