BEHIND THE SCREEN: NAVIGATING LAW ENFORCEMENT REQUESTS POST *R V. BYKOVETS*

Posted on March 22, 2024

Categories: Insights, Publications

In *R v. Bykovets*,[1] a 5-4 majority of the Supreme Court of Canada ("**SCC**") found that individuals have a reasonable expectation of privacy in their IP addresses and, as such, law enforcement require judicial pre-authorization (such as a search warrant or production order) to obtain access to them.[2]

The SCC's decision has obvious impact on law enforcement, but its effects are likely to be seen by businesses, who may receive a decrease in voluntary disclosure requests and an increase in formal production orders seeking personal information about their customers' internet activity.

In this article, we provide a brief overview of the SCC's decision and discuss important considerations under Canadian privacy law when determining the extent to which a business may disclose personal information to law enforcement without consent.

Facts

At the heart of the case was a credit card fraud involving the use of unauthorized credit card data to purchase gift cards. During its investigation, the Cybercrimes unit of the Calgary police learned that the credit card payments were managed by a third-party payment processor. The police asked for and the payment processor voluntarily provided the IP addresses associated with the fraudulent purchases.[3] With the IP addresses in hand the police were able to identify the defendant's internet service provider ("**ISP**") through publicly accessible sources and then obtain a production order to compel the ISP to disclose the name and address of the customers associated with each IP address.[4] This ultimately led to the arrest of the defendant, and eventual appeal before the SCC.

The appellant alleged that the police's original request for the IP addresses to the payment processor violated his right against unreasonable search and seizure under section 8 of the Canadian Charter of Rights and Freedoms (the "***Charter***").[5]

SCC Decision

A 5-4 majority of the SCC found that there is a reasonable expectation of privacy in IP addresses and that, as

such, law enforcement needs judicial authorization to obtain access to them.[6]

The majority's decision emphasized that for section 8 of the *Charter* to effectively safeguard the online privacy of Canadians, it must protect IP addresses.[7] In reaching its conclusion, the majority looked beyond the information that an IP address directly reveals about an internet user and focused instead on the opportunity for further investigation that the IP address enables. In this sense, the majority found that beyond a mere string of numbers, IP addresses are a key to unlocking a user's internet activity.[8] The SCC characterized an IP address as the "first digital breadcrumb" that can lead to an individual's identity and, for this reason, attracts a reasonable expectation of privacy.[9]

The majority's analysis was driven by a concern that the internet's architecture offers law enforcement an opportunity to circumvent *Charter* restrictions through voluntary cooperation with the private sector.

The Court observed that online businesses are well positioned to compile significant repositories of internet user activity and are often requested by law enforcement to voluntarily disclose such information to assist with criminal investigations.[10] The result is the potential displacement of the *Charter* by the private sector as the arbiter of the government's ability to access sensitive personal information. In finding a reasonable expectation of privacy in an IP address, police would instead have to obtain judicial pre-authorization before approaching third parties to access such information.[11]

How Should Businesses respond to Law Enforcement Requests for Customer Information?

Businesses operating in Canada are subject to private sector privacy laws, such as Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") or substantially similar provincial legislation.[12]

Canadian privacy laws generally require businesses to obtain consent to disclose an individual's personal information. However, PIPEDA contains certain exceptions that allow for disclosure to law enforcement without consent in certain circumstances. For example, PIPEDA allows disclosure without consent if the disclosure is made in response to a request by a government institution that identifies its authority to obtain such information or if the disclosure is necessary to comply with a subpoena, warrant, court order or production order.[13] PIPEDA also allows voluntary disclosure of personal information to law enforcement if there is reasonable grounds to believe that the information relates to a matter of national security or to the commitment of a crime or offence.[14]

Bykovets centres on the ability of law enforcement to request information from third parties and does not address the requirement to voluntary cooperate with such requests. With that said, the decision can be expected to result in a decrease in voluntary disclosure requests and an increase in production orders.

While facilitating law enforcement investigations is essential for public safety, it should be balanced with protecting individuals' privacy rights and the organization's requirements under privacy laws.[15] Businesses operating within Canada should therefore conduct an assessment prior to disclosing personal information to law enforcement to ensure a valid exception under applicable privacy laws applies.

[1] *R. v. Bykovets*, 2024 SCC 6 ["*Bykovets*"].
[2] *Bykovets*, at 90 and 91.
[3] *Bykovets*, at 98.
[4] *Bykovets*, at 98.
[5] The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11.
[6] *Bykovets*, at 91.
[7] *Bykovets*, at 28.
[8] *Bykovets*, at 28.
[9] *Bykovets*, at 9 and 91.
[10] *Bykovets*, at 10.
[11] *Bykovets*, at 89.
[12] Canada's other main private sector privacy laws are BC's *Personal Information Protection Act*, SBC 2003, c 63, Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5, and Québec's *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1.
[13] PIPEDA, s. 7(3)(c); s. 7(3)(d).
[14] PIPEDA, s. 7(3)(d).
[15] *Bykovets*, at 11, 71, 86.

by Robbie Grant, Mitch Koczerginski, Ada Ang (Articling Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.