SCC finds warrant is required before first digital breadcrumb can be revealed

06 mars 2024

In a 5-4 split, a majority of the Supreme Court of Canada (SCC) concluded in *R. v. Bykovets* that IP addresses attract a reasonable expectation of privacy, and thus a request by the police for an IP address is a search under section 8 of the *Canadian Charter of Rights and Freedoms* (*Charter*) requiring prior judicial authorization. This decision effectively expands the scope of the reasonable expectation of privacy by finding that not only the subscriber information associated with IP addresses attracts a reasonable expectation of privacy, but also the IP address itself.

The appeal was heard last year on Jan. 17, 2023, by a panel of seven judges Supreme Court judges, including Justice Brown, but not released prior to his leave and then departure from the Court. On Nov. 9, 2023, the Court ordered a re-hearing in writing which took place on Dec. 11, 2023, and was heard by all nine judges. Given the split in the panel, one would expect that the re-hearing was ordered to avoid a 3-3 split (unlike the recent decision in *R. v. Greater Sudbury (City)*.

Background

This case arises from a police investigation into an online fraudulent gift card purchase scheme. The police requested and received the IP addresses attached to the transactions from the payment processing company without prior judicial authorization. The police then presented a production order for the relevant IP addresses' subscriber information to the internet service provider (ISP), and then used the information obtained to acquire a search warrant, which led to the arrest and conviction of the appellant.

The SCC had previously unanimously held in *R v Spencer* that a reasonable expectation of privacy attaches to the subscriber information (name, contact information, and physical address) associated with an IP address. The central question on this appeal was whether an IP address itself attracts a reasonable expectation of privacy.

The trial judge found that it was not objectively reasonable to recognize a subjective expectation of privacy in an IP address used by an individual. At the Court of Appeal for Alberta (ABCA), the appellant relied on *Spencer* to argue that as the police were ultimately after his name and address, and this information fell within his "biographical

core of personal information" it invites a reasonable expectation of privacy. A majority of the ABCA disagreed and distinguished the case from *Spencer*. Since the police only discovered the appellant's identity after lawfully serving the ISP with a production order, they acted within their section 8 obligations and onside *Spencer*. In dissent, Veldhuis JA would have allowed the appeal and ordered a new trial. Justice Veldhuis found the case to be indistinguishable from *Spencer*, noting that the trial judge did not consider the potential of an IP address to reveal further details about a user or subscriber.

For a more detailed background on the facts and lower court decisions, please refer to our first article here.

SCC judgment – Majority: Section 8 of the *Charter* protects IP addresses

The central question on appeal was whether a reasonable expectation of privacy attaches to an IP address such that it would require the police to obtain prior judicial authorization to request it. The majority decision (Karakatsanis, Martin, Kasirer, Jamal, and Moreau JJ.), penned by Justice Karakatsanis, found that the answer to that question is yes. The majority recognized that informational privacy is becoming critical in this current digital age and viewed IP addresses as more than simply a string of meaningless numbers. Rather, it is the link connecting internet activity to a specific location, potentially betraying the identity of the device's user. Karakatsanis J. described it as "the first digital breadcrumb that can lead the state on the trail of an individual's Internet activity".

The majority rejected the Crown's argument that section 8 does not extend to an IP address because an IP address is collected by the police to later obtain a *Spencer* warrant. Karakatsanis J. found this analysis to reflect piecemeal reasoning based on the state's intention, which cannot be the determinative factor. Rather, it is crucial to consider what an IP address, in combination with other available information, could reveal.

To establish a breach of section 8 of the *Charter*, a claimant must show that there was a search or seizure, and that such a search or seizure was unreasonable. Only the first prong of the test was at issue in this case.

To meet the first part of the test and show that there was a search, a claimant must establish that the state invaded his or her reasonable expectation of privacy. This analysis requires the court to consider the subject matter of the search, the claimant's interest in the subject matter, the claimant's subjective expectation of privacy, and whether that subjective expectation of privacy was objectively reasonable.

Karakatsanis J. identified the nub of the subject matter of the search (*i.e.*, what the police were really after) as the information an IP address tends to reveal about a specific Internet user "including their online activity and, ultimately, their identity".

Turning to whether the expectation of privacy was objectively reasonable, the majority confirmed its departure from the American approach, which negates a reasonable expectation of privacy based on the "third party doctrine" (*i.e.*, if information is possessed or known by third parties there is no reasonable expectation of privacy). The

majority said that Canadians' privacy should not be a trade-off for using an ISP's services. In today's age, it does not constitute a meaningful choice, but rather a quasi-impossible one.

The heart of the analysis was in determining the private nature of the subject matter. The SCC has previously established that section 8 protects the "biographical core" of an individual, which includes information that "tends to reveal intimate details". The key question is what information the subject matter of the search tends to reveal. The majority found it entirely irrelevant to look at the police's intention to restrict the use of information in a given case. Instead, it focused on a broader interpretation, taking judicial notice of the ever-increasing intrusion of the Internet into individuals' private lives as a black hole absorbing a trail of information that may be pieced together to disclose deeply private details. The majority placed significant weight on the various categories of information an IP address may reveal, such as a user's political views, sexual preferences, purchase habits or medical history.

Finally, the majority focused on the shift of the topography of privacy under the *Charter* due to technological developments. That is, a third party was added to the constitutional ecosystem between the state and the individual. The *Charter* does not apply to private corporations. But due to the large amounts of personal information and data they hold, the majority found that notwithstanding this exemption, section 8 would apply to the tripartite relationship involving the corporation, the state, and individuals. The underlying reasoning, as Karakatsanis J. noted, is that these private corporations "mediate a relationship which is directly governed by the *Charter*". Private corporations respond to frequent requests by law enforcement and can volunteer the activity associated with the requested IP address. Therefore, they hold the power to share information that can strike at the heart of a user's biographical core, without a *Spencer* warrant.

In striking the appropriate balance between legitimate police investigations combatting increased online crime, and individuals' expectations of privacy, the majority found that such a balance would include police obtaining prior judicial authorization before obtaining an IP address. Given the "around-the-clock access to justices of the peace" and the availability of tele-warrants, they did not find this to be an onerous burden.

SCC judgment – Dissent: An IP address alone does not reveal private information and no reasonable expectation of privacy should be attached

Côté J., writing for the dissent (Wagner C.J., Côté, Rowe and O'Bonsawin JJ.), found that the appellant did not have a reasonable expectation of privacy in an IP address alone, without any other information linking him to that IP address. Côté J. disagreed with the majority's approach in describing the subject matter of the search as the identity of the user. While that may have been the ultimate result, she found that this was not information revealed by the raw IP address alone and was therefore not the subject matter of the search. What an IP address alone reveals is a user's ISP.

The most significant difference between the majority's and the dissent's opinions is that the majority includes in the subject matter analysis all the steps leading up to the ultimate identification of the suspect. Côté J. distinguished this case from *Spencer*,

where the subscriber information was the key to unlocking the identity of the person behind the IP address. Côté J. asserted that a characterization of the subject matter beyond the scope of what the immediate information sought *actually* revealed would be to effectively treat an ultimate goal of many police investigations (*i.e.,* the identification of the suspect) as the subject matter of the search.

Côté J. left the door open to the possibility of finding that in some circumstances, an IP address *may* attract a reasonable expectation of privacy. However, she criticized the majority's result that "not only some, but all, IP addresses attract a reasonable expectation of privacy", noting that such a conclusion "would seriously thwart the police's ability to investigate such serious offences against children".

Key takeaways

- The SCC's decision in *v Bykovets* expands the veil of individuals' reasonable expectations of privacy to account for the role of third-party private corporations as mediators between the state and individuals. That veil is only lifted when an independent judicial officer is satisfied that revealing this information to the state will serve a legitimate law enforcement purpose.
- The constitutional right to privacy will not be based on the state's declared intention with respect to the information sought, or according to one particular use of the information. The analysis must consider what information the subject matter of the search tends to reveal, when pieced together with other available information.
- The majority doubled down on the SCC's decision in *Spencer* by extending the obligation for a prior judicial authorization to the first step of requesting access to an IP address alone, thereby adding an additional investigative step that police will have to undertake when seeking to identify a suspect based on a trail of Internet activity.
- Technological advancements do not require Canadians to make an impossible choice between their privacy and being a part of today's society, which requires access to and use of an ISP's services. The majority rejected the alternative "choice" for Canadians who want to maintain their privacy stating that "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives".
- Privacy does not have one fixed meaning, especially in a time where more unconventional privacy violations are ubiquitous. The majority's decision highlights its progressive view in relation to privacy in light of emerging technologies and evolving societal expectations. The majority decision paves the way for a more robust section 8 interpretation, striking a balance between combatting online crime and individuals' reasonable privacy rights.

Par

Nadine Tawdy, Laura M. Wagner, Nadia Effendi

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels, Litiges, Technologies de l'information, Plaidoirie en appel, Droit des produits, Droits de la personne, Gouvernement et secteur public

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749