Paul-Erik Veel
416-865-2842
pveel@litigate.com

November 25, 2020

I wish we were better strangers: Parliamentâ€™s proposed statutory cause of action for privacy breaches may attract class plaintiffs

Referring to living “in an era in which data is constantly flowing across borders”, Canada recently introduced Bill C-11. If enacted, it will radically alter the Canadian privacy litigation landscape. Bill C-11 contains the *Consumer Privacy Protection Act* (“***CPPA***” or the “***Act***”), and the *Personal Information and Data Protection Tribunal Act* (“***PIDPTA***”), and makes a number of consequential amendments to existing legislation. Bill C-11 would bring Canada closer to the European Union’s *General Data Protection Regulation*, which set the standard for data protection in the developed world.

While much ink has been and will be spilled on the structure and import of Bill C-11, our focus in this post will be on its potential impact on class actions.

Statutory Cause of Action

The *CPPA* creates two private rights of action in ss 106(1) and (2) through which an individual can recover damages for loss or injury they suffered based on contravention of the *Act*. Both can be brought in either the Federal Court or the Superior Court of a province.

In order for an individual to pursue the statutory cause of action under s 106(1), the Privacy Commissioner (under the federal *Privacy Act*) must have either:

1. made a finding under para 92(1)(a) of the *CPPA* (and the time for appeal has expired or an appeal has been dismissed); or

2. made a finding under s 102(1) of the *CPPA* that an organization has contravened the *Act*. Prior to making such a finding, the Commissioner must complete an inquiry into the organization’s compliance with the *Act*.

A finding under paragraph 92(1)(a) is either a finding that an organization has not complied with the terms of the *CPPA*, or that the organization has not complied with the terms of a

compliance agreement it entered into with the Commissioner. The obligations under the *Act* that could be the subject of a finding are broad and have been canvassed by others, and we will not repeat them in detail here. However, in general terms, the *Act* renders an organization accountable for protecting the personal information under its control. It also limits the circumstances in which personal information can be collected, used or disclosed by an organization. It requires organizations to obtain valid, express consent at or before the time personal information is collected, or if information is to be used for some other purpose than for which consent was originally obtained, before using or disclosing the information for that new purpose. The *Act* expressly prohibits tying consent to the provision of goods and services where the consent would go beyond what is required to provide the goods or services.

An individual also has a cause of action under s 106(2) where an organization has been convicted of one of the offences listed under s 125 of the *CPPA*, and the individual has suffered loss or damages from the events underlying the conviction. These offences also give rise to fines that Canada touts as the highest in the G7.

The offences listed under s 125 of the *CPPA* that can ground the second cause of action under the *Act* include the following:

1. failing to report or give notice of any breach of security safeguards involving personal information under an organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual; (s 58(1) and (3));

2. failing to keep and maintain a record of every breach of security safeguards involving personal information under an organization's control. (s 60(1));

3. failing to retain information subject to an individual's request to an organization as to:

    a. whether the organization holds information about them;
    b. how the information is used;
    c. whether the information has been disclosed; and
    d. provide the information to the individual

until the individual has exhausted their recourse under the *Act* (s 69);

4. using de-identified information alone or in combination with other information to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information (s 75);

5. an employer taking action against an employee by reason of:

a. the employee contacting the Commissioner respecting a possible contravention of Part 1 of the *Act*;
b. the employee stating an intention or refused to engage in conduct contravening Part 1 of the *Act*;
c. the employee stating an intention or engaged in conduct required to not contravene Part 1 of the *Act*
d. the employer believing that the employee will do any of the above (s 124(1)).

6. Contravening an order made under s 92(2) by the Commissioner, which required an organization to:

a. take measures to comply with the *Act*;
b. stop doing something in contravention of the *Act*;
c. comply with the terms of a compliance agreement it entered into;
d. make public any measure takes on proposed to correct its policies, practices, or procedures that the organization put in place to fulfil its obligations under the *Act* (s 92(2)); and

7. Obstructing the Commissioner or its delegate in the investigation of a complaint, in conducting an inquiry, or in carrying out an audit (s 125).

These preconditions to bringing the causes of action (with necessary modifications) have been applied in other privacy based statutory causes of action. For example, s 65 of Ontario's *Personal Health Information Protection Act*, *2004* ("***PHIPA***") employs essentially the same structure with different offenses and contraventions. However, the analogous provisions in *PHIPA* are almost never litigated.

The Application of the *CPPA* in Class Proceedings

The provisions of the *CPPA* are intended to be markedly broader in their application than other limited purpose legislation, like *PHIPA*. In the *CPPA*, Parliament recognized the ubiquity, transnationality, and economic import of the flow and exchange of personal information. In this framework, the causes of action created by the *CPPA* are likely to be viewed with great interest from the class plaintiffs' bar.

A number of high-profile data breach class actions have been commenced in recent years without the benefit of the statutory causes of action. As currently drafted, there is no indication that Parliament intends to apply the legislation retrospectively or retroactively — and certainly it would violate the Charter to do so with respect to the offences set out above. However, the *Act* could have consequences on class actions predicated on privacy breaches that occur after the *Act* comes into force.

The statutory causes of action may alter class plaintiffs' counsel's strategic landscape in three ways.

First, plaintiffs' counsel may monitor the Commissioner's findings to assess the relative merits of a potential claim. We note that hearings before the Tribunal are presumptively public(s 15(4). The *Act* also contemplates that the Tribunal will enact its own rules (s 19(1)), which will govern the public availability of its decisions (s 18(1)), and may well permit intervention by interested parties. If intervention is permitted, it is possible that putative plaintiffs' counsel may avail themselves of this tool to increase their chances of later relying upon the statutory cause of action.

Second, class plaintiffs' counsel may be more likely to initiate privacy-based class proceedings on other grounds of relief (including the growing number of recognized common law torts), with a view to amending their claims in the event the Commissioner makes a finding enabling them to plead a statutory cause of action. Further, we would expect plaintiff's counsel to take an expansive interpretation of s 106 when it is first brought before the courts in such proceedings.

Third, one obvious advantage of the statutory causes of action from class plaintiffs' perspective is that, in at least some circumstances, the statutory cause of action may be easier to prove than the torts traditionally applied in the same circumstances. The surviving defences on the merits (including the statutory due diligence defence) will be raised before the Commissioner, or Court as the case may be. If those defences are unsuccessful, it is unlikely that there will be an opportunity for defendants to pursue them in a different forum. Put another

way, after class plaintiffs establish the applicable condition precedent, it appears defendants are left to argue about the fact and quantum of the compensable injury or loss.

By contrast, class plaintiffs would be required to prove the underlying elements of the common law claims (and surmount the defences thereto). For example, in a claim in negligence the plaintiffs are required to establish that a standard of care was owed to the class, and it was breached by the defendants' conduct. To recover in intrusion upon seclusion, class plaintiffs need to show that the defendants' conduct was intentional (including reckless), the defendants invaded the plaintiffs' private affairs and that a reasonable person would regard the invasion as highly offensive, causing distress, humiliation, or anguish. In particular circumstances, these may be more difficult to prove than the statutory cause of action under the *CPPA*.

Of course, the applicability of the *Act* to class actions depends on either the Commissioner making findings or there being prosecutions of the offences under the *Act*. Put differently, if the Commissioner chooses not to make formal findings and no prosecutions are brought, these amendments will have limited impact on class proceedings.

From a prospective defendant's perspective, the *CPPA* clearly incentivizes organizations to avoid findings that would enable an individual to access the statutory cause of action. So long as an organization enters into a compliance agreement with the Commissioner, and abides by its terms, it should not face exposure beyond the existing common law remedies.