Cassels

SCC Weighs in on IP Addresses as Personal Information – But Does the Answer Help?

Bernice Karn, Stephen I. Selznick, Misha Apel

March 6, 2024

By a recent 5/4 split decision in a criminal matter, the Supreme Court of Canada (SCC) found that a reasonable expectation of privacy attaches to an IP address[1] and that a request by police for an IP address is a search for which judicial authorization must be obtained. How relevant is this for companies collecting IP addresses in the normal course of business? Let's discuss.

Facts of the Case

While investigating fraudulent online purchases from a liquor store (using unauthorized credit card data to buy gift cards), police contacted the third-party payment processing company that managed the store's online sales to obtain the IP addresses used for the purchases. The payment processor voluntarily supplied the requested IP addresses to police, who obtained a production order compelling the relevant internet service provider to disclose the name and address of the customer for each IP address. The police then used this information to seek and execute search warrants for the residential addresses of the appellant, Bykovets, and his father. Bykovets challenged the request to obtain the IP addresses, alleging it violated his rights under section 8 of the *Canadian Charter of Rights and Freedoms*,[2] which guarantees the right to be secure against unreasonable search or seizure.

Majority Decision

The majority opinion found that there is a reasonable expectation of privacy in an IP address, and thus a request by the state for an IP address constitutes a search under Section 8 of the Charter. The Court applied a normative standard in analyzing the question, meaning that it looked at what the privacy rights under Section 8 of the Charter *should* be, balancing the individual's privacy rights against society's right to protection.

Writing for the majority, Justice Karakatsanis made the following findings in relation to IP addresses and privacy:

- The normative standard requires a broad, functional approach to the subject matter of the search and that the Court must focus on the potential for this subject matter to reveal personal or

biographical core information.[3]

- IP addresses are not just meaningless numbers. Rather, as the link that connects Internet activity to a specific location, IP addresses may betray deeply personal information — including the identity of the device's user — without ever triggering a warrant requirement. The specific online activity associated with the state's search can itself tend to reveal highly private information.[4]
- An IP address is the crucial link between an Internet user and their online activity…. Viewed normatively, it is the key to unlocking a user's Internet activity and, ultimately, their identity. Thus, an IP address attracts a reasonable expectation of privacy. If s.8 of the Charter is to meaningfully protect the online privacy of Canadians in today's overwhelmingly digital world, it must protect their IP addresses.[5]
- Even if the IP address does not itself reveal the user's identity, the prospect and ease of a *Spencer*[6] warrant means that the user's identity can later be revealed, not only in relation to the potentially criminal Internet activity in question, but in relation to all the information that can be inferred from the user's Internet activity.[7]

Further, Justice Karakatsanis concluded that "the burden imposed on the state by recognizing a reasonable expectation of privacy in IP addresses is not onerous…. [It] adds another step to criminal investigations by requiring that the state show grounds to intrude on privacy online… [which] in the age of telewarrants, [is a] hurdle [that] is easily overcome."[8]

Dissenting Opinion

Although the dissenting justices agreed with the normative standard and functional analytical approach in the case endorsed by the majority, they disagreed about the characterization of scope of the search, noting that the evidence at trial showed that the police did not actually use a third-party website's tracking capabilities to identify the appellant, a possibility that the majority seemed to rely upon in coming to the conclusion that an IP address, without name and address information from the relevant ISP, could lead to the identification of the individual. Justice Côté stated that the most significant difference between the majority and minority opinion was that the majority saw the scope of the search as "every step leading up to the ultimate identification of the suspect notwithstanding the fact that such information is not revealed by the IP addresses alone"[9] whereas the minority considered the IP addresses and the identity of the ISP revealed by them to be the scope of the impugned search.[10]

The dissenting opinion is interesting because the justices mentioned, in obiter, that it is inconsistent with a functional approach to effectively hold that *any* step taken in an investigation engages a reasonable expectation of privacy and that doing so could upset the balance between privacy rights and Canadians' interest in law enforcement.[11] The dissenting justices seemed particularly concerned with hindering undercover police operations, especially with respect to the protection of children.[12]

Another noteworthy comment made by Justice Côté “in passing” concerned third party websites voluntarily providing information without being asked. Justice Côté said that in such cases “the reasonable expectation of privacy analysis — which is always guided by “the totality of the circumstances” — could well be different.”[13] Unfortunately, she also said that this was an “issue for another day in a case where the situation actually arises on the facts.”[14]

Takeaways

Bykovets is a criminal case that has obvious implications for how law enforcement agencies investigating online crime conduct those investigations. However, what does it mean for commercial organizations that may be collecting IP addresses as part of their usual business activities?

The *Personal Information Protection and Electronic Documents Act*[15] contains various provisions that permit organizations engaged in commercial activities to disclose personal information without consent in certain cases. For example, section 7(3)(c.1) permits organizations to disclose personal information to “government institutions” upon request where they have identified their lawful authority to obtain the information and the collection of the information is for one of several enumerated law enforcement-related purposes. Based on *Bykovets*, should organizations that are otherwise willing to provide personal information to law enforcement now be requesting that the police come back with an order for the information? A cautious approach would suggest yes.

Another area to consider is how to handle IP address information – should organizations now be treating it as personal information as a matter of course, obtaining informed consent to collect, use and disclose it for listed purposes and providing appropriate security safeguards along with access and correction rights? As a result of this case, it’s hard to say whether IP addresses will always be treated as personal information; the answer is very much context-dependent. However, we recommend that organizations revisit their privacy policies to discuss their collection and handling of IP addresses. The careful management approach would be to treat these addresses as any other piece of personal information.

---

[1] *R v Bykovets*, 2024 SCC 6 (*Bykovets*).

[2] *Canadian Charter of Rights and Freedoms, s 8, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11* (Charter).

[3] *Bykovets* at para 7.

[4] *Bykovets* at para 9.

[5] *Bykovets* at para 28.

[6] *R v Spencer*, 2014 SCC 43 (*Spencer*). In this case, the SCC ruled that information attaching itself to an IP address has a reasonable expectation of privacy. *Bykovets* builds on this by extending this reasonable expectation of privacy to the IP address itself, not just the information.

[7] *Bykovets* at para 80.

[8] *Bykovets* at para 12.

[9] *Bykovets* at para 138.

[10] *Bykovets* at para 140.

[11] *Bykovets* at para 139.

[12] *Bykovets* at paras 139 and 159.

[13] *Bykovets* at para 135.

[14] *Bykovets* at para 135.

[15] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA).
