OSLER

CLASS ACTIONS

Canadian courts confirm significant limits on privacy class actions

Listen to the audio version

For businesses operating in Canada, 2021 brought welcome guidance: courts across the country repeatedly exercised their gatekeeping role to put a stop to privacy class actions that lack evidence of harm to the proposed class members. In other words, a class action should not automatically follow from a data breach or incident. Even when a class action does follow, defendants have a variety of tools to defend privacy claims or to resolve them early on.

The "some basis in fact" requirement is a meaningful screening device

Several decisions reinforced that certification is meant to be a meaningful screening device in privacy class actions:

- In *Simpson v. Facebook, Inc.*, the plaintiff alleged that a third party named Cambridge Analytica had obtained information about Facebook users from a third-party application developer. The Ontario Superior Court of Justice dismissed the plaintiff's certification motion on the basis that there was no evidence that any Canadian user's data was shared with Cambridge Analytica (and therefore no justification for a class proceeding). Justice Belobaba emphasized the Court's gatekeeping role, stating, "The dismissal of this certification motion is simply a reminder to class counsel that while certification remains a low hurdle it is nonetheless a hurdle." Similarly, in *Kish v. Facebook, Inc.*, the Court of Queen's Bench for Saskatchewan dismissed another application for class certification that was premised on allegations related to Cambridge Analytica. Justice Keene built on the growing trend of cases emphasizing the Court's gatekeeping role at the certification stage, including *Simpson* and *Setoguchi v. Uber* (discussed below). Osler acted for Facebook in both cases. Further information is set out in our Osler Updates on these two certification decisions, Ontario Superior Court denies certification of Cambridge Analytica class action and Another Canadian court denies certification of Cambridge Analytica class action.
- Similarly, in *Beaulieu c. Facebook Inc.*, the Québec Superior Court held that the plaintiff did not satisfy her burden at the authorization stage (Québec's equivalent of the certification stage) to establish an "arguable case." Justice Courchesne found that the plaintiff's allegations – that Facebook's tools allowed employers and companies to illegally exclude certain users from employment and housing opportunities – were "hypothetical and speculative." Osler acted for Facebook in this case as well.

In all three cases, the plaintiffs launched, or sought to launch, appeals. In *Kish*, however, the Court of Appeal for Saskatchewan recently dismissed the plaintiff's motion seeking leave to appeal, finding that the plaintiff's proposed appeal lacked sufficient merit to be heard by a panel of the Court of Appeal. The appeal decisions in the other two cases will likely be released in 2022.

Justice Belobaba emphasized the Court's gatekeeping role, stating, "The dismissal of this certification motion is simply a reminder to class counsel that while certification remains a low hurdle it is nonetheless a hurdle."

Plaintiffs must show evidence of harm

Other decisions confirmed that plaintiffs must show evidence of actual harm in order to obtain certification and to succeed on the merits of a proceeding alleging privacy violations. This requirement presented a serious hurdle for plaintiffs in data breach class actions:

- In *Setoguchi v. Uber*, the Court of Queen's Bench of Alberta denied certification of a proposed class action arising out of an alleged data breach involving Uber. There was no evidence that the hacker used any personal data obtained in the breach to anyone's detriment. Justice Rooke found no evidence of any real (not *de minimis*) harm; there was only "speculation about a **future possibility** of loss or harm" (emphasis in original). The court also distinguished "minor and transient upset" from "compensable injury." Justice Rooke observed that without evidence of compensable loss, "a class proceeding could be a mere 'fishing trip' based on speculation, without any evidence of fish being present."
- In March 2021, the Québec Superior Court released its decision in the first privacy class action in Canada to be determined (and dismissed) on the merits. In *Lamoureux v. IIROC*, the plaintiff alleged that an inspector working at the Investment Industry Regulatory Organization of Canada (IIROC) lost a laptop containing information about thousands of Canadians. The laptop was never found. Justice Lucas dismissed the action finding that, while it is not necessary for class members to have actually fallen victim to identity theft in order to recover, injury beyond general inconvenience must be proven. Given the lack of documentary or medical evidence proving the extent of the damages, the Court categorized the class members' fears and worries as general inconveniences. Justice Lucas also dismissed the claim for punitive damages, finding that IIROC acted diligently and implemented appropriate response measures when the loss came to light. The focus on the absence of compensable harm aligns with recent authority from the common law provinces, including *Setoguchi*. Further information is set out in our blog post First merits decision dismissing privacy class action in Canada on the *Lamoureux* decision.

Limits on intrusion upon seclusion claims against database defendants

In 2021, the Ontario Divisional Court held that a necessary element of the tort of intrusion upon seclusion is that the defendant itself *committed* the intrusion. The tort does not apply where a defendant merely failed to prevent an intrusion by a third party. In *Owsianik v. Equifax Canada Co.*, the plaintiff alleged that a third-party hacker infiltrated Equifax's database exposing personal information about thousands of consumers. A class action was initially certified. However, on appeal, a majority of the Divisional Court held that a claim for intrusion upon seclusion could not succeed against Equifax since *an intrusion* is "the central element of the tort" and Equifax did not intrude.

The Divisional Court's decision marks an important development in Canadian privacy law and reaffirms that certification judges should refuse to certify causes of action that are bound to fail. (A further appeal is being pursued by the plaintiff to the Court of Appeal and will be monitored with interest.)

The Divisional Court's decision marks an important development in Canadian privacy law and reaffirms that certification judges should refuse to certify causes of action that are bound to fail.

Pre-certification motions in privacy cases

Recent decisions have also confirmed that pre-certification motions may be appropriate to resolve privacy actions on their merits. In *Schmidt v. LinkedIn Corporation*, the B.C. Supreme Court granted leave for the defendant to have its summary trial application determined in advance of certification. The plaintiff alleged that LinkedIn's iOS app surreptitiously read and stored the contents of users' clipboards. But the plaintiff presented no evidence supporting those allegations. LinkedIn sought, and the Court granted, an opportunity to disprove these speculative factual allegations at a pre-certification summary trial. Likewise, in *Cronk v. LinkedIn Corporation*, the B.C. Supreme Court accepted LinkedIn's argument that the defendant's summary trial application should be heard concurrently with certification. The plaintiff alleged that LinkedIn violated privacy legislation by showing users their own names and profile pictures in customized "dynamic ads." LinkedIn sought to defend the case on its merits at an early stage, including on the basis that showing someone their own name and photo is not a breach of privacy. The Court agreed that a summary trial had the potential to conclusively determine the core issues in the case at an early stage. Osler acted for LinkedIn in both cases.

Both *Schmidt* and *Cronk* were B.C. cases and therefore did not address recent amendments to the *Class Proceedings Act, 1992* in Ontario, which expressly encourage pre-certification motions that could promptly resolve, or significantly narrow, putative class proceedings. Both cases are consistent with the B.C. Court of Appeal's subsequent decision in *British Columbia v. The Jean Coutu Group (PJC) Inc*. The Court of Appeal rejected older case law that established a presumption that certification should be the first procedural matter to be heard. The Court's new framework for sequencing pre-certification applications will likely expand the opportunities for defendants in privacy cases to argue summary trial applications either before or concurrently with certification, thereby providing a means for finally disposing of the action at an early stage.

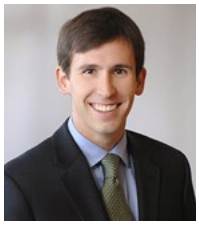
Conclusions

It remains critical for businesses to respond quickly and effectively when data incidents occur; however, businesses should be heartened by this year's developments. Despite the proliferation of privacy class action filings over the last decade, courts across Canada are making it clear that certification is not a rubber stamp. And courts have confirmed that businesses facing privacy class actions have a range of effective tools to defend privacy claims. Osler is at the forefront of these developments and will continue to report as the law regarding privacy class actions matures.

AUTHORS

Mark Gelowitz
Partner, Litigation
mgelowitz@osler.com
416.862.4743

Céline Legendre
Partner, Litigation
clegendre@osler.com
514.904.8108



Robert Carson
Partner, Litigation
rcarson@osler.com
416.862.4235

W. David Rankin
Partner, Litigation
drankin@osler.com
416.862.4895

Emily MacKinnon
Associate, Litigation
emackinnon@osler.com
604.692.2705

Lauren Harper
Associate, Litigation
lharper@osler.com
416.862.4288