Class Action Defence Quarterly

VOLUME 12, NUMBER 1 Cited as (2017), 12 C.A.D.Q. SEPTEMBER 2017

• PRIVACY BREACHES AND POST-BREACH CONDUCT – GUIDANCE FROM CASE LAW AND REGULATORY INVESTIGATIONS •

Chloe Snider, Partner, Thomas Wilson, Associate and Julia Ji, Student, Dentons Canada LLP


Chloe Snider


Thomas Wilson


Julia Ji

I. OVERVIEW

Canadian privacy law has been evolving in response to the rapidly changing digital landscape. This trend began in 2012 with the Court of Appeal for Ontario's decision in *Jones v. Tsige* (*Jones*),[1] which recognized the tort of intrusion upon seclusion in Ontario. In June 2015, another major development in Canadian privacy law occurred when the *Digital Privacy Act* (Bill S-4) received Royal Assent.[2] The Digital Privacy Act enacted several amendments to the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[3], federal legislation which governs the collection, use and dissemination of personal information by private sector organizations. The *Digital Privacy Act* provides for the establishment of privacy breach notification requirements which, once in force, will require organizations to disclose privacy breaches where there is a "real risk of significant harm".[4]

The authors of the 2015 Class Action Defence Quarterly article "*Privacy Breaches: The New Frontier in Class Actions*" observed that breach of privacy class actions were becoming increasingly

CLASS ACTION DEFENCE QUARTERLY

Class Action Defence Quarterly is published four times per year by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only

ISBN 0-433-45401-6 (print) **ISSN 1911-2270**
ISBN 0-433-45403-2 (PDF) **ISSN 1911-2289**
ISBN 0-433-45406-7 (print & PDF)

Subscription rates: $359.00 per year (print or PDF)
$499.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Eliot N. Kolers
Firm: Stikeman Elliott LLP
Tel.: (416) 869-5637
E-mail: ekolers@stikeman.com

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cadq@lexisnexis.ca
Web site: www.lexisnexis.ca

common and accurately predicted that this trend would continue with the enactment of the *Digital Privacy Act*.[5] Since 2015, there has been an increase in the number of class proceedings based on privacy and cybersecurity breaches demonstrating that privacy breaches present significant legal and reputational risk for private sector organizations.[6] Once in force, the breach notification requirements under *PIPEDA* may increase the risk that proceedings will be commenced in the wake of a privacy or cybersecurity breach.[7]

This article examines recent judicial and regulatory treatment of privacy breach incidents and assesses the effect of post-breach conduct on organizations' exposure in this fast developing area in both the regulatory and class action contexts. We will begin by outlining recent legislative developments, the existing voluntary reporting program administered by the Office of the Privacy Commissioner of Canada (OPC) and relevant breach investigation reports from the OPC. We will then address recent class action settlement approval decisions that also address the post-breach conduct of defendant organizations. Notwithstanding the increasing number of privacy related obligations on private organizations, reports of regulatory investigations and existing case law suggest that appropriate and pro-active post-breach conduct may help reduce the attendant risks facing private sector organizations.

II. RECENT LEGISLATIVE DEVELOPMENTS

As set out above, breach notification requirements were introduced by the *Digital Privacy Act* in 2015 but are not yet in force. Privacy law experts expect *PIPEDA*'s mandatory notification provisions to come into force once regulations have been finalized, and have urged organizations to develop comprehensive privacy compliance programs and policies in the interim.[8] The mandatory notification regime has three key requirements: (i) reporting to the OPC; (ii) notifying affected individuals; and (iii) diligent record keeping of all breach incidents.[9]

The obligation to report to the OPC and to notify affected individuals will be triggered if

the breach constitutes a "real risk of significant harm". "Significant harm" is defined broadly as, "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property".[10] In determining whether a given breach meets the notification threshold, factors such as the sensitivity of the information involved in the breach and the likelihood that such information will be misused should be considered. Once the "real risk of significant harm" threshold is met, notification to the affected individuals and reporting to the OPC should be made "as soon as is feasible".[11]

In addition to notification obligations, organizations will be required to document systematically all breaches of security safeguards, even if such breaches do not constitute a "real risk of significant harm".[12] "Breach of security safeguards" is defined by *PIPEDA* as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in Clause 4.7 of Schedule 1 or from a failure to establish those safeguards".[13] Accordingly, under the new regime, it will be important for organizations to be cognizant of the various ways in which a breach could occur and to exercise diligent record keeping.

III. GUIDANCE FROM THE OPC'S VOLUNTARY BREACH REPORTING PROGRAM AND INVESTIGATIONS

While the *PIPEDA*'s mandatory breach notification provisions are not yet in force, a voluntary breach notification program administered by the OPC has been in place since 2007.[14] The OPC's voluntary program closely resembles the mandatory regime under *PIPEDA*. For instance, the voluntary program encourages organizations to report "material" privacy breaches to the OPC and provide notifications to affected individuals while *PIPEDA*, as discussed above, will require notification where there is a "real risk of significant harm".[15] Compliance with the OPC's voluntary breach reporting program has, no doubt, helped organizations strengthen their privacy compliance regimes and become familiar with the upcoming notification requirements under *PIPEDA*.

In Canada, organizations that have reported breaches to the OPC have done so under the voluntary reporting program. Importantly, a number of the OPC's breach incident investigations following these breach notifications have concluded that organizations that complied with the full scope of the voluntary breach reporting program responded in a satisfactory manner to the triggering breach incident. The OPC's reports include details of particular breach incidents and the privacy practices of affected organizations. These reports help identify where and how privacy and cybersecurity vulnerabilities might arise within particular sectors. The OPC's reports identify remedial measures that it has consistently found to be satisfactory — information which may be helpful to organizations looking for guidance, in the absence of detailed direction from a significant body of case law, on appropriate post-breach conduct once *PIPEDA*'s mandatory notification regime comes into force. Three noteworthy OPC investigation reports are discussed in greater detail below.

A) March 2014 – Data Lost in Transit (Insurance Sector)

In March 2014, an insurance company experienced a data breach when files containing personal information regarding customers went missing in transit.[16] As soon as the company became aware of the incident, it notified the affected individuals and the OPC.[17] Further, the company implemented remedial measures including a free credit monitoring service to affected individuals and the implementation of new and enhanced data protection safeguard practices.[18] The OPC's investigation revealed that the company's privacy practices at the time of the breach incident were inadequate.[19] However, the OPC found that the incident was resolved due to the breadth and timeliness of remedial measures taken.[20]

B) July 2015 – Cyberattack on Online Contest Database (Commercial Sector)

In July 2015, a commercial organization suffered a cyberattack on its online database, which contained personal information about its online contest entrants.[21] As soon as the breach was confirmed, the organization reported the incident to law enforcement authorities and the OPC.[22] In addition, 70,000 affected individuals were notified and an independent cyber forensics investigator was retained.[23] The investigator determined that flaws in a third-party hosting service provider's cybersecurity had resulted in the breach.[24] The remedial measures taken by the organization included mandatory privacy training for all employees and the implementation of a new policy requiring consultation with the organization's legal department before engaging with any third-party online service provider.[25] As a result of these remedial measures, the OPC was "satisfied with the actions taken by the company in response to the breach".[26]

C) February 2016 – Mass Mailing Error (Financial Services Sector)

In February 2016, a data breach at a financial institution was discovered when a customer received someone else's RRSP tax contribution statement in the mail.[27] The organization reported the incident to the OPC and notified the affected clients.[28] The organization's investigation revealed that the breach was caused by an error that occurred during the automated print production process.[29] The organization's remedial measures included providing customers with new statements, offering a free credit monitoring service, implementing enhanced controls and safeguards, and increasing the internal monitoring of customers' accounts.[30] In addition, the organization asked its customers to destroy the incorrect statements and further instructed its employees to destroy any returned incorrect statements.[31] In its report, the OPC recommended that other organizations take similar steps in response to data breaches arising from mailing errors.[32]

D) Lessons Learned from the OPC Investigations

The OPC investigations described above confirm that compliance with the voluntary breach reporting program has allowed organizations to avoid negative regulatory findings, which could otherwise lead to a penalty under *PIPEDA*.[33] In addition, the investigation reports demonstrate that certain breach-specific responses will be considered appropriate and satisfactory by the OPC. For instance, where the breach was caused by a third party service provider's inadequate security measures, implementing a new policy that requires consulting with the legal department before engaging with any online service provider was satisfactory. Where the breach was caused by a failure in employee oversight, providing additional privacy training was an appropriate response. While there are various appropriate situation-specific breach responses, some consistent responses are also observed. These include: reporting to the OPC; notifying affected individuals; and offering a credit monitoring service where financial data is at risk. As discussed below, these consistent factors also play an important role in settling class actions arising from privacy and cybersecurity breaches.

IV. GUIDANCE FROM DATA BREACH CLASS ACTION SETTLEMENT APPROVALS

Two recent decisions from the Ontario courts offer guidance on how organizations can take active steps to minimize liability in breach of privacy class proceedings: *Maksimovic v. Sony of Canada Ltd.* (*Sony*)[34] and *Drew v. Walmart Canada Inc.* (*Walmart*),[35] both of which were commenced following breach notification to customers. The decisions suggest that remedial and notification efforts, such as those described in the OPC reports above, will not go unnoticed by the courts.

A) The *Sony* Case

In 2011, Sony's PlayStation Network suffered a third party cyberattack, through which the third

party sought access to account holders' personal information. Upon discovering the attack, Sony temporarily shut down its networks.[36] When services resumed, Sony offered a "welcome back" package to the returning account holders, including free content and subscriptions discounts.[37] Notwithstanding the "welcome back" package, class proceedings were commenced against Sony. The allegations included breach of privacy rights and breach of contract.[38]

The parties in *Sony* agreed to settle the class proceeding. Key settlement terms included reimbursements of up to a maximum of $2,500(CAD) per claim to account holders who could demonstrate that they suffered identity theft as a result of the incident and a cash refund of any unused account balances.[39] These settlement terms constituted a significant reduction from the claimed amount of $500 million (CAD).[40] In approving the settlement, the Ontario Superior Court of Justice took into consideration the value offered by the "welcome back" package and the fact that there had not been any identity theft resulting from the cyberattack.[41] The Court further held that "[t]he Settlement Agreement reflects the state of the law, including possible damage awards, for breach of privacy/intrusion upon seclusion and loss/denial of service claims".[42]

B) The *Walmart* Case

In 2015, Walmart experienced a data breach when third parties accessed Walmart customers' personal and financial information.[43] Walmart directly notified individuals affected by the breach. Following notification, a class action was commenced alleging, among other things, breach of contract, breach of confidence, violation of privacy and intrusion upon seclusion.[44]

The settlement terms approved by the Ontario Superior Court of Justice included: a credit monitoring plan for any member of the class who made a valid claim to the maximum cumulative value of $350,000(CAD) and reimbursements to any member of the class who incurred out-of-pocket losses as a result of the data breach to the maximum cumulative value of $400,000(CAD).[45]

C) Lessons Learned from the Settlement Approvals

The *Sony* and *Walmart* decisions illustrate that where organizations take timely and appropriate remedial action, high-profile data breaches will not necessarily result in costly settlements, even where the breach affects a large number of people. In *Sony*, the claim for $500 million (CAD) was reduced to a cash refund of existing PlayStation account balances and a maximum reimbursement of $2,500 (CAD) to each class member that could prove identity theft as a result of the breach incident. In *Walmart*, a credit monitoring service and reimbursement were offered to any class member who made a valid claim. These settlement approval cases are consistent with the OPC's investigations and highlight the importance of appropriate remedial measures (including credit monitoring services where financial data is breached) in helping to reduce defendant exposure in the class action context (depending on the nature of the data breach at issue).

V. CONCLUSION

Class actions arising out of privacy and cybersecurity breaches appear to be on the rise in Canada. In light of *Jones* and the rapid development of digital technologies, private sector organizations are faced with increasingly stringent privacy and consumer protection laws. The anticipated mandatory breach notification provisions under *PIPEDA* will also require organizations to take an active role in minimizing harm to individuals affected by a data breach. As demonstrated by the OPC's reports, compliance by way of diligent and prompt breach notification to relevant stakeholders can help contain the legal risks, and associated financial burden, of data breaches. Notwithstanding these benefits of breach notification, breach notifications are often the trigger for the commencement of class actions and help to identify the class members.[46] Breach notifications can also attract media coverage of the incident which can damage the organization's reputation and marketplace confidence.[47]

As industries become increasingly reliant on digital information, compliance with breach notification requirements and demonstrating satisfactory post-breach conduct may become a part of what it means to be a good corporate citizen in Canada. As privacy and cybersecurity class actions continue to be certified, private sector organizations should develop and implement a breach response plan, particularly in anticipation of the upcoming mandatory breach notification regime. In doing so, organizations should consider the particulars of their cyber vulnerabilities, provide proper breach response training to their employees, and ensure that third-party service providers also have adequate security measures in place.

[***Chloe Snider** is a partner in Dentons Canada LLP's litigation and dispute resolution group. Her practice focuses on litigating complex commercial disputes and assisting clients manage risk.*

***Thomas Wilson** is a lawyer in Dentons Canada LLP's litigation and dispute resolution group. His practice involves a variety of corporate, commercial, and civil litigation matters.*

***Julia Ji** is a summer student at Dentons Canada LLP and a third year law student at the University of Ottawa.*]

---

1 [2012] O.J. No. 148, 2012 ONCA 32 [*Jones*].

2 *Digital Privacy Act*, S.C. 2015, c. 32.

3 S.C. 2000, c. 5 [*PIPEDA*].

4 *Supra* note 2 ss. 10.1–10.3.

5 Adrian Lang & Lesley Mercer, "*Privacy Breaches: The New Frontier In Class Actions*" (2015) 10:1 Class Actions Defence Quarterly.

6 There have been a number of recent decisions in privacy class actions, both concerning procedural issues and certification. For example, in *Condon v. Canada*, [2014] F.C.J. No. 297, 2014 FC 250, the Federal Court certified a class proceeding concerning breach of privacy allegations regarding an external hard drive containing financial information about students who received government loans that was lost by the office of Human Resources and Skills Development Canada. More recently, in *Drew v. Walmart Canada Inc.*, [2016] O.J. No. 6754, 2016 ONSC 8067, the Ontario Superior Court of Justice approved a settlement of a class proceeding regarding a data breach of Walmart's online photocentre website. Further, in 2017, there was a carriage dispute regarding an alleged privacy breach in *Kaplan v. Casino Rama Services Inc.*, [2017] O.J. No. 2357, 2017 ONSC 2671. Further, and without providing an exhaustive list, the Supreme Court of Canada recently addressed jurisdictional issues in a proposed class action concerning breach of privacy in *Douez v. Facebook Inc.*, [2017] S.C.J. No. 33, 2017 SCC 33.

7 "2012 Consumer Study on Data Breach Notification" *Ponemon Institute LLC* (June, 2012) online: http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf at 24. This also appears to be supported by the case law, including the *Sony* and *Walmart* cases discussed herein.

8 Interview of Tim Banks by DataGuidance (April 2016) at the International Association of Privacy Professionals' Conference in Washington D.C. online: http://www.dataguidance.com/dataguidance-iapp-interview-tim-banks.

9 *Supra* note 2 ss. 10.1–10.3.

10 *Ibid.*, at s. 10.1(7).

11 Innovation, Science and Economic Development Canada, *Data Breach Notification and Reporting Regulations*, (Ottawa: Innovation, Science and Economic Development Canada, 2016) at 12.

12 *Supra* note 2 s. 10.3(1).

13 *Supra* note 3 s. 2(1).

14 *Supra* note 11 at 4.

15 *Ibid.*

16 Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2014-003, "Insurance Company Overhauls Its Security Safeguards Following Privacy Breach" (3 March 2014).

17 *Ibid.*

18 *Ibid.*

19 *Ibid.*

20 *Ibid.*

21 Office of the Privacy Commissioner of Canada, Incident Summary #9, "Online Contest Database Hacked" (10 July 2015).

22 *Ibid.*

23 *Ibid.*

24 *Ibid.*

25 *Ibid.*

26 *Ibid.*

[27] Office of the Privacy Commissioner of Canada, Incident Summary #11, "Financial Institution Reacts Quickly to Mass- Mailing Error" (19 February 2016).
[28] *Ibid.*
[29] *Ibid.*
[30] *Ibid.*
[31] *Ibid.*
[32] *Ibid.*
[33] *Supra* note 3 s. 20.
[34] *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 (ON SC) [*Sony*].
[35] *Walmart*, *supra* note 6.
[36] *Ibid.*, at para. 7.
[37] *Ibid.*
[38] *Ibid.*, at para. 8.
[39] *Ibid.*, at para. 13.
[40] *Maksimovic v. Sony of Canada Ltd.* (2 May 2013), Toronto, 2013 CarsPleadingW 21867 (Statement of Claim).
[41] *Supra* note 34 at paras. 15–1
[42] *Ibid.*, at para. 16.
[43] *Walmart*, *supra* note 6 at para. 5.
[44] *Ibid.*, at para 6.
[45] *Ibid.*, at para 9.
[46] *Supra* note 7.
[47] *Ibid.*, at 14; Further, as noted above, both the *Sony* and *Walmart* cases were commenced following breach notification to affected individuals.

This article was originally published in ***Class Action Defence Quarterly,*** Vol. 12, No. 1