MARCH 22, 2024

The Power and Peril of IP Addresses: The Supreme Court of Canada Weighs in on the Changing Landscape of Online Privacy

Authors: Léon H. Moubayed, Corey Omer, Alexander Max Jarvie, Alexandra Belley-McKinnon and Amélie Lehouillier

The Supreme Court of Canada recently delivered a landmark decision on the privacy rights of Internet users. In *R v Bykovets*, police investigating an alleged online fraud requested and obtained a suspect's Internet Protocol (IP) address from a third-party payment processor without a warrant. The police then used the IP address to identify and locate the suspect, and to seek and execute search warrants, which led to the suspect's arrest. The suspect challenged the police's warrantless request for his IP address as a violation of his right to be protected against unreasonable search and seizure, pursuant to section 8 of the *Canadian Charter of Rights and Freedoms*.

The majority of the Supreme Court held that IP addresses are subject to a reasonable expectation of privacy and that law enforcement must obtain a search warrant in order to access them. The Court's decision recognizes the vast amount of personal information held by private companies and more closely aligns Canadian criminal law with the expectations of privacy regulators. The decision is therefore expected to have important implications for online privacy in Canada.

Background

The appellant, Andrei Bykovets, was convicted of 14 offences related to fraudulent online purchases using unauthorized credit card data after the police requested the IP addresses associated with the purchases from Moneris, a third-party payment processor. Moneris voluntarily complied with the police's request and provided the IP addresses. Using public information, the police identified the Internet Service Provider (ISP) that owned the IP addresses and then obtained a production order for the subscriber information associated with the IP addresses. This production order was obtained in accordance with the requirements laid down by the Supreme Court in *R v Spencer* ("***Spencer***"), a 2014 decision in which the Court recognized a reasonable expectation of privacy in subscriber information held by ISPs. The police then used the subscriber information to obtain search warrants, which eventually led to Bykovets' arrest and subsequent conviction.

Bykovets argued that the police's request to Moneris for the IP addresses associated with the unauthorized purchases violated his section 8 *Charter* rights, and he applied to have the evidence excluded from the file under section 24(2) of the *Charter*. The trial judge held that there was no breach of section 8 and convicted Bykovets. The majority of the Court of Appeal of Alberta (2–1) upheld the conviction, finding that Bykovets did not have a reasonable expectation of privacy in his IP address because, standing alone, an IP address does not reveal any core biographical information. The courts below distinguished the case at hand—in which the police sought only the user's IP address, without any associated information about the user—from cases in which the police requested personal information associated with an IP address, such as the subscriber information in *Spencer*. The dissenting Court of Appeal judge took the position that Bykovets had a reasonable expectation of privacy in his IP address because it was linked to specific Internet activity that was being monitored and that was likely to reveal biographical information.

The Decision

The majority of the Supreme Court (5–4) reversed the Court of Appeal's decision and found that Bykovets had a reasonable expectation of privacy in his IP address. In her majority opinion, Karakatsanis J. emphasized that the Internet had changed the landscape of privacy and of informational self-determination, going so far as to state that the Internet has added private companies to the constitutional

ecosystem, "making the horizontal relationship between the individual and the state tripartite" (para 78). This, to the majority, appeared to justify a shift toward a more purposive approach to informational privacy cases.

In the case here, the majority focused on the potential of IP addresses to reveal intimate details of an individual's lifestyle and personal choices. The majority recognized the ubiquitous character of the Internet in our modern lives and found that IP addresses are the key to unlocking an Internet user's online activity—the first among many "digital breadcrumbs on the user's cybernetic trail" that have the potential to reveal sensitive and personal aspects of the user's life (para 69). The majority found that users may have a legitimate interest in keeping such information private—as they can do through the use of Virtual Private Networks—and that such information therefore deserves constitutional protection. The majority concluded that IP addresses therefore raised a reasonable expectation of privacy in that they are crucial links between Internet users and their online activity and can potentially reveal immense amounts of personal information.

The majority further refused to assess privacy interests in light of the state's declared intention to use the information for a single purpose—for example, to further an investigation. In an era in which private corporations can hold vast amounts of data, the majority cautioned against leaving it up to the private entity to decide whether or not to reveal an IP address. The Court held that state forces must have a search warrant to obtain such a sensitive piece of information. Consequently, the majority of the Supreme Court found that Bykovets' *Charter* right to be secure against unreasonable searches and seizures had been violated.

Writing on behalf of the dissenting justices, Côté J. criticized the majority's analysis and argued that, in this case, Bykovets' IP address, standing alone, hardly revealed private information, let alone deeply sensitive information; it merely revealed the Internet user's ISP. According to the dissenting justices, IP addresses could be compared to fingerprints left at the scene of a crime, over which a user has no control. The dissenting justices additionally warned that recognizing a reasonable expectation of privacy in IP addresses could hamper police investigations, especially those involving serious crimes, such as crimes against children.

Key Takeaways

The decision has significant implications for the privacy rights of Internet users in Canada and law enforcement procedures in the digital age.

First, the Supreme Court has taken a significant step in recognizing the vast amount of information, some of it highly personal and confidential, that may be collected by private companies, and its potential availability to government authorities. In *Bykovets*, the Supreme Court sends a strong message to courts across the country to ensure that applications of section 8 reflect the modern "technological reality" so that fundamental rights will be better protected during law enforcement searches.

Second, the decision underscores the importance of privacy in the online context and, with respect to IP addresses, signals a desire to align the application of section 8 of the *Charter* with the position generally taken by privacy regulators in their application of privacy laws. Regulators take a broad view of what qualifies as personal information, frequently noting that IP addresses can be considered personal information and can provide a starting point to compile a picture of an individual's online activities. Regulators have also paid particular attention to the ways in which personal information can become sensitive on the basis of the context in which it is used or when it is combined with other information. For example, in its Interpretation Bulletin with respect to sensitive information—a key concept in the *Personal Information Protection and Electronic Documents Act*—the Office of the Privacy Commissioner of Canada (OPC) noted that personal information which in isolation might be regarded as innocuous can take on a more sensitive nature when connected to services that may reveal the personal activities and preferences of users or when combined to create profiles.

As appears from the OPC's interpretation, the "sensitivity" of personal information is highly dependent on context, the extent to which the information may be linked with other information, and what inferences such context or combination may allow a third party to draw, echoing the "breadcrumbs" model that the majority of the Supreme Court embraced in *Bykovets*.[1]

Finally, this decision may have broader impacts on practices developed by some companies that track data about their Internet users or build profiles, and which may be willing to voluntarily disclose IP addresses to law enforcement upon request. The decision implies that private companies should be cautious before voluntarily disclosing users' personal information—even information that may at first blush appear non-sensitive or innocuous—in the absence of judicial authorization or clear authority to do so pursuant to applicable legislation.

Companies should also not take requests from law enforcement at face value, and they should, in the case of any doubt, request particulars as well as a copy of any authorization being relied upon.

More broadly, companies should consider adapting their processes and training to ensure requests from law enforcement are properly routed, considered, and responded to. They should also consider updating their personal information protection policies to reflect an appropriate treatment of IP addresses.

[1]This expansive view of personal information and its ability to reveal additional, potentially sensitive information about a person has also been recognized by other legislators, regulators and courts in Canada, the United States and Europe. See, for example: *Act respecting the protection of personal information in the private sector*, RSQ, c. P-39.1, s. 12, fourth paragraph; *California Consumer Privacy Rights Act*, which relies on the concept of "sensitive personal information" as a subcategory of personal information; section 9(1) of the EU's General Data Protection Regulation (full title: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*). Notably, the Court of Justice of the European Union has interpreted the special categories of personal data under the GDPR to include not only data directly reflecting the sensitive categories laid out in article 9(1) of the GDPR, but also "personal data that are liable to disclose *indirectly*" such information.

Key Contacts: Léon H. Moubayed, Corey Omer, Alexander Max Jarvie, Derek D. Ricci and Shari Cohen