CIRCU lawR
A regular publication for legal news and reviews

Court of Appeal Rules Class Action Plaintiffs Can Pursue Claim for Careless Safeguarding of Personal Information

Local governments, take note: your exposure to liability arising from a data breach might be greater than you think. In *G.D. v. South Coast British Columbia Transportation Authority*, 2024 BCCA 252, the Court of Appeal for British Columbia held that an application to certify a class proceeding against a public body whose computer system had been penetrated by hackers should not have been struck for failure to disclose a cause of action. In so doing, the Court recognized that data custodians' obligation to protect personal information they hold is not limited to that set out in the *Freedom of Information and Protection of Privacy Act* ("FIPPA"); likewise, data custodians can commit the statutory tort of violation of privacy found in the *Privacy Act* where they fail to take sufficient steps to protect that personal information. The plaintiffs in the case asserted that the defendant was liable— both under statute and at common law— for taking inadequate steps to prevent a cyberattack and the unauthorized disclosure of a significant amount of sensitive personal information.

In December 2020, the South Coast British Columbia Transportation Authority ("TransLink") discovered that hackers had successfully carried out a phishing operation on one of its employees. The hackers were able to abscond with personal information about current and former employees, some vulnerable clients, and various third parties, including social insurance numbers, banking information, birth dates, and addresses. TransLink notified approximately 39,000 individuals that the hackers may have accessed their information.

A group of former TransLink employees applied to certify a class proceeding on behalf of all individuals whose personal information was compromised by the breach. Under section 4(1)(a) of the *Class Proceedings Act*, a court must find that "*the pleadings disclose a cause of action*" in order to certify a class proceeding. The bar is low and "*will be satisfied as long as it is not 'plain and obvious' that the pleadings disclose no reasonable cause of action*" (*Basyal v. Mac's Convenience Stores Inc.*, 2018 BCCA 235). Among other causes of action, the plaintiffs argued that TransLink violated its statutory obligations to safeguard personal information under FIPPA and the *Privacy Act* and that it was negligent at common law, putting the class

members at serious risk of identity theft and other harms.

The Supreme Court of British Columbia dismissed the plaintiffs' application for certification (2023 BCSC 958), holding that the statutory tort and common law negligence claims were both bound to fail.

With respect to the statutory tort of violation of privacy under section 1 the *Privacy Act*, the application judge held that a person is liable only if they take a positive step to violate another person's privacy without legal entitlement. Justice Wilkinson writes:

> *it is not any act of the data custodian, whether intentional, negligent or even reckless, that is the act which violates privacy (even if the violation would not have occurred but for that conduct). … There is no pleading that TransLink handled information in any manner without an honest belief that it was entitled to do so. Alleged careless conduct below an alleged standard and failure to prevent access is not a wilful breach of privacy under the* Privacy Act. *It was not TransLink that wilfully violated any privacy interests; it was the unauthorized third-party criminals who did.*

In sum, she held, "*the target of th[e] statutory tort in a database breach context can only be the hacker, and not the database defendant*".

The Court of Appeal held that Justice Wilkinson had erred and the language of the *Privacy Act* does not completely preclude a claim against a data custodian that fails to protect the privacy of the individuals about whom it holds personal information. In the context of the *Privacy Act*, "*wilfully and without a claim of right, to violate the privacy of another*" can bear the meaning 'fail to act, deliberately or recklessly, to protect an individual's personal information from disclosure when that individual has a reasonable expectation that it will not be disclosed'. It is up to a trial judge to determine whether the wilful act is actually made out, but preventing a claim from reaching that stage would undermine the broad personal privacy interests the *Privacy Act* aims to protect. Justice Griffin, for the Court of Appeal, writes:

> *Given the expansion of the collection of personal information by private and public entities and the storage of this information on electronic databases, it could well be said that unless data collectors are motivated to protect it, almost all informational privacy interests in the digital world could eventually be lost. It makes no sense to me from a policy perspective that we would remove the deterrent of a class action claim seeking relief under the Privacy Act from the risk-benefit analysis of a potentially reckless data custodian who is considering whether it is worthwhile to incur the cost of reasonable security measures.*

According to the Court of Appeal, then, a careless database defendant can be the target of a statutory tort claim under the *Privacy Act*.

With respect to common law negligence, the application judge dismissed the plaintiffs' claim on the basis that they could not show they were owed a private duty of care. As Justice Wilkinson saw it, the plaintiffs grounded their claim in an alleged breach of section 30 of FIPPA[1], but "*in British Columbia, the courts have held that there is no private law duty of care based on breach of s. 30 of FIPPA and no private law duty of care should be otherwise recognized in the circumstances*". Justice Wilkinson quotes the Court of Appeal's decision in *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468, writing that FIPPA provides "*a comprehensive complaint and remedy scheme for violations of s. 30… it is proper to infer that the legislature did not intend parallel common law remedies to exist*".

While the Court of Appeal found that Justice Wilkinson was correct that the breach of a statutory duty does not give rise to a private law duty of care, it rejected the suggestion that FIPPA is a "*complete code*" for all claims related to disclosure of personal information. The Court held that the existence of a statutory duty does not prevent a plaintiff from making a negligence claim in relation to a common law duty on the same subject. While breach of FIPPA section 30 is not independent grounds for a negligence claim, a failure to adequately safeguard personal information (the subject of the duty it imposes) is: "*[a] common law duty of care can co-exist alongside a statutory duty, as a general rule… FIPPA does not displace common law rights to pursue civil actions that arise from breach of privacy or careless storage of personal information by public bodies*". The Court of Appeal does not say that the plaintiffs' arguments will succeed, or even that they have a good chance of success, but Justice Wilkinson was wrong to find it "*plain and obvious*" that they would not succeed.

The impact of the Court of Appeal's decision to allow the application to proceed remains to be seen. The Court made its comments in the context of certification of class proceedings, where a court's concern is not to too hastily deny plaintiffs their chance at redress in a way that conserves judicial resources and reduces duplication of efforts. For now— barring an appeal— the plaintiffs have a second chance to achieve certification of their class proceeding before the Supreme Court. Nonetheless, public bodies should be mindful of their obligations to protect personal information in their care, because the consequences of careless storage may expose them to statutory and common law liability claims that they might previously have thought were precluded.

July, 2024

Aidan Andrews

Footnotes:

1. **30** A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.

AIDAN ANDREWS
604.358.0252
AIDAN@CIVICLEGAL.CA

Aidan is an associate lawyer with the firm and maintains a general municipal law practice, with particular interest in land use planning, judicial review, and freedom of information and privacy matters. Aidan has provided advice to local governments about zoning compliance, use of park land, and the scope of easements. As well, he has drafted leases and section 219 covenants, advised on conflict of interest and code of conduct issues, and assisted with submissions to the Office of the Information and Privacy Commissioner for British Columbia. Aidan has assisted with the preparation of pleadings in bylaw enforcement matters and written submissions to the Court of Appeal for British Columbia.

Aidan obtained his Juris Doctor from the University of Victoria and was called to the Bar of British Columbia in 2024, after articling with a municipal law boutique in Vancouver. During law school, Aidan spent time working for a full-service law firm, a disability non-profit, and two administrative tribunals. Aidan previously obtained a Bachelor of Arts in Political Science from the University of Regina.

Our lawyers combine legal experience in local government, commercial real estate development, and construction law to provide legal services to local governments, owners, builders and developers on a range of projects, from concept to completion, and beyond.

710 - 900 West Hastings Street, Vancouver, BC V6C 1E5
604.639.3639 | www.civiclegal.ca | @CivicLegal