SCC to decide: Does reasonable expectation of privacy attach to IP address?

January 24, 2023

Introduction

On Jan. 17, 2023, the Supreme Court of Canada (SCC) heard the case of *Andrei Bykovets v. His Majesty the King* (40269). This appeal is of significant importance to Canadians' privacy rights, specifically their informational privacy, as it addresses the interpretation of section 8 of the *Canadian Charter of Rights and Freedoms* (Charter) protecting individuals from unjustified intrusions by the government.

The SCC has already developed a strong body of jurisprudence around section 8 privacy rights and circumstances where an individual's reasonable expectation of privacy (REP) will be violated. For instance, in *R v Spencer*, 2014 SCC 43, the SCC held that police are required to obtain judicial authorization through a search warrant or production order before asking an internet service provider (ISP) to identify a specific user associated with a specific IP address. This case will offer more clarity as to the scope of the REP because the entity in question was not an ISP.

Facts

The police initiated an investigation into online fraudulent gift card purchases after learning the credit card data of several individuals had been used online without their permission. Moneris, the company that processed the online transactions, revealed the two IP addresses attached to the transactions to the police. The police then applied for and received a production order for the IP addresses' subscriber information from TELUS, who provided police with the names and addresses of the appellant and his father. The police subsequently acquired a warrant, lawfully searched the appellant's and his father's house and seized incriminating evidence leading to the appellant's conviction. The appellant filed a notice alleging the breach of his section 8 *Charter* rights (among others) claiming he had a REP attached to his IP address.

Lower court decision

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. She concluded that there

was no breach of section 8 and the appellant was convicted of 13 counts, which he appealed.

At the Court of Appeal of Alberta, the appeal was dismissed. The appellant argued that his name and address were what the police intended to uncover when they approached Moneris without a court order. Relying on the *Spencer* decision, the appellant argued that since this information fell within his "biographical core of personal information," [1] it invites a REP and as a result, the police ought to have obtained a court order before requesting it from Moneris. A majority at the Court of Appeal disagreed and distinguished the case from *R v Spencer*. In *Spencer*, the police obtained, an IP address and its subscriber data without judicial authorization, whereas in this case, the police obtained *only* the IP addresses from Moneris. Since the police only discovered the appellant's identity after lawfully serving TELUS with a production order, they acted within their section 8 obligations and onside the *Spencer* decision. Moreover, with the suppression of crime being a legitimate countervailing technique, the majority found this approach to strike the proper balance between individual REPs and legitimate police investigative techniques.

In dissent, Veldhuis JA would have allowed the appeal and ordered a new trial. Justice Veldhuis found the case to be indistinguishable from *R v Spencer*, noting that the trial judge did not consider the potential of an IP address to reveal further details about a user or subscriber. Veldhuis JA concluded that IP addresses were "linked to a particular, monitored internet activity that could disclose biographical core information,"[2] and agreed with the appellant that there was a REP and accordingly prior judicial authorization was required to obtain the IP addresses from Moneris. Veldhuis JA's conclusion would widen the scope of when a REP is to be expected when considering the privacy interests attached to IP addresses, and would have imposed the *Spencer* court order requirements to the police in this case.

SCC hearing

At the hearing before the SCC, a host of questions arose around the potential implications of finding that a REP is attached, or not, to IP addresses. For instance, what if companies come forward with information about a potential crime happening online and volunteer that information to the police – are the police prohibited from using that information because they did not seek a warrant? Further, if the court attaches a REP to IP addresses only in certain circumstances and in relation to certain crimes, how would the third party company know what the crime at issue is when police approaches them?

On the other hand, if an IP address alone reveals nothing unless combined with subscriber data, why should police need a warrant to access it? Does it not simply add an unnecessary roadblock to the preliminary phase of investigations?

Takeaways

As at the Court of Appeal of Alberta, the core interest permeating the SCC's questioning surrounds balancing individual REPs against legitimate police investigative techniques: should the court rule there is a REP in IP addresses and impose an obligation to seek a

court order before requesting this information, or rule no such REP exists, thereby permitting the police to request IP address information without a warrant?

This is certainly a case to watch in the coming months, as the court's approach to determining individual REPs with respect to IP addresses will undoubtedly inform the court's future approach to section 8 and any privacy rights to be found thereunder - an especially timely indicator given the federal government's imminent release of Bill C-27.

[1] *R v Bykovets*, 2022 ABCA 208 at 14.

[2] *Ibid* at 94.

By

Nadine Tawdy, Shane Morganstein

Expertise

Cybersecurity, Privacy & Data Protection, Disputes, Administrative and Public Law, Appellate Advocacy

---