YOUNG ANDERSON
BARRISTERS & SOLICITORS

September 6, 2022

BULLETIN

BC SUPREME COURT FINDS ICBC VICARIOUSLY LIABLE FOR ITS EMPLOYEE'S BREACH OF THE *PRIVACY ACT*

A recent British Columbia Supreme Court decision has opened possible new areas of liability for public bodies whose employees breach someone's privacy. In *Ari v. Insurance Corporation of British Columbia,* 2022 BCSC 1475, the Court found that an ICBC employee had breached the privacy of a number of ICBC customers, as well as the privacy of people living at those customers' homes. The employee breached their privacy when she accessed ICBC customers' information without authority to do so. The Court held that this violated BC's *Privacy Act*. That Act, which dates to the 1970s, provides that it is a "tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another." Significantly, the Court found that ICBC was liable for its employee's wrongdoing. This means that local governments could in the right circumstances be held liable for damages under the *Privacy Act* where their employees violate someone's privacy.

Background:

In 2011, ICBC was approached by the police as part of an investigation into a series of shootings and arsons committed against the homes and vehicles of several individuals. ICBC discovered that information of 79 ICBC customers had been accessed by one of its employees without an apparent business purpose. It turned out the employee had sold these customers' information to individuals who later carried out the attacks. ICBC fired the employee and she and later pleaded guilty to the crime of fraudulently obtaining a computer service.

The affected customers brought a class action against ICBC and the employee under the *Privacy Act*. After a long series of procedural rulings, which included two trips to the Court of Appeal, the Court held the employee and ICBC liable for invasion of privacy, with damages to be fixed later.

Decision:

The Court held that ICBC's employee had breached the *Privacy Act* when she improperly accessed the customers' personal information. The decision does not clearly describe the entire scope of what personal information was accessed, but it "included registered vehicle owner's names, addresses, driver's licence numbers, vehicle descriptions, vehicle identification numbers, licence plate numbers and claims histories". The Court found that a reasonable person providing this information to ICBC would expect it to be used only in relation to ICBC business, such as vehicle registration and insurance. The Court also ruled that the employee was, or ought to have been,

aware that accessing the information was prohibited. The Court noted that she had read and signed ICBC's information and security policies multiple times in the course of her employment and had completed information and privacy tutorials in the past. There was no evidence that what she did was the result of an accident or mistake.

Significantly, the Court makes it clear that the privacy breach occurred when the employee accessed the information, ruling that it did not matter whether she later sold the information. The privacy breach was complete when she "improperly accessed customer information, whether or not she passed the information to a third party. … Once she improperly accessed an individual customer's information, the customer was at risk from any use she may have chosen to put it to."

Even more significantly, the Court found that ICBC was vicariously liable for the employee's breach of the *Privacy Act*. It held that ICBC had created the risk of wrongdoing by an employee in that position, as her job as a claims adjuster by necessity entailed her accessing personal information stored on ICBC databases. The Court also found that her wrongdoing was directly connected to her employment, and that ICBC should have foreseen this risk, stating that, although she was expected to access the databases solely for purposes directly related to her job:

> … she clearly had the opportunity to access them for improper purposes if she wished to do so. The risk of such conduct by an employee was not only foreseeable, it was actually foreseen. Employees were told of the need to protect the privacy of customers' personal information and warned of adverse consequences if they accessed that information for reasons unrelated to ICBC's business.
>
> ICBC had in place rules and policies forbidding improper use of its databases, but the possibility of an individual employee choosing to ignore them was clearly foreseeable and there is no evidence of any system or method that would have prevented or detected that conduct at the time it happened.

The Court did not explain what "system or method" ICBC ought to have implemented, but presumably an automated system for detecting improper access might qualify. The cost and impracticality of such systems are notable, and it is not clear what else a public body might do to prevent rogue employees from abusing their information access privileges. Perhaps spot audits might pass muster if they are diligently designed and rigorously implemented, but this remains to be tested.

<u>Key Takeaways:</u>

The first key takeaway for local governments is the Court's conclusion that the privacy breach occurred as soon as the personal information was improperly accessed. It did not matter whether the employee sold the information or used it for her own purposes. This is significant because

many instances of improper access to personal information involve someone snooping on others' personal information. An employee may access personal information with the intention of distributing it to embarrass or harass the victim, but without doing so in the end. Or the employee may only be curious to know something about a relative or acquaintance. This decision clearly indicates that, regardless of the purpose for the snooping, and regardless of whether the information is used or not in some way, the breach is complete as soon as the personal information is accessed.

Second, this case shows that a local government may be held liable in damages for their employees' breach of the *Privacy Act*, even if the local government had policies or rules prohibiting the rogue employee from acting as they did. In the past, the greatest risk for a local government whose employee has breached someone's privacy was an investigation by the Office of the Information and Privacy Commissioner, which is serious enough, but *Ari* shows that local governments must now be mindful of the risk of both an OIPC investigation and the potential to be held vicariously liable for their rogue employee's wrongdoing.

Last, *Ari* confirms that damages under the *Privacy Act* may be awarded even if the victims are not out of pocket or otherwise harmed in any tangible way. The Court held that the plaintiffs are entitled to general damages, that they may be entitled to non-pecuniary damages depending on the harm they suffered, and that ICBC's liability for damages extends to property damage caused by the shootings and arson.

The litigation leading to this decision has been hard fought, so *Ari* may be appealed, but if it stands, the privacy compliance landscape has shifted materially.

David Loukidelis & James Barth