Torkin Manes
Barristers & Solicitors

Article

Technology, Privacy & Data Management

February 2020

IP Addresses No Longer Protected in Alberta

From a privacy perspective, the decision is “exceedingly troubling”

By Lisa R. Lifshitz

In a surprising decision, the Court of Queen’s Bench of Alberta recently held in *R. v. Bykovets* that there is no reasonable expectation of privacy in an Internet Protocol (IP) address and, as such, no warrant is required by police to obtain such information from service providers or other third parties.

The accused, Andrei Bykovets, was one of several facing charges under the Criminal Code relating to the possession and use of third-party credit cards and personal identification documents. His defense counsel argued that his rights under ss. 7, 8, 9 and 10(b) of the Charter were violated by the Calgary Polices Service (CPS) during the course of their investigation and asked that all evidence and derivative evidence acquired by the CPS be excluded from his trial.

Beginning in September 2017, the CPS Cybercrimes Investigation Team had begun to investigate certain individuals who allegedly purchased goods from various websites using fraudulent credit card information and gift cards. Payments for the cards were processed by a separate company, a subsidiary of Toronto-based Moneris. In October, CPS asked Moneris for purchaser information relating to five fraudulent purchases and in response, Moneris provided the IP addresses shown in their logs for the orders.

Accessing an open source website, the CPS determined that both IP addresses were issued by Telus. Later that month, CPS applied for and received a production order for the subscriber information associated with those IP addresses and Telus complied, providing the subscribers’ information and addresses, which happened to belong to Bykovets and his father. On November 16, 2017 the CPS obtained a search warrant that authorized them to search both residences. Significantly, Bykovets was prevented from seeking counsel during this time, in part to allow the officers to search the residences and because of concerns that someone could delete information from electronic devices, onsite or remotely.

IP addresses are a numerical identification and address assigned to each device connected to a computer network that uses the Internet Protocol for communication and are used for host or network interface identification and location addressing. Internet Protocol version 4 defines an IP address as a 32-bit number while Internet Protocol version 6 uses 128 bits for its IP addresses. External IP addresses are

assigned to subscribers by their Internet service providers (ISPs). They may be dynamic or static in nature but typically a residential subscriber would receive a dynamic address, which may be changed by an ISP at will and without notice. According to expert evidence presented at trial, the duration of an IP address can vary from a few days to a few months. However, ISPs do keep a record of whom the IP address was assigned and for what period of time (the duration of the record kept as determined by individual ISP); and each IP address is distinctly associated with one subscriber during its lease period.

Section 8 of the Charter states that "everyone has the right to be secure against unreasonable search or seizure" and the critical question for the Court was to determine whether an individual has a reasonable expectation of privacy in an IP address. Noting that the Crown was unable to point to Canadian jurisprudence addressing this specific issue, Justice Bernette Ho canvassed earlier case law, including the Supreme Court of Canada's ruling of *R. v. Spencer* as to whether a reasonable expectation of privacy exists. The court in Spencer considered such factors as the subject matter of the alleged search; the claimant's interest in the subject matter; the claimant's subjective expectation of privacy in the subject matter; and whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of circumstances.

Justice Ho distinguished various decisions (including *R. v. Jennings,* and *X (Re), 2017 FC 1047*) that had found the accused had a reasonable expectation of privacy in international mobile subscriber identity (IMSI) and international mobile equipment identity (IMEI) numbers obtained through the use of mobile device developers. Citing expert evidence, Justice Ho held that the nature of the information obtained from an IP address, or what may be inferred from the information, provides less information (and less personal information) about a particular individual, then IMSI/IMEI information. In her view the nature, quantity and quality of personal information gleaned from an IP address is limited and thus there is a significant difference between the nature of the information or what may be inferred when the police obtain an IP address, as compared to those predecessor cases. Justice Ho also stated that the IP address, on its own, did not provide a link to, or any other information about, a street address or a person. The IP addresses were used by CPS to subsequently seek subscriber information from the ISP, which was later accomplished by obtaining a warrant.

The Court also sought to distinguish the facts of this case against those in the Supreme Court's *R. v. Marakah*, taking a very narrow approach. For example, Justice Ho found that as a collection of numbers, an IP address does not disclose the "biographical core of personal information" nor does it communicate information about a particular claimant without more or reveal intimate details about a person's lifestyle. Accordingly, she determined that it is not objectively reasonable to recognize a subjective expectation of privacy in an IP address used by an individual.

"In my view, an IP address in itself does not reveal information about a subscriber that should be protected in a free and democratic society," Justice Ho wrote in her reasons. "While I acknowledge that the police might be able to obtain information about a user's identity, there are significant limitations on this. Obtaining an IP address is an important investigative step for police, but privacy interests are not triggered by mere police investigation. The Courts must continually ask the question, "what are the police really after?" including where electronic devices, technology and digital information are concerned. There must continue to be a balancing of interests in determining the scope of section 8 of the Charter" (paragraph 62).

The Court observed that the CPS were able to access a public lookup listing IP addresses to identify an ISP and ultimately sought judicial authorization before obtaining specific subscriber information from that ISP. Distinguishing against the facts in the Spencer case, Justice Ho commented that there is "nothing to be gained" from requiring the police to seek a judicial order earlier in the investigation to obtain the IP addresses "since the IP address may not reveal much information to police at all." Justice Ho ultimately concluded that "finding a reasonable expectation of privacy in an IP address would not advance the protection of privacy interests in a free and democratic society" and accordingly Mr. Bykovets'' section 8 Charter rights were not violated.

Interestingly, the Court did find Mr. Bykovets' section 10(b) Charter rights (the right on arrest or detention to retain and instruct counsel without delay and to be informed of that right) to have been violated because the Crown failed to justify their delay of his right to obtain counsel. Justice Ho found as well that the CPS had also violated the accused's section 7 Charter rights (the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice)

because critical evidence against the accused – a manila folder containing, amongst other things, the handwritten notes made by the Forensic Analyst relating to the examination of USB sticks seized at the accused's house – was lost by the CPS. Thus, the Crown failed to discharge the onus that the evidence was not lost due to "unacceptable negligence," resulting in a finding that Mr. Bykovets' section 7 Charter rights were violated. As the Court concluded that it will be necessary for counsel to provide submissions for remedy based on these Charter breaches, it is unclear at this time whether this trial will continue or whether Mr. Bykovets' counsel will challenge the findings regarding s. 8 of the Charter.

This judgment is exceedingly troubling in many respects. For example, the decision is vague as to how the CPS obtained the IP addresses from Moneris – did they just call the up and ask for the information? As merely the third-party payment processor, why did Moneris disclose this information to the CPS without a warrant, since it was not even the website that was actual the subject of the crime? And if so, was this practice in compliance with Alberta's Personal Information Protection Act and if applicable, the federal Personal Information Protection and Electronic Documents Act?

Not surprising, my fellow privacy lawyer and friend David Fraser has publicly raised similar observations, so at least I know I am not the only one bothered by this state of affairs.

Justice Ho's analysis also flies in the face of consistent guidance and decisions from Canadian privacy regulators, including multiple decisions of the Office of the Privacy Commissioner of Canada (OPC), beginning as far back as 2001, that have held IP addresses to be personal information if they can be associated with an identifiable individual.

Moreover, the Court's exceptionally narrow analysis of the larger privacy impact of disclosing IP addresses without warrants on the basis that the "nature, quantity and quality of personal information gleaned from an IP address is limited" struck me as very naïve from a greater privacy, and societal perspective.

In a report prepared by the Technology Analysis Branch of the OPC dated May 2013 entitled "What an IP Address Can Reveal About You," the Commissioner found that knowing an IP address has larger impacts, as it can be used to obtain other information about networks, devices and services, potentially leading the identity of individuals.

Based on the foregoing, I am not persuaded by Justice Ho's assertion that an IP address in itself does not reveal information about a subscriber that should be protected "in a free and democratic society." If we can agree that obtaining IP addresses is an "important investigative step for police," then the police continue to seek warrants to obtain them. Notwithstanding this judgment, let us hope (and assume) this continues to be the practice – and the law – in Canada in the meantime.

This article was originally published in Canadian Lawyer magazine.

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the immediate past president of the Canadian IT Law Association.