SUPREME COURT OF CANADA

CITATION: R. *v.* Bykovets, 2024 SCC 6

APPEAL REHEARD: December 11, 2023
JUDGMENT RENDERED: March 1, 2024
DOCKET: 40269

BETWEEN:

Andrei Bykovets
Appellant

and

His Majesty The King
Respondent

- and -

Director of Public Prosecutions, Attorney General of Ontario, Attorney General of British Columbia, Canadian Civil Liberties Association and British Columbia Civil Liberties Association
Interveners

CORAM: Wagner C.J. and Karakatsanis, Côté, Rowe, Martin, Kasirer, Jamal, O'Bonsawin and Moreau JJ.

REASONS FOR JUDGMENT: (paras. 1 to 92)

Karakatsanis J. (Martin, Kasirer, Jamal and Moreau JJ. concurring)

DISSENTING REASONS: (paras. 93 to 165)	Côté J. (Wagner C.J. and Rowe and O'Bonsawin JJ. concurring)

Andrei Bykovets *Appellant*

v.

His Majesty The King *Respondent*

and

Director of Public Prosecutions,
Attorney General of Ontario,
Attorney General of British Columbia,
Canadian Civil Liberties Association and
British Columbia Civil Liberties Association *Interveners*

Indexed as: R. *v.* Bykovets

2024 SCC 6

File No.: 40269.

Hearing: January 17, 2023.

Present: Wagner C.J. and Karakatsanis, Côté, Brown, Martin, Jamal and O'Bonsawin JJ.

Rehearing: December 11, 2023.

Judgment: March 1, 2024.

Present: Wagner C.J. and Karakatsanis, Côté, Rowe, Martin, Kasirer, Jamal, O'Bonsawin and Moreau JJ.

ON APPEAL FROM THE COURT OF APPEAL OF ALBERTA

Constitutional law — Charter of Rights — Search and seizure — Police investigating fraudulent online transactions — Police contacting payment processing company to request internet protocol ("IP") addresses associated with transactions — Payment processing company voluntarily providing IP addresses to police and accused consequently arrested — Whether reasonable expectation of privacy attaches to IP address — Whether request by state to third party for IP address constitutes search — Canadian Charter of Rights and Freedoms, s. 8.

During an investigation into fraudulent online purchases from a liquor store, police contacted the third-party processing company that managed the store's online sales and 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. B was arrested.

B challenged the request by police to obtain the IP addresses from the processing company, alleging it violated his right against unreasonable search and seizure under s. 8 of the *Charter*. The trial judge held that the police's request to the processing company was not a search under s. 8 of the *Charter* because B did not have

a reasonable expectation of privacy in his IP address; therefore, B's s. 8 right was not engaged. B was convicted of 14 offences related to the fraudulent online purchases. The majority of the Court of Appeal agreed that B had no reasonable expectation of privacy in his IP addresses and dismissed B's conviction appeal. The dissenting judge would have allowed the appeal, on the basis that a reasonable expectation of privacy attached to the IP addresses.

Held (Wagner C.J. and Côté, Rowe and O'Bonsawin JJ. dissenting): The appeal should be allowed and a new trial ordered.

Per **Karakatsanis**, Martin, Kasirer, Jamal and Moreau JJ.: 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. 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. Accordingly, a request by the state for an IP address is a search under s. 8 of the *Charter*.

Section 8 of the *Charter* guarantees the right to be secure against unreasonable search or seizure. Its principal object is the protection of privacy, including informational privacy, that is, the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Personal privacy is vital to individual dignity, autonomy, and

personal growth. Its protection is a basic prerequisite to the flourishing of a free and healthy democracy.

To establish a breach of s. 8, a claimant must first show that there was a search or seizure. A search occurs where the state invades a reasonable expectation of privacy. An expectation of privacy is reasonable where the public's interest in being left alone by the government outweighs the government's interest in intruding on the individual's privacy to advance its goals, notably those of law enforcement. Courts analyze an expectation of privacy by considering many interrelated but often competing factors, which can be grouped together under four categories: (1) the subject matter of the search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy; and (4) whether the subjective expectation of privacy was objectively reasonable. In the case at bar, the parties agreed that B had a direct interest in the IP addresses and a subjective expectation of privacy in their informational content.

With respect to the subject matter of the search, it is defined not only in terms of the information itself, but also the tendency of information sought to support inferences in relation to other personal information. A court must take a holistic view of the subject matter and must be especially careful in describing the subject matter of a search touching electronic data. The approach must not be mechanical, and it must reflect technological reality. The subject matter of the search in the instant case was the information that IP addresses could reveal about specific Internet users including,

ultimately, their identity. Recognizing that police wanted the IP address — as the link between a specific subscriber and location and particular Internet activity — to obtain more information about the user lets the court assess the expectation of privacy in relation to all the information this IP address tends to reveal.

With respect to whether a subjective expectation of privacy is objectively reasonable, courts must look to the totality of the circumstances. While there is no definitive list of factors, courts have often focussed on control over the subject matter, the place of the search, and the private nature of the subject matter. In the informational privacy context, the claimant's control over the subject matter is not determinative. The Internet requires that users reveal subscriber information to their ISP to participate in this new public square, and Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives. Nor is the place where the search occurred detrimental to a reasonable expectation of privacy in such a context. Online spaces are qualitatively different from physical spaces. The information the Internet harbours can reveal much more than information subject to the limits of physical space. Therefore, a lack of physical intrusion reveals little about the reasonableness of an expectation of privacy.

As to the private nature of the subject matter, s. 8 seeks to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. The biographical core is not limited to identity, but includes information which tends to

reveal intimate details of the lifestyle and personal choices of the individual. Section 8's emphasis on such information means that a reasonable expectation of privacy is assessed normatively rather than simply descriptively. It cannot be assessed according to only one particular use of the evidence; nor can its reach be determined according to the police's specific intention in seeking the information. Rather, the purpose of s. 8, appreciated normatively, requires asking what information the subject matter of the search tends to reveal. As the link that connects specific Internet activity to a specific location, an IP address may betray deeply personal information, even before police try to link the address to the user's identity. Moreover, activity associated with the IP address can be correlated with other online activity associated with that address available to the state. An IP address can also set the state on a trail of Internet activity that leads directly to a user's identity, even without a warrant compelling an ISP to disclose the name and address of the customer for the IP address. Access to IP addresses without judicial pre-authorization poses intense privacy risks.

Defining a reasonable expectation of privacy is an exercise in balance. In this case, the balance weighs in favour of extending a reasonable expectation of privacy to IP addresses. The intensely private nature of the information an IP address may betray strongly suggests that the public's interest in being left alone should prevail over the government's interest in advancing its law enforcement goals. The Internet has exponentially increased both the quality and quantity of information stored about Internet users, spanning the most public and the most private human behaviour. The Internet has not only allowed private corporations to track their users, but also to build

profiles of their users filled with information the users never knew they were revealing. By concentrating this mass of information with private third parties and granting them the tools to aggregate and dissect that data, the Internet has essentially altered the topography of privacy under the *Charter*. It has added a third party to the constitutional ecosystem, making the horizontal relationship between the individual and the state tripartite. Though third parties are not themselves subject to s. 8, they mediate a relationship which is directly governed by the *Charter* — that between defendant and police. This shift has enhanced the state's informational capacity.

Weighed against these substantial privacy concerns is society's sometimes conflicting but legitimate interest in the need for safety and security. Police should have the investigative tools to deal with crime that is committed and facilitated online. However, requiring that police obtain prior judicial authorization before obtaining an IP address is not an onerous investigative step. Where the IP address, or the subscriber information, is sufficiently linked to the commission of a crime, judicial authorization is readily available. Recognizing that an IP address attracts s. 8 protection aims to make sure police investigations better reflect what each reasonable Canadian expects from a privacy perspective and from a crime control perspective. Judicial oversight narrows the state's online reach and removes the decision to disclose information — and how much to disclose — from private corporations and returns it to the purview of the *Charter*.

Per Wagner C.J. and **Côté**, Rowe and O'Bonsawin JJ. (dissenting): The appeal should be dismissed. B did not have a reasonable expectation of privacy in the IP addresses on the credit card processor's servers and the ISP they revealed. The police did not need judicial authorization before asking the processor for the IP addresses in order to determine the ISP associated with them. However, this conclusion does not foreclose the possibility that someone may have a reasonable expectation of privacy on different facts.

Section 8 of the *Charter* is meant to protect against state intrusion on an individual's privacy and comes into play only where a person's reasonable expectations of privacy are somehow diminished by an investigatory technique. The reasonable expectation of privacy test is fact-specific and contextual and depends on the totality of the circumstances of a particular case. The test is normative, not descriptive. Its objective is to determine what degree of privacy one ought to have, not what degree of privacy one actually has.

Identifying the subject matter of the search is a key question in the totality of the circumstances analysis. To identify the subject matter of the search, the court must examine the connection between the police investigative technique and the privacy interest at stake. It must consider not only the nature of the precise information sought, but also the nature of the information that it reveals. The court is concerned with the capacity of the precise information sought to give rise to inferences or to reveal further information. These inferences and this further information form part of the true

subject matter of the search. Once the subject matter of the search is identified, the question then becomes whether a subjective expectation of privacy in the subject matter of the search is objectively reasonable. Whether an expectation of privacy is reasonable depends on several factors. These may include the place of the search, control over the subject matter of the search, the private nature of the subject matter, whether the subject matter was in public view, whether the subject matter was abandoned, whether the subject matter was already in the hands of third parties, whether the search method was intrusive in relation to the privacy interest at stake, whether the search method was itself unreasonable, and whether the search exposed core biographical information. Not all factors will be relevant to the analysis in a particular case and no single factor is determinative.

In the instant case, the factors relevant to the reasonableness inquiry are the private nature of the subject matter, control over the subject matter, and the place of the search. The private nature of the subject matter of a purported search can support a finding that an expectation of privacy is reasonable. The issue is not simply whether the subject matter itself is private, but also whether it can reveal other essential private information. This factor is of particular importance with respect to informational privacy interests. Where informational privacy alone is at stake, it may be all but essential that the information itself be private in order for a reasonable expectation of privacy to exist. Control over the subject matter of the search generally supports a finding that there was a reasonable expectation of privacy, while lack of control may weigh against such a finding. The place of the search informs the reasonableness of any

expectation of privacy in it. The idea of place essentially relates to the concept of territorial privacy and necessarily assumes less significance in cases which engage informational privacy.

There is disagreement with the majority's assessment of the subject matter of the supposed search in the instant case. The majority includes in the subject matter 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, according to the evidence in the record. The correct way to characterize the subject matter of the search is to describe it as the IP addresses and the ISP revealed by them.

B's subjective expectation of privacy in the subject matter of the search was not objectively reasonable. The IP addresses at issue were not private and did not, on the facts of the case, reveal private information. Without more, all an IP address reveals to the police is a user's ISP — hardly a particularly private matter, let alone core biographical information. In addition, the factor of control points away from a finding that B's expectation of privacy was reasonable. B had little control over the IP addresses, which an ISP can change at will and without notice. An Internet user who leaves behind IP address data completely loses control over what happens to those numbers. Finally, the alleged search was not carried out at B's home. The place of the search was the credit card processor's database. Its location does not enhance the objective reasonableness of B's subjective expectation of privacy.

Cases Cited

By Karakatsanis J.

Referred to: *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Reeves*, 2018 SCC 56, [2018] 3 S.C.R. 531; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696; *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Ramelson*, 2022 SCC 44; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Spence*, 2005 SCC 71, [2005] 3 S.C.R. 458; *State v. Simmons*, 190 Vt. 141 (2011); *Breyer v. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779; *Vidal-Hall v. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003; *Quebec (Attorney General) v. 9147-0732 Québec inc.*, 2020 SCC 32, [2020] 3 S.C.R. 426; *R. v. Mills*, 2019 SCC 22, [2019] 2 S.C.R. 320; *R. v. Friesen*, 2020 SCC 9, [2020] 1 S.C.R. 424; *R. v. Wong*, [1990] 3 S.C.R. 36.

By Côté J. (dissenting)

R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Evans*, [1996] 1 S.C.R. 8; *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Reeves*, 2018 SCC 56, [2018] 3 S.C.R. 531; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R.

456; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Stairs*, 2022 SCC 11; *R. v. Mills*, 2019 SCC 22, [2019] 2 S.C.R. 320; *Breyer v. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779; *Vidal-Hall v. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003; *Altimo Holdings v. Kyrgyz Mobil Tel Ltd*, [2011] UKPC 7, [2012] 1 W.L.R. 1804; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Feeney*, [1997] 2 S.C.R. 13; *R. v. McNeil*, 2009 SCC 3, [2009] 1 S.C.R. 66; *R. v. O'Brien*, 2023 ONCA 197, 166 O.R. (3d) 114; *R. v. Ilia*, 2023 ONCA 75, 523 C.R.R. (2d) 128; *R. v. Allen*, 2020 ONCA 664, 396 C.C.C. (3d) 1; *R. v. West*, 2020 ONCA 473, 392 C.C.C. (3d) 271; *R. v. Caza*, 2015 BCCA 374, 376 B.C.A.C. 258; *R. v. Smith*, 2005 BCCA 334, 199 C.C.C. (3d) 404; *R. v. Friesen*, 2020 SCC 9, [2020] 1 S.C.R. 424; *R. v. Find*, 2001 SCC 32, [2001] 1 S.C.R. 863; *R. v. McGregor*, 2023 SCC 4; *R. v. Sharma*, 2022 SCC 39; *R. v. Spence*, 2005 SCC 71, [2005] 3 S.C.R. 458; *In re The Board of Commerce Act, 1919, and The Combines and Fair Prices Act, 1919*, [1922] 1 A.C. 191.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, s. 8.

Criminal Code, R.S.C. 1985, c. C-46, ss. 487.015(1), 691 to 693.

Supreme Court Act, R.S.C. 1985, c. S-26, s. 40(3).

Authors Cited

Austin, Lisa M. “Getting Past Privacy? Surveillance, the Charter, and the Rule of Law” (2012), 27 *C.J.L.S.* 381.

Austin, Lisa M. “Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints” (2016), 17 *Theoretical Inquiries L.* 451.

Canada. Office of the Privacy Commissioner. *What an IP Address Can Reveal About You: A report prepared by the Technology Analysis Branch of the Office Privacy Commissioner of Canada*. Gatineau, 2013.

Cockfield, Arthur J. “Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance” (2003), 29 *Queen’s L.J.* 364.

Hasan, Nader, et al. *Search and Seizure*. Toronto: Emond Montgomery, 2021.

Hogg, Peter W., and Wade K. Wright. *Constitutional Law of Canada,* 5th ed. Supp. Toronto: Thomson Reuters, 2022 (updated 2023, release 1).

Kennedy, Pagan. “William Gibson’s Future Is Now”, *The New York Times*, January 13, 2012 (online: https://www.nytimes.com/2012/01/15/books/review/distrust-that-particular-flavor-by-william-gibson-book-review.html).

Magotiaux, Susan. “Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence” (2015), 71 *S.C.L.R.* (2d) 501.

Matsumi, Hideyuki. “Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?” (2017), 48 *Cumb. L. Rev.* 149.

Olivetti Rason, Nino, and Sara Pennicino. “Comparative Law in the Jurisprudence of the Supreme Court of Canada”, in Giuseppe Franco Ferrari, ed., *Judicial Cosmopolitanism: The Use of Foreign Law in Contemporary Constitutional Systems*. Boston: Brill/Nijhoff, 2019, 140.

Panneck, Travis. “Incognito Mode Is in the Constitution” (2019), 104 *Minn. L. Rev.* 511.

Sharpe, Robert J., and Kent Roach. *The Charter of Rights and Freedoms,* 7th ed. Toronto: Irwin Law, 2021.

Slane, Andrea. “Privacy and Civic Duty in *R v Ward*: The Right to Online Anonymity and the *Charter*-Compliant Scope of Voluntary Cooperation with Police Requests” (2013), 39 *Queen’s L.J.* 301.

Tene, Omer. “What Google Knows: Privacy and Internet Search Engines”, [2008] *Utah L. Rev.* 1433.

APPEAL from a judgment of the Alberta Court of Appeal (Veldhuis, Schutz and Crighton JJ.A.), 2022 ABCA 208, 55 Alta. L.R. (7th) 76, 509 C.R.R. (2d) 213, [2023] 5 W.W.R. 51, [2022] A.J. No. 738 (Lexis), 2022 CarswellAlta 1454 (WL), affirming a decision of Ho J., 2020 ABQB 70, 10 Alta. L.R. (7th) 103, 453 C.R.R. (2d) 347, [2020] A.J. No. 135 (Lexis), 2020 CarswellAlta 174 (WL). Appeal allowed, Wagner C.J. and Côté, Rowe and O'Bonsawin JJ. dissenting.

Heather Ferg and *Sarah Rankin*, for the appellant.

Rajbir Dhillon, for the respondent.

David W. Schermbrucker and *Allyson Ratsoy*, for the intervener the Director of Public Prosecutions.

Andrew Hotke, for the intervener the Attorney General of Ontario.

Micah B. Rankin and *Michael Barrenger*, for the intervener the Attorney General of British Columbia.

Anil K. Kapoor and *Cameron Cotton O'Brien*, for the intervener the Canadian Civil Liberties Association.

Daniel J. Song, K.C., and *Vibert M. Jack*, for the intervener the British Columbia Civil Liberties Association.

The judgment of Karakatsanis, Martin, Kasirer, Jamal and Moreau JJ. was delivered by

KARAKATSANIS J. —

I. Introduction

[1] The Internet has shifted much of the human experience from physical spaces to cyberspace. It has grown to encompass public squares, libraries, markets, banks, theatres, and concert halls, becoming the most expansive cultural artifact our species has ever created. Along with our shopping mall and our town hall, for many of us, the Internet has become a constant companion, through which we confide our hopes, aspirations, and fears. Individuals use the Internet not only to find recipes, pay bills, or get directions, but also to explore their sexualities, to map out their futures, and to find love.

[2] These new realities have forced courts to grapple with "a host of new and challenging questions about privacy" (*R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 1). In *Spencer*, this Court determined that a reasonable expectation of privacy attaches to subscriber information — the name, address, and contact information — associated with an individual Internet Protocol (IP) address. A request for this information by the state is a "search" under s. 8 of the *Canadian Charter of Rights and Freedoms*.

[3] This appeal asks whether an IP address itself attracts a reasonable expectation of privacy. The answer must be yes.

[4] An IP address is a unique identification number. IP addresses identify Internet-connected activity and enable the transfer of information from one source to another. They are necessary to access the Internet. An IP address identifies the source of every online activity and connects that activity (through a modem) to a specific location. And an Internet Service Provider (ISP) keeps track of the subscriber information that attaches to each IP address.

[5] But because IP addresses consist of numbers that can usually be changed by an ISP without notice, the Crown submits — and the majority of the Court of Appeal agreed — that an IP address does not attract a reasonable expectation of privacy. Here, the Crown contends that police were after no more than the collection of numbers that would ultimately allow them to obtain the production order contemplated by *Spencer*. Thus, the Crown reasons, the state did not infringe on the appellant's right to privacy because *Spencer* sufficiently protected his personal information.

[6] I respectfully disagree. This analysis runs counter to this Court's jurisprudence under s. 8 of the *Charter*. We have never approached privacy piecemeal, based on police's stated intention to use the information they gather in only one way. The right against unreasonable search and seizure, like all *Charter* rights, must receive a broad and purposive interpretation, reflective of its constitutional source. Since *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, we have held that s. 8 seeks to prevent

breaches of privacy, rather than to condemn or condone breaches based on the state's ultimate use of that information. Privacy, once breached, cannot be restored.

[7] To that end, our Court has applied a normative standard to reasonable expectations of privacy. We have defined s. 8 in terms of what privacy *should* be — in a free, democratic, and open society — balancing the individual's right to be left alone against the community's insistence on protection. This normative standard demands we take a broad, functional approach to the subject matter of the search and that we focus on its *potential* to reveal personal or biographical core information (*R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 32).

[8] Informational privacy is particularly critical — and particularly challenging. Our jurisprudence recognizes that computers are unique and present privacy risks that differ from s. 8's traditional objects. Thus, this Court has determined that s. 8 generally prevents police from seizing a computer without a warrant — even though the device itself provides no information without judicial permission to search its contents — because seizing the computer gives the state the means through which to access its content (*R. v. Reeves*, 2018 SCC 56, [2018] 3 S.C.R. 531, at para. 34).

[9] Casting the subject matter of this search as an abstract string of numbers used solely to obtain a *Spencer* warrant goes against these precedents. 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. Correlated with other online information associated with that IP address, such as that volunteered by private companies or otherwise collected by the state, an IP address can reveal a range of highly personal online activity. And when associated with the profiles created and maintained by private third parties, the privacy risks associated with IP addresses rise exponentially. The information collected, aggregated and analyzed by these third parties lets them catalogue our most intimate biographical information. Viewed normatively and in context, an IP address is the first digital breadcrumb that can lead the state on the trail of an individual's Internet activity. It may betray personal information long before a *Spencer* warrant is sought.

[10] And the Internet has concentrated this mass of information with private third parties operating beyond the *Charter*'s reach. In this way, the Internet has fundamentally altered the topography of informational privacy under the *Charter* by introducing third-party mediators between the individual and the state — mediators that are not themselves subject to the *Charter*. Private corporations respond to frequent requests by law enforcement and can volunteer all activity associated with the requested IP address. Private corporate citizens can volunteer granular profiles of an individual user's Internet activity over days, weeks, or months without ever coming under the aegis of the *Charter*. This information can strike at the heart of a user's biographical core and can ultimately be linked back to a user's identity, with or without a *Spencer* warrant. It is a deeply intrusive invasion of privacy.

[11] Weighed against society's legitimate interest in privacy is society's legitimate interest in "[s]afety, security and the suppression of crime" (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 17). While the right to be left alone must keep pace with technological developments, the way in which crime is committed and investigated also evolves. Easy access to the Internet and user anonymity combine to facilitate the commission of crime and challenge effective law enforcement. Clearly, the particularly insidious nature of much online crime, including child pornography and luring, presents serious and pressing social harm. Police must have the tools to investigate these crimes. And when an IP address (or subscriber information) is clearly linked to a crime — as it obviously can be for child pornography or luring — prior judicial authorization is readily available. A production order for an IP address would require little additional information to what police must already provide for a *Spencer* warrant. Both society's interest in effective law enforcement and its interest in protecting the informational privacy rights of all Canadians must be respected and balanced.

[12] On balance, the burden imposed on the state by recognizing a reasonable expectation of privacy in IP addresses is not onerous. This recognition adds another step to criminal investigations by requiring that the state show grounds to intrude on privacy online. But in the age of telewarrants, this hurdle is easily overcome where the police seek the IP address in the investigation of a criminal offence. Section 8 protection would let police pursue the Internet activity related to their law enforcement goals while barring them from freely seeking the IP address associated with online

activity *not* related to the investigation. Judicial oversight would also remove the decision of whether to reveal information — and how much to reveal — from private corporations and return it to the purview of the *Charter*.

[13] As a crucial component inherent in the structure of the Internet, an IP address is the key that can lead the state through the maze of a user's Internet activity and is the link through which intermediaries can volunteer that user's information to the state. Thus, s. 8 ought to protect IP addresses. Doing so would safeguard the first "digital breadcrumb" and shroud the trail of an Internet user's journey through cyberspace; it would further s. 8's purpose of preventing potential infringements of privacy rather than circumscribe its scope according to the state's stated intentions about how it will use this key.

[14] I would allow the appeal. There is a reasonable expectation of privacy in an IP address. A request by the state for an IP address constitutes a search.

II. Background

[15] The appellant, Andrei Bykovets, was convicted of 14 offences for using unauthorized credit card data to buy gift cards online, using those gift cards to make purchases in store, and possessing material related to credit card fraud.

[16] During the Calgary Police Service's investigation into fraudulent online purchases from a liquor store, police learned that the store's online sales were managed

by Moneris, a third-party payment processing company. Police contacted Moneris to obtain the IP addresses used for the transactions, and Moneris voluntarily identified two. Police then obtained a production order compelling the addresses' ISP to disclose the subscriber information — the name and address of the customer — for each IP address, as required by *Spencer*. One was registered to the appellant, the other to his father.

[17] Police then used this subscriber information to seek and execute search warrants for the residential addresses of the appellant and his father. The appellant was arrested, convicted after a trial, and his convictions were confirmed on appeal.

[18] Before trial, the appellant alleged that the police's request to Moneris violated his right against unreasonable search and seizure under s. 8 of the *Charter*. The key issue on the *voir dire* was whether the appellant had a reasonable expectation of privacy in his IP address.

[19] Defence counsel submitted a forensic investigator's expert report providing a technical summary of IP addresses and their functions. The report showed that there are internal and external IP addresses. External IP addresses are used to transfer information across the Internet from one source to another through a modem rented from the ISP. An external IP address is much like the street address of an individual's house. Without one, a user can neither send nor receive data. A modem or router also assigns an internal IP address to each device on a local network, roughly equivalent to the individual rooms in a house.

[20] IP addresses can also be static or dynamic. Most are dynamic, meaning that the ISP can change a user's external IP address without notice and for any number of reasons. ISPs keep a record of which subscriber each external IP address was assigned to and for what time period.

[21] A user's ISP can be determined by entering their IP address into an IP lookup website. The police can then request subscriber information for the assigned IP address from the ISP, as contemplated by *Spencer*. That said, the expert explained that one may still take steps to determine a user's identity, without resorting to an ISP, through the information logged on the website of a third-party company. Third-party companies, such as Google or Facebook, can track the external IP addresses of each user who visits their site and log this information to varying degrees. These companies can determine the identity of those individual users based on their Internet activity on their sites (expert report, reproduced in A.R., at p. 311). The effect is compounded when information from multiple sites is collected (p. 312).

[22] Thus, in the expert's view, if those seeking to identify a particular Internet user have access to information logged by third-party companies, "it is not necessary to obtain ISP-held subscriber information in order to accurately identify a particular internet user" (p. 312).

III. Decisions Below

A. *Court of Queen's Bench of Alberta, 2020 ABQB 70, 10 Alta. L.R. (7th) 103 (Ho J.)*

[23] The trial judge held that the police's request to Moneris was not a search under s. 8 of the *Charter* because the appellant did not have a reasonable expectation of privacy in his IP address. Considering the factors laid down by this Court in *Tessling*, she defined the subject matter of the alleged search as IP addresses sought for the purpose of furthering the investigation. She considered the expert report and reasoned that, on their own, IP addresses do not provide a link to, or any other information about, an Internet user (para. 44).

[24] As a result, the appellant's subjective expectation of privacy in his IP address was not reasonable because the IP address did not disclose a "biographical core of personal information" without access to a third-party website (para. 56). The trial judge saw "little to be gained from a normative perspective" by "requiring the police to seek judicial authorization" when accessing the IP address itself rather than when accessing the subscriber information connected to that IP address (para. 64, citing *Spencer*).

B. *Court of Appeal of Alberta, 2022 ABCA 208, [2023] 5 W.W.R. 51 (Schutz and Crighton JJ.A., Veldhuis J.A. Dissenting)*

[25] The majority of the Court of Appeal dismissed the appeal, largely for the reasons of the trial judge. Schutz and Crighton JJ.A. agreed that the appellant had no reasonable expectation of privacy in his IP address because, standing alone, it reveals

nothing of a person's lifestyle or core biographical information. What little information the IP address communicated was overwhelmed by "legitimate countervailing concerns": ". . . safety, security, and the suppression of crime . . ." (para. 22).

[26] In dissent, Veldhuis J.A. would have allowed the appeal because the trial judge did not "undertake her analysis with the normative approach in mind" (para. 62). Properly characterized, the subject matter of the search was not the IP address itself, but "the identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity" (para. 77).

[27] Veldhuis J.A. concluded that the appellant's expectation of privacy in that subject matter was reasonable. A person communicating financial information to make an online purchase would expect the IP address used to remain private, and that information was of a private nature because it could identify an Internet user "without any requirement for reasonable suspicion or grounds to support judicial authorization" (para. 88). Thus, a reasonable expectation of privacy attached to these IP addresses because "they were linked to a particular, monitored internet activity that could disclose biographical core information" (para. 94).

IV. Analysis

[28] This appeal raises a single issue: Does a reasonable expectation of privacy attach to an IP address? In my view, the answer is yes. As I will explain, an IP address is the crucial link between an Internet user and their online activity. Thus, the subject

matter of this search was the information these IP addresses could reveal about specific Internet users including, ultimately, their identity. To find that s. 8 does not extend to an IP address because police collected it only to obtain a *Spencer* warrant ignores the information it *can* reveal without a warrant. Such an analysis reflects piecemeal reasoning based on how the state intends to use the information in a specific case, contrary to the broad, purposive approach required by s. 8's constitutional status. Nor can the analysis be limited to the privacy interests affected by what the IP address can reveal *on its own*, without consideration of what it can reveal in combination with other available information, particularly from third-party websites. Viewed normatively, an IP address is the key to unlocking a user's Internet activity and, ultimately, their identity, such that it attracts a reasonable expectation of privacy. If s. 8 is to meaningfully protect the online privacy of Canadians in today's overwhelmingly digital world, it must protect their IP addresses.

A. *Legal Framework*

[29] Section 8 of the *Charter* guarantees "the right to be secure against unreasonable search or seizure". Its principal object is the protection of privacy, or the individual's "right to be left alone" (*R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 67). Personal privacy is vital to individual dignity, autonomy, and personal growth (*R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696, at para. 38). Its protection is a basic prerequisite to the flourishing of a free and healthy democracy.

[30] To establish a breach of s. 8, a claimant must show there was a search or seizure, and that the search or seizure was unreasonable. Only the first requirement — whether the request for the IP addresses was a search — is at issue here.

[31] A search occurs where the state invades a reasonable expectation of privacy. An expectation of privacy is reasonable where the public's interest in being left alone by the government outweighs the government's interest in intruding on the individual's privacy to advance its goals, notably those of law enforcement (*Hunter*, at pp. 159-60). Courts analyze an expectation of privacy by considering many interrelated but often competing factors, which can be grouped together under four categories: (1) the subject matter of the search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy; and (4) whether the subjective expectation of privacy was objectively reasonable (*Spencer*, at para. 18, citing *Tessling*, at para. 32).

[32] This case is about informational privacy, or "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (*Tessling*, at para. 23, quoting A. F. Westin, *Privacy and Freedom* (1970), at p. 7). In other words, this aspect of privacy is concerned with "informational self-determination" (*Jones*, at para. 39).

[33] The parties agree that the appellant had a direct interest in the IP addresses and a subjective expectation of privacy in their informational content. In the next

sections, I address the subject matter of the search and whether the appellant's expectation of privacy in that subject matter was reasonable.

B. *The Subject Matter of the Search*

[34] Considering the subject matter of the alleged search allows the court to identify the privacy interests at issue (*Spencer*, at para. 22). A guiding question in defining the subject matter of the alleged search is "what were the police really after?" (*Marakah*, at para. 15, citing *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 67). A court must take a holistic view of the subject matter of the search. The approach must not be mechanical, and it must reflect technological reality (*Spencer*, at paras. 26 and 31; *Marakah*, at para. 17).

[35] Here, the appellant asks us to adopt the dissenting judge's characterization of the subject matter. What the police were really after, he says, was "to connect an internet activity to a specific person. Obtaining an IP address was an essential step in identifying the internet user responsible for specific internet activity" (A.F., at para. 37).

[36] The respondent Crown argues for the characterization of the trial judge and the majority of the Court of Appeal. Police "wanted the IP addresses to further [their] investigation" (R.F., at para. 53).

[37] In my view the trial judge and the majority of the Court of Appeal adopted an artificially narrow description of the subject matter of this alleged search. It is at odds with our precedents' normative approach and fails to capture the privacy interests at stake in this case.

[38] This Court has never described the constitutional right to privacy according to the state's declared intention, or according to one particular use of the information. Rather, we have consistently taken a broad and functional approach to the subject matter of the search, "examining the connection between the police investigative technique and the privacy interest at stake" (*Spencer*, at para. 26). The subject matter is defined not only in terms of the information itself, but also "the tendency of information sought to support inferences in relation to other personal information" (para. 31). In *Marakah*, for example, the issue was whether the sender of a text message has a reasonable expectation of privacy in that text message on the recipient's device. Writing for the majority, McLachlin C.J. determined that the subject matter of the search was not the recipient's telephone, or even the text message itself, but an "electronic conversation" including "any inferences about associations and activities that can be drawn from that information" (para. 20).

[39] Courts must be especially careful in describing the subject matter of a search touching electronic data (*Marakah*, at para. 14). In *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, where police had examined the contents of a computer, this Court

described the subject matter of the alleged search as "the data, or *informational content* of the laptop . . . not the devic[e] [itself]" (para. 41 (emphasis in original)).

[40] Similarly, in *Reeves*, where police had seized the appellant's shared home computer, the search was not merely for the computer itself, but "ultimately the data it contained about Reeves' usage, including the files he accessed, saved and deleted" (para. 30). The state engaged s. 8 by seizing the computer *even though* police needed a warrant to search its contents because, through the seizure, police "obtained the means through which to access [highly private] information" (para. 34).

[41] The same is true here. Police were not "really after" IP addresses in the abstract. As "a collection of numbers", an IP address is of no interest to police. Rather, police were after the information an IP address tends to reveal about a specific Internet user including their online activity and, ultimately, their identity "as the source, possessor or user of that information" (*Spencer*, at para. 47). As the identifier of Internet-connected activity originating at a specific location, an IP address is a powerful tool that allows the state — with or without another warrant — to collect a user's Internet activity over the time period a particular IP address is linked to that source. Thus, as in *Reeves*, an IP address provided the state with the *means* through which to draw immediate and direct inferences about the user behind specific Internet activity. The information inferred from a device's Internet activity can be deeply personal, including linking that activity to a particular user's identity (see *Spencer*, at para. 47).

[42] This description takes a broad and functional view of the subject matter. By "properly avoid[ing] a mechanical approach that defines the subject matter in terms of physical acts, spaces, or modalities of [informational] transmission", it "reflects the technological reality" (*Marakah*, at para. 17). This description does not extend the shield of *Charter* protection to every investigatory step. Instead, it affirms that investigative techniques that reveal seemingly innocuous information must still be examined in connection with the privacy interest at stake (*Spencer*, at para. 26). Recognizing that police wanted the IP address — as the link between a specific subscriber and location and particular Internet activity — to obtain more information about the user lets the court assess the expectation of privacy in relation to *all* the information this IP address "tends to reveal" (*Spencer*, at para. 27 (emphasis in original), quoting *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293), and, therefore "by reference to the nature of the privacy interests potentially compromised by the state action" (*Marakah*, at para. 15, citing *Ward*, at para. 65 (emphasis added)).

[43] Thus, the subject matter of this alleged search is an IP address as the key to obtaining more information about a particular Internet user including their online activity and, ultimately, their identity as the source of that information. Here, police sought to obtain that information through a production order as contemplated by *Spencer*. But, as the expert report states, a *Spencer* warrant is not the only way an IP address can reveal intimate details of an Internet user's lifestyle and personal choices. Online activity associated to the IP address may itself betray highly personal

information without the safeguards of judicial pre-authorization. I turn to that issue next.

C. *Was the Expectation of Privacy Reasonable?*

[44] Section 8 is engaged only where a subjective expectation of privacy is objectively reasonable. The question, in all cases, is "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement" (*Hunter*, at pp. 159-60).

[45] Courts must make this determination in the totality of the circumstances. While there is no definitive list of factors (*Cole*, at para. 45), courts have often focussed on the claimant's control over the subject matter, the place of the search, and the private nature of the subject matter (see, e.g., *Marakah*, at para. 24).

(1) Control Over the Subject Matter

[46] In the informational privacy context, the claimant's control over the subject matter is not determinative (*Reeves*, at para. 38). The self-determination at the heart of informational privacy means that individuals "may choose to divulge certain information for a limited purpose, or to a limited class of persons, and nonetheless retain a reasonable expectation of privacy" (*Jones*, at para. 39). Anonymity is a

particularly important conception of privacy when it comes to the Internet (*Spencer*, at para. 45, citing Westin, at p. 32).

[47] Our approach is distinct from that of the United States, where the so-called "third-party doctrine" negates a reasonable expectation of privacy "if information is possessed or known by third parties" (T. Panneck, "Incognito Mode Is in the Constitution" (2019), 104 *Minn. L. Rev.* 511, at p. 520, quoting D. J. Solove, "A Taxonomy of Privacy" (2006), 154 *U. Pa. L. Rev.* 477, at p. 528). This Court rejected the American approach at an early stage of our s. 8 jurisprudence (*R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 429-30, per La Forest J.).

[48] The non-determinative nature of control in our analysis is particularly relevant for the Internet, which requires that users reveal subscriber information to their ISP to participate in this new public square. As we said in *Jones*, "the only way to retain control over the subject matter of the search vis-à-vis the service provider was to make no use of its services at all. That choice is not a meaningful one. . . . Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives" (para. 45).

(2) The Place of the Search

[49] Nor is the place where the search occurred detrimental to a reasonable expectation of privacy here. This factor was largely developed in the context of territorial privacy, and digital subject matter "does not fit easily within the strictures

set out by the jurisprudence" (*Marakah*, at para. 27). As this Court recently remarked, "online spaces are *qualitatively* different" from physical spaces (*R. v. Ramelson*, 2022 SCC 44, at para. 49 (emphasis in original)).

[50] The architecture of the Internet has led to a broad, accurate, and continuously expanding permanent record "without precedent in our society" (*R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at para. 40 (emphasis in original), quoting A. D. Gold, "Applying Section 8 in the Digital World: Seizures and Searches", prepared for the 7th Annual Six-Minute Criminal Defence Lawyer (June 9, 2007), at para. 3). The information the Internet harbours can reveal much more than information subject to the limits of physical space (see *Vu*, at paras. 44 and 47). Therefore, the lack of physical intrusion highlighted by the trial judge tells us little about the reasonableness of an expectation of privacy.

(3) The Private Nature of the Subject Matter

[51] Section 8 seeks "to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" (*Plant*, at p. 293). The "biographical core" is not limited to identity, but "include[s] information which tends to reveal intimate details of the lifestyle and personal choices of the individual" (p. 293).

[52] Section 8's emphasis on information which individuals "would wish to maintain and control from dissemination to the state" means that a reasonable

expectation of privacy is assessed normatively rather than simply descriptively (*Spencer*, at para. 27, quoting *Plant*, at p. 293). The normative approach has an aspirational quality. "The question is whether the privacy claim must 'be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society'" (*Reeves*, at para. 28, quoting *Ward*, at para. 87). Thus, s. 8 will extend as far as privacy ought to extend to protect individual dignity, autonomy, and personal growth, and no further. Or, as Doherty J.A. put it, recognizing a reasonable expectation of privacy means "the impugned state conduct has reached the point at which the values underlying contemporary Canadian society dictate that the state must respect the personal privacy of individuals unless it is able to constitutionally justify any interference with that personal privacy" (*Ward*, at para. 82). This analysis is inevitably "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy" (*R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 14).

[53] Thus, a reasonable expectation of privacy, as s. 8's operative component, cannot be assessed according to only one particular use of the evidence. Nor can its reach be determined according to the police's specific intention in seeking the information. Rather, the purpose of s. 8, appreciated normatively, requires that we ask what information the subject matter of the search tends to reveal. Because this analysis seeks to determine "whether people generally have a privacy interest" in the subject matter of the state's search, we consider not only the information that police seek to

uncover in a particular case, but all the information that the subject matter may tend to uncover (*Patrick*, at para. 32).

[54] This principle is especially clear where there is a search of digital information. Computers are different. These devices store immense amounts of information — some of which is automatically generated and retained unbeknownst to the user — which can touch the biographical core of personal information (*Vu*, at para. 41). These privacy interests can be even more palpable if the device is used to connect to the Internet (*Cole*, at para. 47). Indeed, "it is difficult to imagine a more intrusive invasion of privacy" than searches concerning an individual's use of the Internet (*R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 105).

[55] The unique and heightened privacy interests in personal computer data flows from its *potential* to expose deeply revealing information. In *Vu*, this Court found that the search of a computer requires specific pre-authorization because computers are a repository for an almost limitless universe of information (at para. 41); and information relating to the user's Internet activity "can also enable investigators to access intimate details about a user's interests, habits, and identity" (para. 42). Even though police in that case were merely trying to determine who lived in the home, the Court still concluded there were serious privacy interests engaged by the search.

[56] Similarly, in *Reeves*, the severity of the privacy concerns arising from the seizure of a computer was unaffected by the police's specific intention to search the computer for child pornography. Rather, these concerns stemmed from "the personal

or confidential nature of the data that is preserved and potentially available to police through the seizure of the computer" (para. 33 (emphasis added), citing *Marakah*, at para. 32). The Constitution should protect against the seizure of a computer because, in doing so, police "obtained the means through which to access [highly private] information" (*Reeves*, at para. 34).

[57] The police's specific intention to restrict the use of information in a particular case — no matter how well-intentioned — is thus irrelevant to s. 8. The "reasonable expectation of privacy" analysis revolves around the *potential* of a particular subject matter to reveal an individual's biographical core to the state, not whether the IP addresses revealed information about the appellant *on these facts*. McLachlin C.J. made this point explicit in *Marakah* where she wrote that "the potential for revealing private information is a factor to consider in determining whether an electronic conversation attracts a reasonable expectation of privacy" (para. 31; see also para. 32). Thus, text messages attracted a reasonable expectation of privacy regardless of whether the text messages sought revealed any information on the facts of that case.

[58] Moreover, in applying a normative standard, it is not helpful to focus on the narrowest interpretation of the expert evidence. Rather, we must assess the evidence in its broader context, including the prevailing social realities and the impact of our decision in other circumstances. This Court has frequently taken judicial notice of these broader "social facts" to "construct a frame of reference or background context for deciding factual issues crucial to the resolution of a particular case . . . [;] they help to

explain aspects of the evidence" (*R. v. Spence*, 2005 SCC 71, [2005] 3 S.C.R. 458, at para. 57; see also P. W. Hogg and W. K. Wright, *Constitutional Law of Canada* (5th ed. Supp.), at § 60:8). In my view, the ever-increasing intrusion of the Internet into our private lives must be kept in mind in deciding this case. It is widely accepted that the Internet is ubiquitous and that vast numbers of Internet users leave behind them a trail of information that others gather up to different ends, information that may be pieced together to disclose deeply private details. And, as the expert evidence describes, an IP address is attached to all online activity; it is a fundamental building block to all Internet use. This social context of the digital world is necessary to a functional approach in defining the privacy interest afforded under the *Charter* to the information that could be revealed by an IP address.

[59] Similarly, interveners play a critical role in this Court's adjudication — not only by identifying the consequences of particular legal decisions but also by reflecting the diversity of views that inform our normative approach. "The acceptance of intervenors is a reflection of the fact that the decision of the court on a constitutional matter will have broad public ramifications and a recognition of the fact that those who have particular interests that are affected and who can assist the court should be heard" (R. J. Sharpe and K. Roach, *The Charter of Rights and Freedoms* (7th ed. 2021), at p. 128).

[60] The Crown suggests that an IP address is useless without a *Spencer* warrant. Respectfully, I cannot agree. First, as the link that connects specific Internet

activity to a specific location, an IP address may betray deeply personal information, even before police try to link the address to the user's identity. Second, activity associated with the IP address can be correlated with other online activity associated with that address available to the state — with particularly concerning consequences when coupled with access to third-party-held information. Finally, an IP address can set the state on a trail of Internet activity that leads directly to a user's identity, even without a *Spencer* warrant. The instances when an IP address may betray biographical core information are not all captured by *Spencer*. In light of these three points, which I elaborate below, access to IP addresses without judicial pre-authorization poses intense privacy risks, and IP addresses attract a reasonable expectation of privacy.

[61] First, the activity associated with the IP address can itself be deeply revealing, even before any attempt to determine identity. Here, the activity was a series of financial transactions through an online intermediary, Moneris. Linked to financial intermediaries like Moneris or PayPal, an IP address can reveal all of a user's transactions on that intermediary over the period the IP address was assigned to them. For example, Moneris associated five different online transactions with these IP addresses (*voir dire* reasons, at paras. 7-8).

[62] These purchases may "broadcas[t] a wealth of personal information capable of revealing personal and core biographical information about the [purchaser]" (*Marakah*, at para. 33), from the restaurants they frequent, the destinations they visit, the hobbies they enjoy, to the health supplements they use. Internet users may even

have “an acute privacy interest in the *fact* of their electronic [purchases]”, especially as our marketplaces rapidly migrate online (para. 33 (emphasis in original)).

[63] Other online activities can reveal information that goes directly to a user’s biographical core. Websites offering dating services or adult pornography can give the state a depiction of the user’s sexual preferences. An Internet user’s history on medical, political, or other similar online chatrooms can reveal their health concerns or political views. If an IP address is not protected, this information is freely available to the state without the protection of the *Charter* whether or not it relates to the investigation of a particular crime.

[64] Second, the specific activity associated to the IP address by the search can be correlated with other online activity associated to that IP address.

[65] Without the protection of s. 8, nothing prevents the state from pre-emptively collecting IP addresses and comparing that user’s IP address against their database. Further, and significantly, the scope of information that an IP address can reveal is enormous if correlated against information held by a third party. Cases suggest that third parties provide this information without being asked. For example, in *State v. Simmons*, 190 Vt. 141 (2011), the police, after identifying a suspect, contacted MySpace, a social media site, and requested that they share the IP addresses that had accessed his MySpace profile (para. 3). MySpace provided records showing not just the IP addresses themselves, but also *every time* each IP address had logged into

Simmons' MySpace account — including that one IP address had logged into the account "more than 100 times over the course of a week" (para. 3).

[66] As the expert explained, third-party websites can track the external IP address of each user who visits their site. Some websites, like Google, also collect massive amounts of other information such as YouTube history, Google searches, and location history. This information can be of an extremely personal nature.

[67] A great deal of online activity is performed anonymously (*Spencer*, at para. 48; *Ward*, at para. 75). People behave differently online than they do in person (*Ramelson*, at para. 5). "Some online locations, like search engines, allow people to explore notions that they would be loath to air in public; others, like some forms of social media, allow users to dissimulate behind veneers of their choosing" (para. 46). We would not want the social media profiles we linger on to become the knowledge of the state. Nor would we want the intimately private version of ourselves revealed by the collection of key terms we have recently entered into a search engine to spill over into the offline world. Those who use the Internet should be entitled to expect that the state does not access this information without a proper constitutional basis.

[68] Finally, link by link, an IP address can set the state on a trail of anonymous Internet activity that leads directly to a user's identity. The expert uses the example of an IP address that logs onto a particular social media profile or email account containing information from which the user's identity can be inferred, such as their name. From there, the user's identity is but a short inference away. It is not an answer

to say — as Crown counsel does — that a *Spencer* warrant is required if the IP address is sought in relation to information that can unveil the identity of the Internet user. It cannot be left to police or private companies to determine whether the information provided on the website will (perhaps in combination with other information) assist in identifying the source of the activity, the identity of the user or otherwise compromise privacy interests.

[69] Thus, to say that a *Spencer* warrant protects against the privacy concerns raised by IP addresses is simply not supported by modern technological realities. IP addresses play a crucial role in the inherent structure of the Internet. They are the means by which Internet-connected devices both send and receive data. As such, they are the key to unlocking an Internet user's online activity — the first "digital breadcrumbs" on the user's cybernetic trail (*Jones*, at para. 42, citing S. Magotiaux, "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015), 71 *S.C.L.R.* (2d) 501, at p. 502). Those breadcrumbs may establish an Internet user's entire daily, weekly, or even monthly online activity, leading to an electronic roadmap of the user's cybernetic peregrinations (*Morelli*, at para. 3). Like the computer in *Reeves*, an IP address provides the state with the means that can lead them to a trove of personal information.

[70] Consequently, an IP address may betray an intensely private array of information, touching directly on the intimate details of the lifestyle and personal choices of an individual user (*Marakah*, at para. 32; *Spencer*, at para. 27).

(4) Does the Balance Weigh in Favour of a Reasonable Expectation of Privacy?

[71] Defining a reasonable expectation of privacy is an exercise in balance. Individuals are entitled to insist on their right to be left alone by the state. "At the same time, social and economic life creates competing demands. The community wants privacy but it also insists on protection" (*Tessling*, at para. 17).

[72] Here, the intensely private nature of the information an IP address may betray strongly suggests that the public's interest in being left alone should prevail over the government's interest in advancing its law enforcement goals. I will elaborate.

[73] The Internet has exponentially increased both the quality and quantity of information stored about Internet users, spanning the most public and the most private human behaviour (*Ramelson*, at para. 45). It is highly centralized, easily accessible, and "not filtered through human memory and motivation but can be produced as a copy of its original form" (L. M. Austin, "Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints" (2016), 17 *Theoretical Inquiries L.* 451, at p. 457). Information once revealed to the state in pieces can now be "compiled, dissected and analyzed to lend new insights into who we are as individuals or populations" (*Ramelson*, at para. 48). An IP address attaches to each of these pieces. It is the key that links them to one another.

[74] Even "information that may at first blush appear mundane and outside of the biographical core may be profoundly revealing when situated in context with other data points" (N. Hasan et al., *Search and Seizure* (2021), at p. 59). Aggregation "creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected" (O. Tene, "What Google Knows: Privacy and Internet Search Engines", [2008] *Utah L. Rev.* 1433, at p. 1458, quoting Solove, at p. 507). The ubiquity of the Internet means we must increasingly consider "the ways in which different data sets *in combination* with other data sets affect privacy rights" (Hasan, at p. 60 (emphasis in original)).

[75] Not only does the Internet keep an accurate permanent record, it has concentrated this mass of data in the hands of third parties, investing these third parties with immense informational power. It has given large private corporations the ability to collect vast stores of user information and to aggregate that data into sharp images of their users' online activity to determine what their users want and when they want it. In exchange, these corporations are "building possibly the most lasting, ponderous, and significant cultural artifact in the history of humankind" (Tene, at p. 1435, quoting J. Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (2005), at p. 6).

[76] The Internet has not only allowed private corporations to track their users, but also to build profiles of their users filled with information the users never knew

they were revealing. “Browsing logs, for example, may provide detailed information about users’ interests. Search engines may gather records of users’ search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns” (*Spencer*, at para. 46). Commentators have even suggested that companies can use the data they collect to infer “what you are going to purchase, the kind of person you are going to get into a relationship with, whether you will be good at a new job, how long you will stay at that job, and whether you’ll get sick” (H. Matsumi, “Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?” (2017), 48 *Cumb. L. Rev.* 149, at p. 149).

[77] This is far from speculation. Indeed, it is common knowledge that the largest social media companies in the world use IP addresses to, for example, personalize the advertisements their users see, identify their users’ preferences, and infer even more information about their users, such as their age, their gender, and their interests. When it comes to tracking users on the Internet, to paraphrase science fiction novelist William Gibson, “[t]he future is already here” (P. Kennedy, “William Gibson’s Future Is Now”, *The New York Times*, January 13, 2012 (online)).

[78] By concentrating this mass of information with private third parties and granting them the tools to aggregate and dissect that data, the Internet has essentially altered the topography of privacy under the *Charter*. It has added a third party to the constitutional ecosystem, making the horizontal relationship between the individual and the state tripartite. Though third parties are not themselves subject to s. 8, they

"mediat[e] a relationship which is directly governed by the *Charter* — that between the defendant and police" (A. Slane, "Privacy and Civic Duty in *R v Ward*: The Right to Online Anonymity and the *Charter*-Compliant Scope of Voluntary Cooperation with Police Requests" (2013), 39 *Queen's L.J.* 301, at p. 311).

[79] That shift has enhanced, rather than constrained, the state's informational capacity. "[T]echnological developments are permitting government actors to expand their surveillance powers significantly, in part by tapping into detailed information collected by the private sector" (A. J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" (2003), 29 *Queen's L.J.* 364, at p. 406). Professor Austin describes this state of affairs as the "new public/private nexus of surveillance", where intermediaries can "allo[w] the state to access the content of our communications as well as a treasure trove of other associated data" (p. 453). As a result, "in the context of intermediary cooperation state power is augmented" (p. 458).

[80] Even if the IP address does not itself reveal the user's identity, the prospect and ease of a *Spencer* 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. As the appellant argues, comparing the IP address of an identified user with other online activities "shatters [online] anonymity completely" (A.F., at para. 45).

[81] Some foreign jurisdictions have responded by recognizing that IP addresses amount to private information deserving of protection, even if recourse to third-party information is necessary. In *Breyer v. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779, the European Court of Justice concluded that an IP address was personal data relating to an "identifiable person" according to art. 2 of *Directive 95/46/EC of the European Parliament and of the Council*, [1995] O.J. L. 281/31. It did not matter if a third party was needed to make this person "identifiable": a user's IP address is *itself* "personal data" because the IP address can reasonably tend to reveal the user's identity — in that case, through information held by a private intermediary (para. 44).

[82] Likewise, the Court of Appeal for England and Wales concluded that whether "browser-generated information" — such as an IP address — was personal data under the *Data Protection Act 1998* (U.K.), 1998, c. 29, was a serious issue to be tried on the merits (*Vidal-Hall v. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003, at para. 107). The court reasoned that it was clearly arguable that such information is personal data because it "'individuates' the individual, in the sense that they are singled out and distinguished from all others" (para. 115). It was "immaterial" to their finding that the information does not name the user because "in most cases — including cases with dynamic IP address allocation — the necessary data will be available to identify the user(s) of the IP address" (para. 117).

[83] I agree with the intervener the British Columbia Civil Liberties Association that these authorities offer a persuasive account of the interaction between IP addresses and the normative approach our Court has consistently applied to s. 8 of the *Charter*. They recognize IP addresses as private information because IP addresses could reasonably reveal — that is, they tend to reveal — the identity of the user whether or not recourse to a third party is required. These authorities provide "*support* or *confirmation*" for this Court's methodology towards privacy (*Quebec (Attorney General) v. 9147-0732 Québec inc.*, 2020 SCC 32, [2020] 3 S.C.R. 426, at para. 22 (emphasis in original)). Our Court has looked to comparative authorities for their persuasive force throughout its history (see N. Olivetti Rason and S. Pennicino, "Comparative Law in the Jurisprudence of the Supreme Court of Canada", in G. F. Ferrari, ed., *Judicial Cosmopolitanism: The Use of Foreign Law in Contemporary Constitutional Systems* (2019), 140, at p. 146).

[84] Weighed against these substantial privacy concerns is society's sometimes conflicting but legitimate interest in the need for safety and security. As technology evolves, how crime is committed and investigated also evolves (*R. v. Mills*, 2019 SCC 22, [2019] 2 S.C.R. 320, at paras. 38-39). Easy access to the Internet and user anonymity combine to allow for the commission of a wide range of crime, including sexual offences and crimes against children. The amplified impact and permanence of harm done to victims of online crime, especially children, must be considered in defining and calibrating the law enforcement interest implicated by this appeal (see *R. v. Friesen*, 2020 SCC 9, [2020] 1 S.C.R. 424, at paras. 1, 5 and 50-73; Magotiaux, at

p. 502). Police should have the investigative tools to deal with crime that is committed and facilitated online.

[85] In my view, however, requiring that police obtain prior judicial authorization before obtaining an IP address is not an onerous investigative step, and it would not unduly interfere with law enforcement's ability to deal with this crime. Where the IP address, or the subscriber information, is sufficiently linked to the commission of a crime, judicial authorization is readily available and adds little to the information police must already provide for a *Spencer* production order. For example, under s. 487.015(1) of the *Criminal Code*, R.S.C. 1985, c. C-46, a production order for information relating to a specified transmission of a communication is available if there are reasonable grounds to *suspect* that an offence has been or will be committed. Police often apply for and obtain multiple authorizations to protect different territorial privacy interests. The same is true to protect informational privacy.

[86] On balance, the burden imposed on the state by recognizing a reasonable expectation of privacy in IP addresses pales compared to the substantial privacy concerns implicated in this case. Law enforcement will need to demonstrate enough grounds to intrude on an individual's privacy but, in the age of telewarrants and around-the-clock access to justices of the peace, this burden is not onerous. Police engaging in legitimate investigatory activities can readily establish the requisite constitutional grounds. Recognizing that an IP address attracts s. 8 protection will not thwart police investigations involving IP addresses; rather, it aims to make sure police investigations

better reflect what each reasonable Canadian expects from a privacy perspective *and* from a crime control perspective.

[87] A reasonable expectation of privacy limits the state to searches motivated by legitimate law enforcement concerns. The benefits to privacy are significant. Judicial pre-authorization considerably narrows the state's online reach and prevents it from acquiring the details of a user's online life revealed by their IP address that are not relevant to the investigation. This significantly reduces the potential of any "arbitrary and even discriminatory" exercises of discretion that would empower the state to identify information about any Internet user it pleases for any reason it sees fit (L. M. Austin, "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law" (2012), 27 *C.J.L.S.* 381, at p. 392). In a democratic society, it is "inconceivable that the state should have unrestricted discretion to target whomever it wishes for surreptitious [digital] surveillance" (*R. v. Wong*, [1990] 3 S.C.R. 36, at p. 47).

[88] Judicial oversight in respect of an IP address is the way to accomplish s. 8's goal of preventing infringements on privacy. Since *Hunter*, we have held that s. 8 seeks to prevent breaches of privacy, not to condemn or condone breaches after the fact based on the state's use of that information. Privacy, once breached, cannot be restored.

[89] Finally, judicial oversight removes the decision to disclose information — and how much to disclose — from private corporations and returns it to the purview of the *Charter*. The increase in state power occasioned by the Internet is thus offset by a broad, purposive approach to s. 8 that meets our "new social, political and historical

realities" (*Hunter*, at p. 155). To leave it to the private sector to decide whether to provide police with information that may betray our most intimate selves strikes an unacceptable blow to s. 8. To leave the protection of the *Charter* to the next intended step in the investigation is insufficient. As I have explained, the next step might be too late.

[90] Thus, viewed normatively, s. 8 of the *Charter* ought to extend a reasonable expectation of privacy to IP addresses. They provide the state with the means through which to obtain information of a deeply personal nature about a specific Internet user and, ultimately, their identity whether or not another warrant is required. An IP address plays an integral role in maintaining privacy on the Internet. It is the key to unlocking an Internet user's online activity and the key to identifying the user behind online activity. Given these serious privacy concerns, the public's interest in being left alone should prevail over the relatively straightforward burden imposed on law enforcement. Recognizing a reasonable expectation of privacy in IP addresses would ensure that the veil of privacy all Canadians expect when they access the Internet is only lifted when an independent judicial officer is satisfied that providing this information to the state will serve a legitimate law enforcement purpose.

[91] In my view, the reasonable and informed person concerned about the long-term consequences of government action for the protection of privacy would conclude that IP addresses should attract a reasonable expectation of privacy.

Extending s. 8's reach to IP addresses protects the first "digital breadcrumb" and therefore obscures the trail of an Internet user's journey through the cyberspace.

V. Disposition

[92] I would find the request by the state for an IP address is a search under s. 8 of the *Charter*. I would allow the appeal, set aside the conviction, and order a new trial.

The reasons of Wagner C.J. and Côté, Rowe and O'Bonsawin JJ. were delivered by

CÔTÉ J. —

I. Introduction

[93] In this digital age, concerns about online privacy are prevalent. So are concerns about online crime.

[94] In this case, the Calgary police investigated a series of fraudulent purchases made online. As a result of that investigation, the appellant, Andrei Bykovets, was arrested, tried, and convicted of a number of offences relating to fraud through the use of the Internet. The police were able to identify him by taking several steps, including obtaining a production order as required by *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212. The first step in the investigation was retrieving the appellant's Internet

Protocol ("IP") addresses from an intermediary, which the police did without a warrant. The appellant alleges that he had a reasonable expectation of privacy in his IP addresses, such that his rights under s. 8 of the *Canadian Charter of Rights and Freedoms* were violated when the police obtained the IP addresses from the intermediary. According to the appellant, the police needed prior judicial authorization to obtain the addresses.

[95] Our Court is called upon to determine whether the appellant had a reasonable expectation of privacy in the IP addresses alone — without any other information linking those addresses to him as an Internet user — in the circumstances of this case. I conclude that the appellant did not have a reasonable expectation of privacy. Accordingly, I would dismiss the appeal.

II. Facts

[96] The facts are not disputed by the parties.

[97] In September 2017, the Calgary police commenced an investigation related to the purchase of virtual gift cards using fraudulent credit card information. The purchases were made online through businesses, including a liquor store called Co-op Wine Spirits Beer. The payments were processed by a subsidiary of the credit card processor, Moneris.

[98] In the course of their investigation into the fraud, the police contacted Moneris and asked for the IP addresses associated with the purchases. Moneris provided the IP addresses shown in its logs for the transactions. The police then used a publicly-accessible lookup website and learned that the IP addresses had been issued by TELUS. They obtained a production order requiring TELUS to provide the subscriber information associated with the IP addresses. One address was registered to the appellant and one was registered to his father. I note that there is no distinction between those two addresses for the purposes of this appeal.

[99] The police then applied for and obtained warrants to search the two residences associated with the IP addresses. During the search, the police found a magnetic stripe card reader and writer, government identification bearing the names of third-party individuals, computers, USB sticks, fake immigration documents, and firearms. The appellant was arrested and charged with 33 offences related to the possession and use of third parties' credit cards and personal identification documents as well as the possession and storage of firearms.

[100] Prior to trial, the appellant applied to exclude the evidence discovered as a result of the police's use of his IP addresses, alleging that the police had infringed his rights under s. 8 of the *Charter*. He tendered the report of Matthew Musters, whom the trial judge qualified as an expert in electronic forensic analysis and in the nature and operation of IP addresses. The Crown consented to the admission of Mr. Musters'

expert report and did not seek to cross-examine him. The Crown also expressed agreement with the contents of the report.

[101] The relevant parts of the report may be briefly summarized.

[102] First, the report explains that there are two types of IP addresses: external and internal. This appeal concerns external IP addresses only. An external IP address is assigned to a subscriber by an Internet service provider ("ISP") and is used in the transfer of information across the Internet from one source to another. Without an external IP address, a user cannot send or receive data. Each external IP address is distinctly associated with one subscriber during its lease period. Most commonly, residential subscribers are assigned dynamic external IP addresses which an ISP can change at will and without notice. Each ISP keeps a record of which subscriber each external IP address was assigned to and for what period of time.

[103] Next, the report explains that in a typical Internet browsing session, a user's external IP address is known only by the destination server (excluding any hops it went through on its way). The report describes two methods by which a user's identity can be discovered from his or her external IP address. The first involves entering the IP address into an ISP lookup website to determine which ISP owns the IP address, and then obtaining the subscriber information from the ISP. The other is based on the assumption that one is able to access the information logged by third-party companies' websites. Websites are able to track the IP address of each user who visits the site. Based on that information, one could attempt to determine the identity of an individual

using a company's online service by examining the user's activity on the website in question.

III. Judicial History

A. *Court of Queen's Bench of Alberta, 2020 ABQB 70, 10 Alta. L.R. (7th) 103 (Ho J.)*

[104] In her *voir dire* ruling, the trial judge stated that the primary issue to be determined in respect of s. 8 of the *Charter* was whether an individual has a reasonable expectation of privacy in an IP address. The Crown conceded that if the appellant had a reasonable expectation of privacy in the IP addresses, then his s. 8 rights were violated. To determine whether a reasonable expectation of privacy exists, the trial judge applied the "totality of the circumstances test" as set out by this Court in *Spencer*.

[105] The trial judge found that the subject matter of the alleged search was the IP addresses. Both on their face and in light of what could be inferred from them, the IP addresses could only provide limited information about an Internet user. Only with other information could an IP address lead to the identification of a particular individual. In this case, the police were "really after" the IP addresses themselves to discover the suspected fraudster's ISP and then obtain a production order to identify him or her.

[106] The trial judge accepted that the appellant had a direct interest and a subjective expectation of privacy in the IP addresses. However, she found that this subjective expectation of privacy was not objectively reasonable. Contrary to the appellant's submission, the search took place not in his home but in the credit card processor's database. As collections of numbers, the IP addresses did not disclose personal information or reveal intimate details of the appellant's lifestyle. The ISP was able to control the subject matter of the search through its ability to change the appellant's IP addresses, though this factor was not determinative.

[107] Considering all the factors, the trial judge held that the appellant did not have a reasonable expectation of privacy in the IP addresses. Therefore, his s. 8 rights were not engaged by the search. The appellant was ultimately convicted of 14 of the 33 offences with which he had been charged.

B. *Court of Appeal of Alberta, 2022 ABCA 208, [2023] 5 W.W.R. 51*

(1) Majority (Schutz and Crighton JJ.A.)

[108] The appellant appealed and challenged the trial judge's finding that there was no breach of his s. 8 rights. The majority of the Court of Appeal dismissed the appeal and held that the trial judge had correctly interpreted the scope of s. 8 and applied the correct principles, and that her factual findings revealed no palpable and overriding error. The trial judge interpreted the subject matter of the search functionally, as she was required to do. She understood what the police were "really

after": IP addresses to further the investigation, in the hope that the authorized further investigation would uncover names and addresses associated with the IP addresses. The trial judge found that the IP addresses revealed no private information; the appellant therefore had no reasonable expectation of privacy in them. The majority thus agreed with the trial judge's analysis and conclusions.

[109] The majority also agreed with the trial judge that *Spencer* was distinguishable because the police in this case did not obtain *subscriber data* in addition to the IP addresses themselves. Without that data, the police simply believed that "an unknown person using a known IP address was committing fraud from an unknown address", which was not enough to give rise to a reasonable expectation of privacy (para. 17). In the majority's view, an "IP address is an abstract number that reveals none of the core biographical information the issuer of that IP address attaches to it. Standing alone, it reveals nothing" (para. 21). Only with subscriber information could an IP address reveal personal information, and the police could only obtain that subscriber information by complying with *Spencer*.

(2) Dissent (Veldhuis J.A.)

[110] Veldhuis J.A., in dissent, would have found that the appellant had a reasonable expectation of privacy in the IP addresses because they were linked to a particular, monitored Internet activity that could disclose biographical core information. Accordingly, she would have found a breach of the appellant's s. 8 rights and ordered a new trial.

[111] Veldhuis J.A. was of the opinion that the trial judge had failed to apply the normative approach to reasonable expectations of privacy. In her view, the case was indistinguishable from *Spencer*. Both *Spencer* and this case involved an attempt by the police to identify a particular user of the Internet so that they could "gather further information to draw inferences about the intimate details of the lifestyle and personal choices of the internet user" (para. 62).

[112] In Veldhuis J.A.'s view, this failure to apply the normative approach led the trial judge to characterize the subject matter of the search too narrowly. She noted that the expert evidence showed how an IP address could be used to identify an Internet user from third-party websites, and if there were no reasonable expectation of privacy, then there would be nothing requiring the police to obtain a warrant before doing so. For Veldhuis J.A., the true subject matter of the search, and what the police were really after, was "the identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity" (para. 77). This subject matter engaged the idea of privacy as anonymity, which is very important in the context of the Internet.

[113] According to Veldhuis J.A., the trial judge's error in characterizing the subject matter of the search led to a further error in her finding that the appellant's subjective expectation of privacy was not objectively reasonable. With respect to the place of the search as a factor in assessing such reasonableness, Veldhuis J.A. noted that s. 8 "protects people, not places", and held that a person would expect credit card

information and the IP address from which it is sent to remain private. With respect to the private nature of the subject matter, Veldhuis J.A. reiterated her earlier comments about the possibility of identifying an Internet user by using an IP address, which raises privacy interests going beyond the user's name and address. With respect to control over the subject matter, Veldhuis J.A. found that control is not lost simply because an IP address can be accessed by others. She held that there is no meaningful choice between not using the Internet at all and giving up control of one's IP address.

[114] Veldhuis J.A. concluded that the appellant had a reasonable expectation of privacy in the IP addresses "because they were linked to a particular, monitored internet activity that could disclose biographical core information" (para. 94).

[115] The appellant now appeals to this Court on the strength of Veldhuis J.A.'s dissent.

IV. Issue

[116] The single issue in this case is whether a reasonable expectation of privacy attached to the IP addresses. If it did, then the Crown concedes that the appellant's s. 8 *Charter* rights were violated.

V. Analysis

[117] The law with respect to reasonable expectations of privacy is well-established. This case calls for a straightforward application of the law to a situation where an IP address is given to the police by an online credit card processor.

[118] Section 8 of the *Charter*, which provides that "[e]veryone has the right to be secure against unreasonable search or seizure", is meant to protect against state intrusion on an individual's privacy. But as this Court has observed, "not every form of examination conducted by the government will constitute a 'search' for constitutional purposes" (*R. v. Evans*, [1996] 1 S.C.R. 8, at para. 11). Section 8 comes into play only "where a person's reasonable expectations of privacy are somehow diminished by an investigatory technique" (*ibid.*).

[119] The reasonable expectation of privacy test is fact-specific and contextual. Whether someone has a reasonable expectation of privacy depends on "the totality of the circumstances of a particular case" (*R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 31). This Court has identified a non-exhaustive list of factors to be considered in this regard. The relevant factors are often conveniently grouped under four main headings:

(1) What was the subject matter of the alleged search?

(2) Did the claimant have a direct interest in the subject matter?

(3) Did the claimant have a subjective expectation of privacy in the subject matter?

(4) If so, was the claimant's subjective expectation objectively reasonable?

[120] As has often been noted, the inquiry is normative, not descriptive (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 42; *R. v. Reeves*, 2018 SCC 56, [2018] 3 S.C.R. 531, at para. 28). The objective is to determine what degree of privacy one *ought* to have, not what degree of privacy one *actually* has. As Binnie J. put it in *Tessling*:

> In an age of expanding means for snooping readily available on the retail market, ordinary people may come to fear (with or without justification) that their telephones are wiretapped or their private correspondence is being read. . . . Suggestions that a diminished *subjective* expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed. It is one thing to say that a person who puts out the garbage has no reasonable expectation of privacy in it. It is quite another to say that someone who fears their telephone is bugged no longer has a *subjective* expectation of privacy and thereby forfeits the protection of s. 8. [Emphasis in original; para. 42.]

[121] Bearing this normative approach in mind, I now turn to its application to the facts of this case. Like the trial judge, I accept that the appellant had a direct interest in the IP addresses and a subjective expectation of privacy in their informational content. The principal points of disagreement before this Court are in connection with the first and fourth parts of the analysis: the subject matter of the search, and the

objective reasonableness of the expectation of privacy, specifically in relation to the private nature of the subject matter. I will address them in turn.

A. *Subject Matter of the Search*

[122] Identifying the subject matter of the search is a key question in the "totality of the circumstances" analysis. Our Court has taken a "broad and functional approach" to this inquiry. The subject matter of the search must not be defined "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action" (*R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 15, quoting *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 65). Accordingly, to identify the subject matter of the search, the court must examine the connection between the police investigative technique and the privacy interest at stake (*Marakah*, at para. 15). It must consider "not only the nature of the precise information sought, but also . . . the nature of the information that it reveals" (*Spencer*, at para. 26).

[123] When assessing the subject matter of an alleged search, the court's task is to determine "what the police were really after" (*Marakah*, at para. 15, quoting *Ward*, at para. 67). This guiding question highlights the fact that the subject matter of the search may go beyond the precise object or information obtained by the police. When the court inquires into "what the police were really after", it is not concerned with the police's objective in the criminal investigation (i.e., *why* the police sought the information). Nor is it concerned with their subjective intentions. Rather, the court is

concerned with the capacity of the precise information sought to give rise to inferences or to reveal *further* information. These inferences and this further information form part of the true subject matter of the search.

[124] *Spencer* illustrates these principles. In that case, in the course of an investigation into child pornography, the police had requested subscriber information (a name and a physical address) from the ISP that owned a particular IP address. The Court disagreed with the contention that such subscriber information by itself was the true subject matter of the search. That "characterizatio[n] gloss[es] over the significance of an IP address and what such an address, once identified with a particular individual, is capable of revealing about that individual, including the individual's online activity in the home" (para. 32 (emphasis added), quoting *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, at para. 35). Instead, this Court concluded that the subject matter of the search was "the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity" (para. 33). The precise information sought — subscriber information — provided a link between a specific individual and the particular online activity associated with an anonymous IP address. All of this constituted the subject matter of the search.

[125] Similarly, in *Marakah*, McLachlin C.J. held that the subject matter of the search was not merely the cell phone that had been seized by the police. Rather, it included text message conversations contained in the cell phone as well as any

inferences about associations and activities "that can be drawn from th[e] information" shared in those conversations (para. 20 (emphasis added)).

[126] Finally, and importantly, while the subject matter of the search cannot be defined too narrowly, it must still be anchored to what can be drawn from the evidence itself. Specifically, the capacity of the precise information sought to give rise to inferences or to reveal further information must be supported by the evidence; it cannot be based on mere conjectures or hypotheses. This principle can be traced back through this Court's jurisprudence. In *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456, for example, Deschamps J., dissenting, but not on this point, explained that what was significant about the dog sniff of the accused's bag was that sniffer dogs are relied on by the police with a success rate of over 92 percent and that the dogs do not simply identify the odours emanating from a bag but, by doing so, actually identify the contents of the bag (i.e., a controlled substance) (para. 174). In that case, the dog sniff therefore allowed a "strong, immediate and direct inference" to be drawn about the contents of the accused's bag, which was what the police were really interested in searching (para. 175). The capacity of the precise information sought — the odours detected by the dog — to reveal other information was supported by the evidence on the record in that case.

[127] By contrast, in *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, the police suspected that the accused was involved in producing marijuana. They asked a utility company to install a device to measure electrical power flowing into the accused's

residence. This Court relied on the evidentiary record to assess what the precise information sought (from the device) discloses and what inferences it supports. The Court of Appeal had concluded that some information about what is taking place in a house may be inferred from the device. Several members of this Court disagreed, as this finding was not supported by the evidence on the record. Instead, the record showed that the device reveals only the consumption of electricity; it reveals nothing about the intimate or core personal activities taking place inside a home (para. 14). The evidentiary record thus constrained the subject matter of the search.

[128] In the circumstances of this case, the subject matter of the search comprises the IP addresses and the identity of their associated ISP. While the police had the ultimate goal of identifying the person alleged to have committed fraud, their investigative objective is not the focus of the "broad and functional approach" for ascertaining the subject matter of the search (*Spencer*, at para. 26). Rather, the subject matter must reflect the information revealed by the precise information sought (*Spencer*, at para. 26). I disagree with Veldhuis J.A.'s assertion that the subject matter was "the identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity" (para. 77). While that may have been the ultimate goal of the investigation, it was not information revealed by the raw IP addresses alone, and it is therefore not the subject matter of the search.

[129] I fully appreciate that the numbers constituting an IP address are not sought for their own sake. They are sought for the information they reveal. However, the

evidentiary record in this case establishes that an IP address, on its own, reveals only limited information. It does not reveal a "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" (*R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293). On its own, an IP address does not even reveal browsing habits. What it reveals is a user's ISP — hardly a more private piece of information than electricity usage (*Plant*) or heat emissions (*Tessling*).

[130] Only when an IP address is combined with other information can it give rise to inferences about a user's identity, which fundamentally distinguishes this case from *Spencer*. In *Spencer*, subscriber information was the key that unlocked the identity of the person behind an IP address and revealed his activities online. A reasonable expectation of privacy attached to the subscriber information because it provided the link between anonymous Internet activity and a specific person. But in the present case, there was no such link. The question, then, is this: What information do IP addresses, on their own, disclose, and what inferences do they support?

[131] As discussed, the uncontested expert evidence in this case established that there are two methods by which a user's identity can be discovered from his or her external IP address. The first method is to identify the ISP that owns an IP address using an "IP lookup website" (A.R., at p. 311). The expert explained that "[o]nce the ISP of a particular IP address has been identified, it is possible to determine the subscriber of the account by requesting that information from the ISP in control of that

IP address" (A.R., at p. 311). This is what happened in *Spencer*. In response, our Court held that individuals have a reasonable expectation of privacy in such subscriber information. Following *Spencer*, the police must now obtain a production order to acquire that information. It is noteworthy that obtaining such an order is exactly what the police did in this case.

[132] According to the expert report, the second method by which an IP address may be used to determine the identity of an individual using the Internet is to access "the information logged by the third-party company's website", which is "able to track the external IP address of each user who visits" (A.R., at p. 311). According to the expert, an IP address could be provided to a company like Google, and Google could use that IP address to identify a user's activity which the company tracks. This seems to have been Veldhuis J.A.'s main concern, and it seems that my colleague Karakatsanis J. has the same concern.

[133] There are two answers to this concern about third-party websites.

[134] First, on the facts of this case, the police simply did not use a third-party website's tracking of the appellant in order to identify him. As the trial judge found, the police sought the IP addresses in order to investigate further, specifically to discover their associated ISP. The primary investigator's testimony was to this effect. The investigation that followed was carried out with a production order, which is consistent with this Court's judgment in *Spencer*. Thus, the concern does not arise here.

[135] Second, as conceded by the Crown, such a scenario (using a third-party website) seems indistinguishable from *Spencer*. *Spencer* established that a reasonable expectation of privacy may exist in the link between a user's identity and specific Internet activity. Whether the identity of an anonymous Internet user is revealed by combining his or her IP address with subscriber information held by an ISP or by combining his or her IP address with other information held by third-party websites, the result is the same. The user's privacy interest in anonymity is undermined. Accordingly, as the Crown accepts, *Spencer* requires the police to obtain judicial authorization before requesting data of this nature — in other words, data that unveils the identity of an individual whose Internet connection is linked to particular, monitored online activity. I mention in passing that if a third-party website were to spontaneously provide information without being asked, the reasonable expectation of privacy analysis — which is always guided by "the totality of the circumstances" — could well be different (cf. *Reeves*, at para. 46). That, however, is an issue for another day in a case where the situation actually arises on the facts.

[136] Finally, the appellant relies upon *Reeves* to argue that the mere fact that the police had to take further steps to identify him and link him to particular Internet activity does not mean that he lacked a reasonable expectation of privacy in the IP addresses. In my respectful view, this reliance is misplaced. In *Reeves*, the police had *seized* a computer shared by the accused and his spouse, with the latter's permission. The seizure of the computer necessarily entailed a seizure of its data. This Court held that the accused had a reasonable expectation of privacy in the computer and its data.

While a warrant was indeed necessary to search the computer notwithstanding the seizure (see *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at para. 49), the seizure itself deprived the accused of control over the private data in the computer (*Reeves*, at para. 34). Moreover, it provided the police with possession of the data in which the accused had an interest. In this case, however, the IP addresses alone did not give the police possession of any private information about the appellant, whether immediately accessible or not. Only by obtaining a production order to require the ISP to provide the subscriber information did the police uncover constitutionally-protected information, namely the link between the appellant's identity and his Internet activity.

[137] Thus, the correct way to characterize the subject matter of the search is to describe it as the IP addresses and the ISP revealed by them. A characterization of the subject matter that goes far beyond the scope of the information actually revealed by the precise information sought by the police effectively treats an important goal of *many* police investigations, i.e., ultimately leading to the identification of the suspect, as conclusive of the subject matter of the search. Of course, the police were seeking to identify the person who used the IP addresses in the commission of the offences, but they were doing so through a series of steps, and the step in question here revealed only the user's ISP.

[138] My colleague correctly recognizes that the information revealed by the IP addresses is part of the subject matter of the supposed search. However, she includes in the subject matter 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, according to the evidence in the record. With respect, I believe this to be the most significant difference between her position and mine.

[139] I add in passing that it would be inconsistent with a functional approach to defining the subject matter of the search to effectively hold that *any* step taken in an investigation engages a reasonable expectation of privacy. Such a holding would upset the careful balance that this Court has struck between the interest of Canadians in actual privacy and the interest of Canadians in not hindering law enforcement (see, e.g., *Tessling*, at para. 17; *Kang-Brown*, at para. 10; *Vu*, at para. 21; *R. v. Stairs*, 2022 SCC 11). In rejecting a claim that there was a reasonable expectation of privacy in an online conversation with a police officer posing as a child, my colleague put the point well in her concurring reasons in *R. v. Mills*, 2019 SCC 22, [2019] 2 S.C.R. 320: "The alternative conclusion would significantly and negatively impact police undercover operations, including those conducted electronically, [and it] simply does not strike an appropriate balance between individual privacy and the safety and security of our children" (para. 52). I view the consequences of my colleague's broad holding in this case similarly.

[140] Thus, I conclude that the subject matter of this search was the IP addresses, i.e., the collections of numbers, and the identity of the ISP that is revealed by them. The trial judge and the majority of the Court of Appeal were correct in their determinations on this issue.

B. *Objective Reasonableness of the Expectation of Privacy*

[141] The question then becomes whether the appellant's subjective expectation of privacy in the subject matter of the search was objectively reasonable. I conclude that it was not.

[142] Whether an expectation of privacy is reasonable depends on several factors. These may include the place of the search, control over the subject matter of the search, the private nature of the subject matter, whether the subject matter was in public view, whether the subject matter was abandoned, whether the subject matter was already in the hands of third parties, whether the search method was intrusive in relation to the privacy interest at stake, whether the search method was itself unreasonable, and whether the search exposed core biographical information (see, e.g., *Tessling*, at para. 32). This list is not exhaustive. No single factor is determinative.

[143] Not all factors will be relevant to the analysis in a particular case. Considering the type of privacy interest at stake can sometimes be helpful in determining which factors are relevant.

[144] The three types of privacy interests that emerge from the jurisprudence are personal, territorial, and informational. The last of these is what is clearly at stake in this case. Informational privacy may be defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information

about them is communicated to others" (*Tessling*, at para. 23, quoting A. F. Westin, *Privacy and Freedom* (1970), at p. 7).

[145] On the facts of this case and particularly in light of the informational privacy interest involved, the factors relevant to the reasonableness inquiry are the private nature of the subject matter, control over the subject matter, and the place of the search (see *Marakah*, at para. 24). These are the factors focused on by the parties and the courts below, and I will consider them in turn.

[146] But before doing so, I want to address my colleague's reliance on foreign authorities as offering a "persuasive account of the interaction between IP addresses and the normative approach our Court has consistently applied to s. 8" (para. 83). With respect, I am of the view that these authorities are irrelevant. To begin with, they dealt with different statutory frameworks in different countries. *Breyer v. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779, considered whether a person was identifiable through an IP address *by the website accessed*, not by the state *per se*. *Vidal-Hall v. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003, simply answered the question of whether service *ex juris* should have been allowed in that case, and the Court of Appeal's affirmative answer was akin to refusing to strike out a pleading as disclosing no reasonable cause of action (*Altimo Holdings v. Kyrgyz Mobil Tel Ltd*, [2011] UKPC 7, [2012] 1 W.L.R. 1804, at paras. 84-86). Most fundamentally, however, these authorities dealt with different facts and different records.

(1) Private Nature of the Subject Matter

[147] The private nature of the subject matter of a purported search can support a finding that an expectation of privacy is reasonable. This follows from the purpose of s. 8, namely protecting people "from unjustified state intrusions upon their privacy" (*Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 160). As with the identification of the subject matter, the issue is not simply whether the subject matter itself is private, but also whether it can reveal other essential private information, such as core biographical information (*Gomboc*, at para. 14). This factor is of particular importance with respect to informational privacy interests, like the one at issue in this case. Where informational privacy alone is at stake, it may be all but essential that the information itself be private in order for a reasonable expectation of privacy to exist.

[148] In this case, the IP addresses were not private and did not, *on these facts*, reveal private information of any sort, let alone core biographical information. According to the expert evidence, it is only when an IP address is combined with other information that an IP address may tend to reveal intimate information about an individual. As I have shown above, nothing in the evidence suggests that the police can obtain any private information about an individual with an IP address alone. Without more, all an IP address reveals to the police is a user's ISP — hardly a particularly private matter, let alone "core biographical information".

[149] My colleague concludes that IP addresses, without more, reveal highly sensitive and personal information, including the identity of their user. While I appreciate that the normative approach to s. 8 analyses requires some degree of

flexibility, I am of the view that this case must be decided based on the actual evidentiary record and nothing else. The evidence available on the record must not be ignored; that evidence was before the trial judge and was tested by the rigorous adversarial process.

[150] Additionally, nobody in this case contended that a mere purchase is private information, whether made online or otherwise (paras. 61-62). Nobody made such a submission, probably because without identifying the purchaser, the fact of the purchase is meaningless.

[151] All of this strongly points away from a finding that any expectation of privacy was reasonable.

(2) Control Over the Subject Matter

[152] Control over the subject matter of the search generally supports a finding that there was a reasonable expectation of privacy, while lack of control may weigh against such a finding (*Marakah*, at para. 38). The idea is simple: when we control something, we can expect — and to some degree require — others to respect our interest in it. This reasoning does not make control necessary to establish a reasonable expectation of privacy, but the existence of control is a factor which may support a finding of one.

[153] In light of the expert evidence, the appellant seemed to have little control over the IP addresses. An ISP can change a user's IP address at will and without notice. This significantly distinguishes IP addresses from text messages, as in *Marakah*, where the majority of this Court held that people "exercise meaningful control over the information they send by text message by making choices about how, when, and to whom they disclose the information" (para. 39).

[154] On the evidence, it seems that the IP addresses would have been visible only to websites that the appellant chose to visit, which is a limited measure of control. That said, a useful comparison may be drawn between leaving fingerprints at the scene of a crime and leaving an IP address visible to a website. An Internet user who leaves behind IP address data completely loses control over what happens to those numbers, just as someone loses control over what happens to his or her fingerprints after touching something. It cannot be seriously suggested that a police investigation that involves dusting for fingerprints and keeping them — without more — could engage a reasonable expectation of privacy. The same — again, without more — is true of obtaining an IP address.

[155] The factor of control therefore tends to point away from a finding that the appellant's expectation of privacy was reasonable.

(3) Place of the Search

[156] The place of the search informs the reasonableness of any expectation of privacy in it. The idea of place essentially relates to the concept of territorial privacy (*Tessling*, at para. 22). It is therefore somewhat remote from the facts of this case, which, as noted, engage informational privacy, and it necessarily assumes less significance. In the courts below, as here, the issue was whether the place of the search could be characterized as the appellant's home, as he contends. It has long been recognized that one has an increased expectation of privacy in one's home (see, e.g., *R. v. Feeney*, [1997] 2 S.C.R. 13, at para. 78). Thus, characterizing the place of the search as the appellant's home would in some sense support his assertion of a reasonable expectation of privacy.

[157] In my view, however, the correct characterization of the place is the credit card processor's database. That is where the IP addresses were stored and where the processor retrieved them from in order to respond to the police inquiry. As the trial judge rightly recognized, the alleged search was not carried out at the appellant's home, and its location does not enhance the objective reasonableness of his subjective expectation of privacy.

(4) Conclusion on Reasonable Expectation of Privacy

[158] Considering the factors together, I find that the appellant did not have a reasonable expectation of privacy in the IP addresses on the credit card processor's servers and the ISP they revealed. The police did not need judicial authorization before

asking the processor for the IP addresses in order to determine the ISP associated with them. The police followed the teachings of *Spencer* to the letter.

[159] To be clear, in holding that the appellant did not have a reasonable expectation of privacy in the IP addresses in the circumstances of this case, I am not at all foreclosing the possibility that someone may have such an expectation on different facts. This is because, as noted, "[t]he existence of a reasonable expectation of privacy . . . is always a contextual, fact-based inquiry" (*R. v. McNeil*, 2009 SCC 3, [2009] 1 S.C.R. 66, at para. 12). Indeed, the analysis must be conducted in light of "the totality of the circumstances of a particular case" (*Edwards*, at para. 31 (emphasis added)). Nevertheless, while the instant case deals with the offence of fraud, it is noteworthy that police investigations involving IP addresses also take place in the context of other criminal offences. Indeed, the case law is replete with examples of police investigating offences against children, including child pornography and child luring, using IP addresses (see, e.g., *R. v. O'Brien*, 2023 ONCA 197, 166 O.R. (3d) 114; *R. v. Ilia*, 2023 ONCA 75, 523 C.R.R. (2d) 128; *R. v. Allen*, 2020 ONCA 664, 396 C.C.C. (3d) 1; *R. v. West*, 2020 ONCA 473, 392 C.C.C. (3d) 271; *R. v. Caza*, 2015 BCCA 374, 376 B.C.A.C. 258; *Ward*; *Trapp*; *R. v. Smith*, 2005 BCCA 334, 199 C.C.C. (3d) 404).

[160] The result reached by my colleague that not only some, but all, IP addresses attract a reasonable expectation of privacy (see paras. 12 and 87-88) would seriously thwart the police's ability to investigate such serious offences against children. As

"some of the most vulnerable members of our society" (*R. v. Friesen*, 2020 SCC 9, [2020] 1 S.C.R. 424, at para. 1), children must receive "enhance[ed] protection . . . from becoming victims of sexual offences" (*Mills*, at para. 23, per Brown J.). As my colleague wrote in her concurring reasons in *Mills*, a child luring case, "as technology evolves, the ways in which crimes are committed — and investigated — also evolve" (para. 39). Given this evolution of online crime, requiring that police seek authorization to obtain an IP address in every case would also exacerbate the existing challenges faced by the criminal justice system. In this regard, I would highlight the words of Moldaver J. (dissenting, albeit on a different s. 8 issue) in *Marakah*, at para. 185, in reference to the functioning of the justice system:

> The increased need for these judicial authorizations could strain police and judicial resources in an already overburdened criminal justice system. Investigations would be slowed, more judicial officers would be required, and the administration of criminal justice as a whole will suffer.

[161] I stress that to reach the same result as my colleague in this case, I would need to consider different factual scenarios in order to draw new conclusions about what information an IP address may reveal and to discuss what third parties might voluntarily do with data that they collect. I cannot, because doing so would mean ignoring the limits on our Court's jurisdiction, the standard of review for factual findings, the specific evidence in the record, and also procedural fairness. A court must consider the facts as they are, not as they might be, whether because of technological change (*Tessling*, at paras. 28-29 and 55) or a different evidentiary record. If the facts

are changed, then, in the ancient words of Plowden, "the case is altered". But that would not be this case.

[162] Stated summarily, our Court's jurisdiction in criminal appeals is limited to questions of law (*Criminal Code*, R.S.C. 1985, c. C-46, ss. 691 to 693; *Supreme Court Act*, R.S.C. 1985, c. S-26, s. 40(3)), which means that setting aside the factual findings of the courts below is not an available option. Even if it were, nobody suggested that the standard of review for setting aside factual findings is met in this case. Nobody made that suggestion because at first instance the parties agreed with the defence's expert evidence upon which the factual findings underlying the s. 8 analysis were based.

[163] Setting aside the factual findings of the courts below would also essentially amount to taking judicial notice of various contestable facts involving IP addresses and the information that may be gleaned from them, which in my view would be incompatible with this Court's jurisprudence on judicial notice (*R. v. Find*, 2001 SCC 32, [2001] 1 S.C.R. 863, at para. 48). On this note, I would also like to address the reliance by one of the interveners on governmental and other documents in its factum (e.g., Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You: A report prepared by the Technology Analysis Branch of the Office Privacy Commissioner of Canada* (2013)). While I agree with my colleague that interveners play an important role, that role is circumscribed. Recent judgments of this Court have made it clear that interveners may not supplement the evidentiary record on appeal and

have explained why this rule exists (*R. v. McGregor*, 2023 SCC 4, at para. 24, citing *R. v. Sharma*, 2022 SCC 39, at para. 75). The general point that evidence tested by the adversarial process, rather than judicial notice, should be used to establish facts in the constitutional context is also well-established (*R. v. Spence*, 2005 SCC 71, [2005] 3 S.C.R. 458, at para. 68; *In re The Board of Commerce Act, 1919, and The Combines and Fair Prices Act, 1919*, [1922] 1 A.C. 191 (P.C.), at p. 201).

[164] With the utmost respect, I believe that the effect of my colleague's reasoning is to answer a question that is not asked, on the basis of factual scenarios different from the one in this case, in order to address a social problem that is not in issue here. I would say nothing more on this, so as not to prejudge the matter should it ever arise.

VI. Conclusion

[165] I find that the majority at the Court of Appeal was correct in upholding the trial judge's determination that the appellant lacked a reasonable expectation of privacy in the IP addresses in the circumstances of this case. Therefore, I would dismiss the appeal.

Appeal allowed, WAGNER C.J. *and* CÔTÉ, ROWE *and* O'BONSAWIN JJ. *dissenting.*

Solicitors for the appellant: McKay Ferg, Calgary.

Solicitor for the respondent: Alberta Crown Prosecution Service, Calgary.

Solicitor for the intervener the Director of Public Prosecutions: Public Prosecution Service of Canada, Halifax.

Solicitor for the intervener the Attorney General of Ontario: Ministry of the Attorney General of Ontario, Crown Law Office — Criminal, Toronto.

Solicitor for the intervener the Attorney General of British Columbia: Attorney General of British Columbia — Criminal Appeals and Special Prosecutions, Victoria.

Solicitors for the intervener the Canadian Civil Liberties Association: Kapoor Barristers, Toronto.

Solicitors for the intervener the British Columbia Civil Liberties Association: Pringle Chivers Sparks Teskey, Vancouver; British Columbia Civil Liberties Association, Vancouver.