David Young Law
Compliance Bulletin

April 2024

IP addresses are personal - significance of the Supreme Court's ruling

In a split decision handed down March 1,[1] the Supreme Court of Canada ruled that Internet Protocol (IP) addresses – the numbered codes that are assigned to every device connected to the Internet – are information that attract a reasonable expectation of privacy. In other words, they are personal information.

In its narrowest sense, the decision tells us that IP addresses are personal information in any context, even if not attached to other identifiable information. However, more broadly, the decision characterizes such addresses as only one category of data provided by users when they interact with the Internet, data which inevitably must be considered personal even if not directly attached to identifiable information.

The decision focusses on the protections against unreasonable search and seizure provided under section 8 of the *Canadian Charter of Rights and Freedoms* and the implications for IP addresses in that context. However, the majority's reasons contain an insightful examination of the character and privacy implications of today's digital world. They accurately recognize the character of information flow on the Internet and the full scope of the Internet's dynamics, a characterization that is equally applicable to both public and private sector privacy ethics.

The Court's decision

During an investigation into fraudulent online purchases from an Alberta liquor store, police contacted the credit card processor that managed the store's online sales (Moneris) and, without a warrant, obtained the IP addresses used for the purchases. Police then obtained a production order compelling the Internet service provider ("ISP") to disclose the name and address of the customer for each IP address. Police used this subscriber information to seek and execute search warrants at the defendant's premises.

The defendant challenged the request by police to obtain the IP addresses from Moneris, alleging they violated his right against unreasonable search and seizure under s. 8 of the *Charter*. The trial judge convicted the accused, holding that the police's request to the processing company was not a search protected under s. 8 because the defendant did not have a reasonable expectation of privacy in his IP address. The Alberta Court of Appeal agreed.

The Supreme Court, on appeal, held that an IP address does attract a reasonable expectation of privacy and that the request by the police for the IP addresses was a search under s. 8 of the *Charter,* requiring a warrant. As a result, the Court allowed the appeal and ordered a new trial.

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

 © David Young Law 2024

An IP address is a unique identification number for any device connected to the Internet, assigned by the ISP to whose system the device is connected. It identifies the source of any online activity by the user of the device and through its "tracking" function enables the transfer of information from that source to another location on the Internet. IP addresses are necessary to any Internet activity.

The Crown argued that because IP addresses consist of simply numbers that can usually be changed by an ISP without notice, an IP address on its own does not attract a reasonable expectation of privacy.

The Court disagreed. It stated that IP addresses are not just meaningless numbers but, as the link that connect Internet activity to a specific location, they may betray deeply personal information — including the identity of the device's user. When combined with other online information associated with that IP address, such as that available from other Internet actors including search engines and social media, an IP address can reveal highly personal information resulting from the user's online activity. When associated with the profiles created and maintained by organizations whose function is to provide such profiles for commercial uses such as targeted marketing, the privacy issues related to such IP addresses are clear. The information collected, aggregated and analyzed by these providers enables them to develop files containing intimate biographical information about the user. The Court posited that an IP address is the first "digital breadcrumb" that can lead to the trail of an individual's Internet activity.

Significance of the decision

The ruling, while made in the context of a *Charter* challenge to a police search, has significant implications for the interactions of private sector organizations with online media.

The Court recognized the now ubiquitous presence of the Internet and its intrusion into our private lives. Most insightfully, the Court identified that Internet users leave behind a trail of information - which it characterized as "digital breadcrumbs" – collected by other Internet actors (e.g. websites, data brokers, ad networks) for potentially different purposes than those intended by the users. The Court posited that this information may be pieced together by such other parties to provide a deeply personal picture of an individual.

Recognition of this potentially expansive information gathering scope of the Internet is not a particularly novel or recent insight. Evolving laws and practices have led to ever-increasing rigour in protocols for privacy-compliant data collection (e.g. cookie notices).[2] However the Court's reasons in *Bykovets* articulate a recognition that, far beyond just IP addresses, the online world provides indicia of personal information in any interaction between users and the medium. Taking the Court's reasoning to its logical conclusion, almost any collection of such information, for any purpose, requires compliance with privacy rules - meaning that if consent is not understood or implied in the context, it must be obtained expressly.

[2] See for example, the EU *Cookie Directive* also known as the *ePrivacy Directive*, which requires sites to get consent from visitors before placing cookies on their devices; Quebec's *Law 25*, s. 8.1 which requires opt-in consent to any internet-based tracking for profiling purposes; *Meta Ireland* (opt-in consent required for data collection for ad targeting purposes).

In allowing the appeal the Court rejected the argument that the IP address on its own did not attract a reasonable expectation of privacy – that only with the additional information such as was obtained by warrant with aid of the IP address did privacy and section 8 become an issue. The Court stated that because of its potential to link to the extensive trove of information about the user that is available through the Internet, the IP address itself attracts a reasonable expectation of privacy.

The Court's decision will put an end to the uncertainty – even controversy – as to whether IP addresses should be considered personal information, in the absence of other, identifying information. An IP address is personal per se, based on what it can or might reveal, not only that which would be revealed in the context of its actual use. Notwithstanding that the circumstances and legal rules applied in the case were specific to the *Charter* and the public sector, the decision will have the likely result that in all instances IP addresses must be considered personal information requiring the same level of protection under both public and private sector privacy laws as is stipulated for more straightforward, identifiable instances of such information.

Takeaways

Several important take-aways can be identified.

Firstly, as noted, while a *Charter* case, the ruling likely will be determinative of the characterization of IP addresses generally and in particular as regulated by private sector privacy laws.

Secondly, IP addresses per se are personal information, not only if they are factually connected to other identifiable information.

Thirdly, IP addresses should be considered as just one example of the "digital breadcrumbs" left by Internet users, all of which likely warrant privacy protection. Online activity cannot be characterized as anonymous even if no identifiable personal information is disclosed within the actual interaction.

Finally, the Court recognized the concentration of personal information in the hands of what it called third (i.e. private) parties – meaning the diverse spectrum of online data collectors and users, including not only social media sites but also data brokers and various ad network parties – which it characterized as performing a role of "mediators" between law enforcement and private individuals. While the Court characterized parties in this sector as beyond the scope of *Charter* jurisdiction, it posited that their data collection activities have implications for privacy protections under the *Charter,* primarily because public sector parties such as the police often must rely on information held by such parties in conducting their investigations.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. © David Young Law 2024