

IN THE SUPREME COURT OF CANADA
(On Appeal from the Court of Appeal of Alberta)

BETWEEN:

ANDREI BYKOVETS

APPELLANT

- and -

HER MAJESTY THE QUEEN

RESPONDENT

-

FACTUM OF THE APPELLANT
(Pursuant to Rule 42 of the *Rules of the Supreme Court of Canada*)

MCKAY FERG LLP
1800, 639 6th Ave SW
Calgary Alberta T2P OM9

Sarah Rankin LSA #19961
Ian McKay LSA #12035
Heather Ferg LSA #16808

Tel: 403-984-1919
Fax: 1-844-895-3926
Email: sarah@mckayferg.com

Counsel for the Appellant

POWER LAW
99 Bank St., Suite 701
Ottawa, Ontario K1P 6B9

Jonathan Laxer

Tel & Fax: 613-907-5652
Email: jlaxer@powerlaw.ca

Agent for the Appellant

ORIGINAL : Registrar of the Supreme Court of Canada

Copies To:

Alberta Crown Prosecution Service

Appeals Branch
300, 332 6th Ave SW
Calgary, AB T2P 0B2

Rajbir Dhillon

Tel: 403-297-8444
Fax: 403 -297-4311

TABLE OF CONTENTS

PART I – OVERVIEW AND STATEMENT OF FACTS1

I. OVERVIEW1

II. STATEMENT OF FACTS.....1

A. Background Facts & Evidence1

i. The Police Investigation & Arrest.....2

ii. The Charter Challenge at Trial.....2

iii. The Trial Judge’s Findings4

iv. Reasons of the Alberta Court of Appeal5

PART II – QUESTION IN ISSUE7

PART III – STATEMENT OF ARGUMENT.....7

A. RELEVANT LAW7

i. The Threshold Question for Section 8.....7

ii. Section 8 and Informational Privacy8

iii. Informational Privacy and Anonymity Online8

iv. The Contours of Digital Privacy9

v. The Responsive Approach to Section 8 in Canada.....10

vi. Section 8 and IP Addresses11

B. APPLICATION OF THE LAW12

i. Misidentifying What the Police Were After12

ii. The Realities of Mass Data Collection.....15

C. CONCLUSION.....17

PART IV – COSTS18

PART V – ORDER SOUGHT18

PART VI – CASE SENSITIVITY.....18

PART VII - TABLE OF AUTHORITIES19

PART I – OVERVIEW AND STATEMENT OF FACTS

I. OVERVIEW

[1] This appeal is about whether digital privacy reflects digital reality. No one can use the internet without connecting to it. The technical reality of internet connections risks revealing an anonymous internet user as a specific individual in a specific location. It may reveal them down to the device in their hands. The question of whether an Internet Protocol (“IP”) address attracts a reasonable expectation of privacy determines whether connecting to the internet means surrendering anonymity to the state for all purposes.

[2] For over a decade, this Court has crafted responsive and evolving protections for the rights of Canadians to think, act and communicate online. The decision of the majority of the Alberta Court of Appeal (“ABCA”) renders those protections meaningless. Upholding it means upholding a limitless police power to monitor and surveil Canadians’ online activities.

[3] The Appellant asks this Court to endorse the holding of the dissenting Justice below. IP addresses engage a reasonable expectation of privacy because they are “the identity of an internet user which corresponds to [that] particular IP address [and are] linked to a particular, monitored internet activity.”¹ The *Criminal Code* contains the tools police need to get this information. A reasonable expectation of privacy ensures they are only able to do so when the intrusion is justified.

II. STATEMENT OF FACTS

A. Background Facts & Evidence

[4] The Appellant stands convicted of 14 offences for using unauthorized credit card data to purchase gift cards online, using those gift cards to make purchases in stores, and possessing credit card related material which was found during the execution of a search warrant on his home.² The address information underlying the search warrant was obtained as a direct result of police

¹ Memoranda of Judgment of Schutz, Crighton and Veldhuis JJ.A., 13 June 2022 at para 77 Appellant’s Record [AR], **Tab 1D [CA Judgment]**.

² Exhibit 1, Agreed Statement of Facts on the Voir Dire, March 5, 2020, **AR Tab 4A**. A magnetic strip reader and encoder, 8 payment cards, and four counterfeit certificates of Canadian citizenship.

identifying the Appellant’s IP address. He raised three *Charter* arguments at trial – including that the warrantless seizure of his IP address violated his s 8 rights. The trial judge found there was no violation of s 8, because there is no expectation of privacy in an IP address.

i. The Police Investigation & Arrest

[5] In October of 2017, Co-Op (a grocery store chain) reported some online transactions to the Calgary Police Service (“CPS”), believing that they may be fraud. CPS began investigating whether the purchases were made with illegally obtained credit card information.

[6] CPS learned that Co-Op did not manage their own online sales. They used Moneris, a specialized company, to process credit card transactions on Co-Op’s website. Detective Laustsen (the “Primary Investigator”) tasked an officer with contacting Moneris to obtain the IP addresses for the transactions being investigated.^{3 4} The Primary Investigator wanted this information to connect the online purchases to the physical location of the purchaser.⁵ Moneris responded to the CPS email request with the two IP addresses that engaged in the transactions.⁶

[7] With the IP addresses, CPS identified the Internet Service Provider whose customer used those addresses. Police obtained the customer information *via* production order, and learned each IP address was associated to a different customer and residential address. The Primary Investigator believed one address belonged to the Appellant, and the other to his parents.⁷ She obtained search warrants for both addresses, and they were executed back-to-back on November 21, 2017.⁸ As part of the investigative itinerary, the Appellant was arrested at 8:00AM that morning when his vehicle was stopped after leaving his residence.

³ Reasons for Judgment of Ho J., Court of Queen’s Bench of Alberta, 29 January 2020 at paras 5-6, **AR Tab 1C [VD Reasons]**.

⁴ Trial Transcript at pp 56, 26-32, **AR Tab 3A**.

⁵ Trial Transcript at pp 56, 39-41, **AR Tab 3A**.

⁶ VD Reasons at para 7, **AR Tab 1C**.

⁷ Trial Transcript at pp 57, 3-18, **AR Tab 3A**.

⁸ VD Reasons at para 10, **AR Tab 1C**.

ii. The Charter Challenge at Trial

[8] An expert report tendered at trial provided information about IP addresses.⁹ It explained that there are internal and external IP addresses. An external IP address is like a home address, and an internal IP address is like a room in a house. The external address is what the internet service provider assigns to a router, and it is what the outside world identifies and connects to. Typical residential internet subscriptions receive a dynamic external IP address, meaning it may change from time to time. The external IP address is assigned by the internet service provider, and each IP address is assigned to only one subscriber at a time. So, while the IP address might be changed, it will always be tied to the subscriber who had it at the time that the relevant internet activity happened. Like a home address, it is possible a family's address might change, but it will always be possible to say where the family lived at a particular time, and that the people who sent or received mail at that address at that time were the people who lived there then.

[9] The internet transmits information in packets of data. Everything seen, sent or received online is broken down into packets of data sent through the internet, received at a destination, and displayed for the internet user. IP addresses are the mailing addresses of the internet: they are the way that the internet knows where to send data. If a computer user types a website address into their internet browser, the request for the data that will make the website appear is useless unless the internet knows which IP address it should send information to. When that information arrives at the router from anywhere in the world, the internal IP address is how the router keeps track of which phone, tablet or other device is connected to the network, and should receive the information. The internal IP address is why search results don't display on every device we own, when we perform that search from our cell phone or tablet.

[10] Unlike a home address, an IP address maintains a log of every letter, postcard or communication that the person who lives there has ever sent. The expert explained this means an IP address's internet activity is capable of directly identifying the internet user who performed that activity. If John Smith used his laptop to check his Google email address, and then did a Google maps search for directions from his home to Walmart, his IP address would be connected to these activities. Google would have the name and home address of the internet user which performed

⁹ Exhibit VD-2, Agreed Statement of Facts, 9 January 2020, **AR Tab 4C**.

these online activities. Without accessing his ISP subscriber information, John Smith’s use of one of the internet’s most common sites would have located and identified him. It is “not necessary to obtain the ISP-held subscriber information in order to accurately identify a particular internet user” if information held by third party companies is available to the person seeking to identify the internet user.¹⁰

iii. The Trial Judge’s Findings

[11] The Trial Judge considered whether there is a reasonable expectation of privacy in an internet user’s IP address.¹¹ She referred to the factors which govern the inquiry into whether a reasonable expectation of privacy exists: the subject matter of the search, the claimant’s interest in the subject matter, the claimant’s subjective expectation of privacy in the subject matter, and whether that expectation is objectively reasonable in the totality of the circumstances.¹² She described the normative inquiry relevant to s 8 – whether sanctioning the surveillance in question would diminish freedom and privacy in ways inconsistent with the aims of a free and open society.¹³

[12] The Trial Judge considered the subject matter of the search. She acknowledged that she had been asked to interpret the subject matter of the search functionally, rather than narrowly.¹⁴ She asked herself what the police were really after, and held the subject matter of the search was “the IP addresses which [police] sought for the purpose of being able to further the investigation.”¹⁵

[13] The Trial Judge found that the Appellant had an interest in the subject matter of both IP addresses (the one he was the subscriber for and the one used at his father’s address). She was also prepared to assume the Appellant had a subjective expectation of privacy in relation to the IP address.¹⁶

¹⁰ Exhibit VD-2, Agreed Statement of Facts, 9 January 2020, **AR Tab 4C**.

¹¹ VD Reasons at para 26, **AR Tab 1C**.

¹² VD Reasons at para 32, **AR Tab 1C**.

¹³ VD Reasons at para 33, **AR Tab 1C**.

¹⁴ VD Reasons at para 38, **AR Tab 1C**.

¹⁵ VD Reasons at para 44, **AR Tab 1C**.

¹⁶ VD Reasons at paras 46-47, **AR Tab 1C**.

[14] The Trial Judge went on to ask whether the expectation of privacy was objectively reasonable. She considered the argument that the IP address information reflected activities done in the home, but held that the place of the search was “within the database of a third-party.”¹⁷ This made it a non-determinative factor. The fact that ISPs assign and can change IP addresses was also non-determinative.¹⁸

[15] The trial judge considered the nature of the subject matter. She found that IP addresses are “a collection of numbers” which do not disclose the “biographical core of personal information.”¹⁹ She held that police would need to identify which third party website to access, and then gain access in order to identify a specific user through their IP address. It therefore did not reveal intimate details of a claimant’s lifestyle.

[16] The trial judge determined that there is no reasonable expectation of privacy in an IP address. This decision was “heavily influenced by the analysis regarding the subject matter of the search.”²⁰ She held that an “IP address in itself does not reveal information about a subscriber that should be protected in a free and democratic society.”²¹ She emphasized that the Expert Report specified that identifying an individual through their IP address would require police to “gain access to a third-party website.”²² She questioned why “an investigator would do that when they are able to access a public resource listing IP addresses to identify an ISP” and then “seek judicial authorization before obtaining specific subscriber information from that ISP.”²³

iv. Reasons of the Alberta Court of Appeal

[17] The majority at the ABCA described IP addresses as an “abstract” number that, standing alone, reveals nothing.²⁴ They upheld the trial judge’s conclusion that “the appellant has no

¹⁷ VD Reasons at paras 52-54, **AR Tab 1C**.

¹⁸ VD Reasons at para 58, **AR Tab 1C**.

¹⁹ VD Reasons at para 56, **AR Tab 1C**.

²⁰ VD Reasons at para 62, **AR Tab 1C**.

²¹ VD Reasons at para 62, **AR Tab 1C**.

²² VD Reasons at para 63, **AR Tab 1C**.

²³ VD Reasons at para 63, **AR Tab 1C**.

²⁴ CA Judgment at paras 3, 17 and 21, **AR Tab 1D**.

reasonable expectation of privacy in an IP address and there is no requirement for the police to obtain judicial authorization at that preliminary stage in the investigation.”²⁵

[18] The majority rejected the comparison of IP addresses to cases finding an expectation of privacy in the IMSI or IMEI numbers used to identify cell phones. The majority stated that, “in those cases, the subject or identity of the target is generally known” and “[m]ore importantly, in those situations, over time the police can glean ‘significant personal information’ from the IMSI and IMEI numbers such as drawing inferences about a target’s cell usage and web browsing.”²⁶ They rejected the comparison between an IP address and a house address on the basis that an IP address does not tell police where the address is being used or who is using it.²⁷

[19] Justice Veldhuis’s dissenting judgment would have allowed the appeal. She found the trial judge erred in finding there is no reasonable expectation of privacy in an IP address and as such, the seizure of that information required prior judicial authorization.

[20] Veldhuis J. held that while the trial judge was alive to the requisite normative inquiry, she failed to “undertake her analysis with the normative approach in mind. Had she done so, she would have concluded that this situation is indistinguishable from *Spencer*.”²⁸ She held seizing IP addresses linked to particular internet activity is no different than asking for subscriber information – both are investigative techniques aimed at identifying an internet user and gathering information to draw inferences about the intimate details of their lifestyle and personal choices.²⁹ By viewing the subject of the search as simply a collection of numbers separated by periods, the trial judge performed an “extremely narrow analysis of the subject matter” contrary to this Court’s direction in *Spencer*.³⁰ Treating an IP address as generic information was in error because it ignored how it can be used as a pathway to identification and there was no consideration of the ability of that information to reveal further details about the user.³¹ IP addresses act as a trace; the question in issue was the *tendency* of that information to support inferences about other personal

²⁵ CA Judgment para 22, **AR Tab 1D**.

²⁶ VD Reasons at para 18, **AR Tab 1C**.

²⁷ VD Reasons at para 21, **AR Tab 1C**.

²⁸ VD Reasons at para 62, **AR Tab 1C**.

²⁹ VD Reasons at para 62, **AR Tab 1C**.

³⁰ VD Reasons at para 66, **AR Tab 1C**.

³¹ VD Reasons at paras 68-71, **AR Tab 1C**.

information.³² Veldhuis J. found that when one took a “broad and functional approach” the subject matter of the search was not a collection of numbers, “but rather the identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity.”³³ This is a content neutral analysis that engages the issue of privacy as anonymity and the IP addresses in question attracted a high level of informational privacy.³⁴

[21] Veldhuis J. found the trial judge’s error in characterizing the subject matter of the search was compounded in her analysis of whether the Appellant’s subjective expectation of privacy was objectively reasonable. When the analysis was conducted with the full breadth of the subject matter taken into account, the expectation of privacy was objectively reasonable.

PART II – QUESTION IN ISSUE

[22] The Appellant raises the following ground of appeal:

- I. Does a reasonable expectation of privacy attach to an internet protocol address?

PART III – STATEMENT OF ARGUMENT

A. RELEVANT LAW

i. The Threshold Question for Section 8

[23] Section 8 is engaged where, and only where, an individual has a reasonable expectation of privacy in the target of the proposed search or seizure. Assessing whether a reasonable expectation exists is content-neutral, and turns “on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought.”³⁵ Determining whether a reasonable expectation of privacy exists requires considering the following factors:

- I. What was the subject matter of the search?

³² VD Reasons at paras 73-74, **AR Tab 1C**.

³³ VD Reasons at para 77, **AR Tab 1C**.

³⁴ VD Reasons at para 80, **AR Tab 1C**.

³⁵ *R v Spencer*, [2014 SCC 43](#) at para 36 [*Spencer*]; *R v Patrick*, [2009 SCC 17](#) at para 32 [*Patrick*].

- II. Did the respondent have a direct interest in the subject matter?
- III. Was there a *subjective* expectation of privacy in the subject matter?
- IV. If so, was the expectation *objectively* reasonable?³⁶

[24] The approach to the analysis is normative, not descriptive.³⁷ The issue is whether the target of the search should be “beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society.”³⁸ An expectation of privacy does not prevent state access to the target. It determines whether the state may intrude at its sole discretion, without oversight.

ii. Section 8 and Informational Privacy

[25] Informational privacy protection safeguards “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.”³⁹ It also protects an individual’s interest in “when, how, and to what extent information... is communicated to others.”⁴⁰ Considering whether information has “sufficient capacity to reveal personal activities within the home” is relevant to evaluating whether it “support[s] the existence of a reasonable expectation of privacy.”⁴¹ The analysis is not simply about what the information amounts to. It must go “beyond the data itself to the reasonable inferences available from the data and what those inferences could say about activities within the home.”⁴²

iii. Informational Privacy and Anonymity Online

[26] In the digital era, informational privacy concerns both the contents of communications, and the context in which they take place. This includes both the fact and content of an online activity, and the connection of an individual to that activity. The right to anonymity is “particularly important in the context of internet usage” and interpreting section 8 “must include this

³⁶ *R v Tessling*, [2004 SCC 67](#) [*Tessling*].

³⁷ *Tessling* at para 42; *Spencer* at para 18; *Patrick* at para 14.

³⁸ *R v Ward*, [2012 ONCA 660](#) at para 87.

³⁹ *Tessling* at para 25.

⁴⁰ *Tessling* at para 23.

⁴¹ *R v Orlandis-Habsburgo*, [2017 ONCA 649](#) at para 66 [*Orlandis-Habsburgo*].

⁴² *Orlandis-Habsburgo* at para 66.

understanding of privacy.”⁴³ The privacy right attached to anonymity protects someone who has shared information but has done so with the understanding and expectation “it will not be identified with the person providing it.”⁴⁴ The mere fact that the information is visible, and that the person has relinquished some control, does not extinguish their right to remain anonymous and unconnected to the information. Anonymity “permits individuals to act in public places but preserve freedom from identification and surveillance.”⁴⁵ This is essential in the digital age, given “one of the defining characteristics of some types of Internet communication” is that it “may be accessible to millions of people but it is not identified with its author.”⁴⁶

iv. The Contours of Digital Privacy

[27] Digital privacy is *sui generis*. The Supreme Court has observed it “is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer.”⁴⁷ While the law has attempted to make sense of the risks through analogies to the analog world, certain features of digital systems mean this “kind of information has no analogue in the physical world.”⁴⁸

[28] The analogies break down both because of the sheer volume and personal nature of digital information, but also because of how much of it is automatically generated without a user’s knowledge. Browsers retain “information about the websites the user has visited in recent weeks and the search terms that were employed to access those websites” which can “enable investigators to access intimate details about a user’s interests, habits, and identity, drawing on a record that the user created unwittingly.”⁴⁹ A user may not know this record exists, it may survive their attempts to delete it, or it may be that a user could never delete it.⁵⁰

⁴³ [Spencer](#) at para 41.

⁴⁴ [Spencer](#) para 42.

⁴⁵ [Spencer](#) at paras 42-43.

⁴⁶ [Spencer](#) at paras 44-45 relying on A.F. Westin, *Privacy and Freedom* (1970); *R v Wise*, [\[1992\] 1 SCR 527](#).

⁴⁷ *R v Vu*, [2013 SCC 60](#) at para 40 relying on *R v Morelli*, [2010 SCC 8](#) and *R v Cole*, [2012 SCC 53 \[Vu\]](#).

⁴⁸ [Vu](#) at para 40.

⁴⁹ [Vu](#) at para 42.

⁵⁰ [Vu](#) at para 43.

v. The Responsive Approach to Section 8 in Canada

[29] The heightened exposure of personal information in the digital era has driven consistently robust decisions of this Court to protect it. When scrutinizing the seizure of electronic conversations, societal interests in protecting individual freedoms will outweigh state concerns regarding effective law enforcement.⁵¹ Section 8 protections afforded to private communications “should not be lightly denied”;⁵² the state’s “unfettered discretion to record and transmit our words” remains an “insidious danger.”⁵³

[30] A key feature of the approach is a renewed emphasis on defining the target of the search purposively and normatively. More than ever, Courts must understand what is at stake in a search and perform an analysis that goes beyond a literal description of the information seized. This Court has led the way in a sustained manner for over a decade. *Spencer* concerned access to the account information held by an internet service provider. The account information consisted of “simply a name and address” but the Court was clear this was the wrong way to define the terms of the search: what the police were really after was the connection between this information, and what it had the capacity to reveal about particular activity on the internet.⁵⁴ In *Marakah*, the interest at stake in police access to text messages was not simply the “actual contents of the messages the police have seized” but the potential for the text conversation to “reveal personal or biographical information”, and “to betray ‘information which tends to reveal intimate details of the lifestyle and personal choices of the individual.’”⁵⁵ When the police seized a computer from the home in *Reeves*, the object of the computer was not what was at risk.⁵⁶ “[W]hat the police were really after” was “the data it contained about Reeves’ usage, including the files he accessed, saved and deleted.”⁵⁷

[31] For the law to be responsive to digital privacy concerns, it must also ensure that its approach does not extinguish digital privacy rights by placing inappropriate emphasis on basic features of digital activity. In particular, Courts must be attentive to the unavoidable fact that digital

⁵¹ *R v Marakah*, [2017 SCC 59](#) at para 53 relying on *R v Plant*, [\[1993\] 3 SCR 281](#) [*Marakah*].

⁵² *Marakah* at para 53.

⁵³ *Marakah* at para 40 citing *R v Duarte*, [\[1990\] 1 SCR 30](#) at 44 [*Duarte*].

⁵⁴ *Spencer* at paras 32-33.

⁵⁵ *Marakah* at para 32.

⁵⁶ *R v Reeves*, [2018 SCC 56](#) [*Reeves*].

⁵⁷ *Reeves* at paras 29-30.

activity requires third party service providers and infrastructure. The section 8 protection is *as against the state* and activities that provide information to third parties do not dictate the outcome of the analysis. Communications rely on intermediary service providers, but customers are entitled to assume they will not share the contents of their communications.⁵⁸ More than ever, communications are committed to writing, but that does not mean the sender must forego any reasonable, ongoing expectation by the originator of the communication that the recipient will keep the information to himself.⁵⁹ A privacy interest in an electronic communication against the state is not lost even though the recipient could forward the message to some other person.⁶⁰

[32] The same holds for information created because digital communication requires the use of third-party services. This has been considered in the context of cell phones, which cannot communicate without cell towers that retain information about the devices that connect to them. This data amounts to collections of numbers and requires a comparison or connection to other data to produce identifying information or patterns. Courts have found that police are not entitled to simply obtain large tranches of that information, even *via* production order.⁶¹ They are also not entitled to indiscriminately suck that information out of the air with specialized search devices.⁶² While a single deployment of such a device, or the raw data produced from towers, may produce numbers without any identifying context, failing to protect the information with a reasonable expectation of privacy would allow unfettered access. This presents the possibility such investigative measures would “begin to build a profile of personal information” through patterns.⁶³

vi. Section 8 and IP Addresses

[33] This Court has considered the broader issues at stake in identifying an internet user through their IP address. The issue in *Spencer* was identifying the individual responsible for a particular piece of internet activity by obtaining their information from their Internet Service Provider. The Court found this information is private. Information identifying “specifically observed,

⁵⁸ *R v Jones*, [2017 SCC 60](#) at para 37.

⁵⁹ *Marakah*; *Spencer* at para 40 adopting *R v Dymont*, [\[1988\] 2 SCR 417](#) at 429-30. See also: *R v Pelucco*, [2015 BCCA 370](#) at paras 52 and 71.

⁶⁰ *Marakah* at paras 32, 40-41 and 54.

⁶¹ *R v Rogers Communications Partnership*, [2016 ONSC 70](#).

⁶² *R v Jennings*, [2018 ABQB 296](#) [*Jennings*].

⁶³ *Jennings* at para 66.

anonymous Internet activity engages a high level of informational privacy” because a “reasonable and informed person concerned about the protection of privacy would expect one’s activities on one’s own computer used in one’s own home would be private.”⁶⁴ Informational privacy covers more than whether information is known or seen, protecting it requires protecting the interest a person has in keeping their information secret or confidential – and in ensuring that recipients of that information will hold it in trust and confidence. The right protects the power to control one’s information, including to whom, when, how and to what extent it is shared or disseminated. A person may not keep certain information secret from the whole world, but it is still reasonable for a person to expect “that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged” and that expectation “must be protected.”⁶⁵

B. APPLICATION OF THE LAW

[34] The majority erred in concluding that an IP address is simply a meaningless string of numbers.⁶⁶ This error was rooted in misidentifying what was at stake when the state obtains an IP address. The ABCA majority applied an artificially narrow approach to what makes information private. The majority also failed to address the implications of its decision more broadly and instead took comfort in unjustified and unsupportable assumptions about how IP address seizures will be used by police. The result was errors in defining the subject matter of the search and an erroneous conclusion that IP addresses do not attract a reasonable expectation of privacy.

i. Misidentifying What the Police Were After

[35] Defining the subject matter of a search is an essential step in ensuring s 8 serves its purposes. The interpretation of s 8 has entrenched it as a normative and prospective right. The content of the right is reflected in the analytical approach taken to giving it effect. Our privacy law embodies our collective concern for protecting spaces for dissent, grown and exploration, and awareness of what losing these spaces costs us as a whole. This is built-in to the content neutral approach to the right - ensuring that novel s 8 issues are always considered through the lens of society as a whole. It is built-in through an inquiry that asks what *should* be private rather than

⁶⁴ [Spencer](#) at para 51.

⁶⁵ [Duarte](#) at 46.

⁶⁶ CA Judgment at para 21, **AR Tab 1D**.

accepting any *status quo* as determinative. And it is built-in to the first question in determining whether a reasonable expectation of privacy exists in the target of the search: what are the police really after?

[36] The trial and majority ABCA decisions in this case took a “mechanical” and reductive view of this question.⁶⁷ The majority’s definition is a mere description, holding an IP address is “an abstract number” that “reveals nothing.”⁶⁸ This approach stopped short at “the nature of the precise information sought” and failed to engage with “the nature of the information that it reveals.”⁶⁹ The majority and the trial judge asked what the police were after when they seized IP addresses, and held the answer was IP addresses. *Spencer* specifically admonished this approach. It collapses the privacy interest in the “identity of a subscriber whose Internet connection is linked to particular, monitored activity” into “the mundane” basic description of the information sought.⁷⁰

[37] The police explanation for seeking the information made its capacity to identify or support identifying inferences clear. CPS did not want a string of numbers. CPS wanted 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. The majority’s approach, however, was to find that nothing short of completely identifying information is private. This turned the animating concern in *Spencer* on its head. Internet user account information was protected by *Spencer* because online activity is deeply private, and what tends to identify us with our online activities is therefore private.

[38] The majority’s reliance on the fact that police needed to take an additional investigative step to identify the internet user in this case was misplaced and inconsistent with the approach urged by this Court.⁷¹ Outside and within the digital sphere, our law has long recognized information may be deeply private without being directly identifying. The collection of organic chemicals which comprises DNA, for example, is useless for identification unless police have other information from a suspect or an existing databank. Vehicle tracking information is unhelpful

⁶⁷ [Marakah](#) at para 17.

⁶⁸ CA Judgment at para 21, **AR Tab 1D**.

⁶⁹ [Spencer](#) at para 26.

⁷⁰ [Spencer](#) at paras 25-33.

⁷¹ [Spencer](#) at para 44.

without information about the owner and, more likely, the driver of the vehicle. In *Reeves*, this Court recognized that seizing a home computer did not take police directly to the information they wanted – they needed a distinct search warrant to search that computer. In all these scenarios, we recognize that privacy interests are placed at incrementally heightened risk as the state gets closer to ultimately identifying information, or as the rights-holder loses their ability to shield personal information from the state.

[39] The majority’s approach reflected none of these principles. The analysis considered only whether the information capable of being revealed by an IP address was identical to the information revealed by the subscriber information in *Spencer*. Finding it was not, the majority concluded no information was revealed at all. The analysis decontextualized the question and so misapprehended the interests at stake, finding an IP address “is an abstract number that reveals none of the core biographical information the issuer of that IP address attaches to it” and that “[s]tanding alone, it reveals nothing.”⁷²

[40] What was missed by the majority is apparent in the decision of the dissenting Justice. Her ruling reflects that the issue was not whether this information was identical to the information in *Spencer*. Her analysis is animated by questions that reflect the core purposes of section 8 – why police wanted the IP address and whether the animating principles of digital privacy cases including *Spencer* meant they should be allowed unfettered access to it. Having identified these as the central concerns, the dissent concluded that the privacy interest in this case was similar to that in *Spencer* because, “[b]oth investigative techniques are aimed at gathering information to ascertain the identity of an internet user and allow the police to gather further information to draw inferences about the intimate details of the lifestyle and personal choices” of an internet user.⁷³

[41] Recognizing this did not mean treating the information as though it was identifying in the same way. Rather, the dissenting Justice’s emphasis on examining the police purpose in seeking the information, and the risks it represents, permitted meaningful consideration of whether unrestricted state access to IP address information should be tolerated in a free and democratic

⁷² CA Judgment at para 21, **AR Tab 1D**.

⁷³ CA Judgment at para 62, **AR Tab 1D**.

society. The dissenting Justice’s approach to the question, and her ultimate conclusion that IP addresses are protected by a reasonable expectation of privacy, should be upheld by this Court.⁷⁴

ii. The Realities of Mass Data Collection

[42] The majority’s emphasis on whether IP addresses are directly identifying set too high a bar for privacy protection. It also reflected errors regarding the capacity of IP addresses to identify internet users, or associate them with particular internet activities. As a result, the majority erred in assessing the broader risks in leaving IP addresses unprotected by s 8. Their approach failed to recognize IP address collection is a stand-alone way of tracking and identifying users through data triangulation. As Veldhuis J. observed, “if this decision stands, there is nothing preventing third parties from handing over IP addresses without warrant, whenever asked by the police for whatever reason, so that the police can gather digital breadcrumbs about a particular internet user.”⁷⁵ Unlimited IP address collection opens the door to mass data collection, and indiscriminate online surveillance by police. The existence of the authorization requirement in *Spencer* offers no protection against investigative techniques capable of identifying internet users in other ways.

[43] The evidence in this case included the example that an IP address would be logged if someone accessed their Facebook or email account.⁷⁶ The IP address of a person who checked their email address, johnsmith1965@gmail.com, would be associated to that email.⁷⁷ Obtaining the identity of a user in such circumstances is a one-step process. The person who logged into the Facebook account with John Smith’s picture is highly likely to be John Smith. The person who checked John Smith’s email is probably also John Smith. If the same IP address does both, that IP address appears to belong to John Smith.

[44] The evidence that an IP address is connected to each instance a person opens their Facebook profile is significant. The example of Facebook applies equally to a person who uses LinkedIn, Twitter, a site which maintains resumes for virtual job postings, or any other website. The decision in this case enables police to ask for the IP address that last logged into their account.

⁷⁴ CA Judgment at para 65, **AR Tab 1D**.

⁷⁵ CA Judgment at para 70, **AR Tab 1D**.

⁷⁶ Exhibit VD-2, Agreed Statement of Facts, 9 January 2020, **AR Tab 4C**.

⁷⁷ Exhibit VD-2, Agreed Statement of Facts, 9 January 2020, **AR Tab 4C**.

The picture, city, work history and friend network of the person who opens the website may be publically visible on their profile. Police now have an IP address connected to a name, geographical area, professional skillset, and a myriad of other information. This can be compared to other instances where the same IP address was used.

[45] The privacy interests at stake are brought into stark relief when this type of data collection is considered at scale. As above, some online activities identify the user on their face – a Facebook account in one’s own name, for example. Obtaining the IP address associated with activity on that Facebook page draws a direct link to the user. Comparing that IP address with other online activities conducted anonymously shatters anonymity completely. *Spencer* addressed one method of identifying internet users without judicial authorization – through their account information. The privacy interest at stake in anonymity online is also engaged where those internet users may be identified in another way – through associating their IP address with activities online which are capable of identifying them and which “ten[d] to reveal intimate details of the lifestyle and personal choices of the individual”, or which enable “strong and reliable inference[s]” through patterns.⁷⁸

[46] The majority’s approach reflected the trial judge’s reasoning on this point. The trial judge was satisfied that “an IP address in itself does not reveal information about a subscriber that should be protected in a free and democratic society.”⁷⁹ Although she acknowledged “police might be able to obtain information about a user’s identity” through IP address information, she questioned “why an investigator would do that when they are able to access a public resource listing IP addresses to identify an ISP” and then “seek judicial authorization before obtaining specific subscriber information from that ISP.”⁸⁰ In the end, she saw “little to be gained from a normative perspective” since investigators could simply get a production order for subscriber information and would not need to try to identify individuals based on IP addresses alone.⁸¹

[47] Nothing supports the assumption that IP addresses will be sought solely during investigations and exclusively as precursors to *Spencer* warrants. The majority’s ruling makes this

⁷⁸ *Spencer* at para 27. See also *R v Gomboc*, [2010 SCC 55](#) at para 81.

⁷⁹ VD Reasons at para 62 (emphasis added), **AR Tab 1C**.

⁸⁰ VD Reasons at para 63, **AR Tab 1C**.

⁸¹ VD Reasons at paras 63-65, **AR Tab 1C**.

assumption untenable. Limiting police access to IP addresses to investigative contexts where it is justified is achieved by recognizing an expectation of privacy. In the absence of that, collecting them proactively and for any purpose is fair game for law enforcement. There is no constraint on building an IP address equivalent of a facial recognition database for internet activity. The majority's decision permits police to notice online content that interests or bothers them, and ask a website for the poster's IP address as they please.

[48] The issue in this case was when “in the iterative process of police gathering electronic information do they [the police] need to seek a warrant to ensure that there is a warrant at the point the numbers are associated with a particular person?”⁸² Veldhuis J. held that privacy protection starts at the beginning of the investigative chain police may use to identify an internet user. She affirmed that the point at which constitutional protection begins is answered by examining what the information “tends to reveal,” particularly in the context of privacy as anonymity.⁸³ Noting police have the statutory tools to seek this information, her answer ensures this information is only available if the pressing public interest in a criminal investigation justifies its release to the state.

C. CONCLUSION

[49] The misidentification of the subject of the search, the mistaken belief that police would be somehow limited from approaching third-parties if no section 8 protection applied, and the error in identifying the information at stake and whether it was already protected by *Spencer*, lead the trial judge and subsequently the majority into error on the issue of whether IP addresses attract a reasonable expectation of privacy. The risks of leaving this information unprotected are grave, and the decision in this case should not be permitted to stand.

⁸² CA Judgment at para 73, **AR Tab 1D**.

⁸³ CA Judgment at paras 74, 79, **AR Tab 1D**.

PART IV - COSTS

[50] The Appellant does not seek costs against the Crown and requests that no costs be awarded against him.

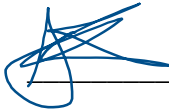
PART V – ORDER SOUGHT

[51] The Appellant asks that this Court allow the appeal and return the matter for a new trial.

PART VI – CASE SENSITIVITY

[52] There are no restrictions listed in Rule 42(2)(f) of the Rules of the Supreme Court of Canada in this case that would have an impact on this Court’s reasons.

ALL OF WHICH IS RESPECTFULLY SUBMITTED THIS 22nd DAY OF AUGUST, 2022



SARAH RANKIN

HEATHER FERG

Counsel for the Appellant

PART VII - TABLE OF AUTHORITIES

CASE LAW	PARA(S)
<i>R v Cole</i> , 2012 SCC 53	27
<i>R v Duarte</i> , [1990] 1 SCR 30	29, 34
<i>R v Dymment</i> , [1988] 2 SCR 417	31
<i>R v Gomboc</i> , 2010 SCC 55	46
<i>R v Jennings</i> , 2018 ABQB 296	32
<i>R v Jones</i> , 2017 SCC 60	31
<i>R v Marakah</i> , 2017 SCC 59	29-31, 37
<i>R v Morelli</i> , 2010 SCC 8	27
<i>R v Orlandis-Habsburgo</i> , 2017 ONCA 649	25
<i>R v Patrick</i> , 2009 SCC 17	23-24
<i>R v Pelucco</i> , 2015 BCCA 370	31
<i>R v Plant</i> , [1993] 3 SCR 281	29
<i>R v Reeves</i> , 2018 SCC 56	30
<i>R v Rogers Communications Partnership</i> , 2016 ONSC 70	32
<i>R v Spencer</i> , 2014 SCC 43	23-24, 26, 30-31, 34, 37, 39, 46
<i>R v Tessling</i> , 2004 SCC 67	23-25
<i>R v Vu</i> , 2013 SCC 60	27-28
<i>R v Ward</i> , 2012 ONCA 660	24
<i>R v Wise</i> , [1992] 1 SCR 527	26