File Number: 40269

IN THE SUPREME COURT OF CANADA

(ON APPEAL FROM THE COURT OF APPEAL OF ALBERTA)

BETWEEN:

ANDREI BYKOVETS

Appellant
(Appellant)

- and -

HIS MAJESTY THE KING

Respondent
(Respondent)

FACTUM OF THE RESPONDENT
HIS MAJESTY THE KING

RULES 36 AND 42 OF THE *RULES OF THE SUPREME COURT OF CANADA*

RAJBIR DHILLON
Counsel for the Respondent
Alberta Crown Prosecution Service
300, 332 – 6 Avenue S.W.
Calgary, AB T2P 0B2
Telephone: 403-297-6005
Fax: 403-297-3453
Email: rajbir.dhillon@gov.ab.ca

D. LYNNE WATT
Ottawa Agent for the Respondent
Gowling WLG (Canada) LLP
2600, 160 Elgin Street
Ottawa, ON K1P 1C3
Phone: (613) 786-8695
Fax: (613) 788-3509
Email: lynne.watt@gowlingwlg.com

SARAH RANKIN
IAN MCKAY
HEATHER FERG
Counsel for the Appellant
McKay Ferg LLP
1800, 639 – 6 Avenue S.W.
Calgary, AB T2P 0M9
Phone: (403) 984-1919
Fax: (403) 1-844-895-3926
Email: sarah.mckayferg.com

JONATHAN LAZER
Ottawa Agent for the Appellant
Power Law
Suite 701, 99 Bank Street
Ottawa, ON K1P 6B9
Phone/Fax: (613) 907-5652
Email: jlaxer@powerlaw.ca

TABLE OF CONTENTS

Page No.

PART I – OVERVIEW AND FACTS 1

OVERVIEW 1
THE FRAUD INVESTIGATION 2
CHARTER ISSUES 3
TRIAL JUDGE'S RULING 4
ALBERTA COURT OF APPEAL 8

PART II – ISSUES 11

PART III – ARGUMENT 12

GOVERNING LAW 12
NO LINK, NO NEED FOR A WARRANT 13
THE SUBJECT MATTER CANNOT BE REDUCED TO THE INVESTIGATION'S PURPOSE 17
THE TOTALITY OF CIRCUMSTANCES SHOULD NOT INCLUDE SPECULATION 18
FUTURE PREDICTIONS DO NOT ESTABLISH A BREACH OF S 8 18
THE TOTALITY OF CIRCUMSTANCES CANNOT PRESUME BAD FAITH 19
NO OBJECTIVELY REASONABLE EXPECTATION OF PRIVACY 21
CONCLUSION: THE POLICE DID NOT NEED A WARRANT 22

PART IV – COSTS 22

PART V – ORDER SOUGHT 23

PART VI – SUBMISSIONS ON CASE SENSITIVITY 23

PART VII – TABLE OF AUTHORITIES AND LEGISLATION 24

AUTHORITIES 24
LEGISLATION 24

FACTUM OF THE RESPONDENT

PART I – OVERVIEW AND FACTS

Overview

1. An internet protocol ("IP") address is an abstract number. Here, the numbers over which the appellant asserts a reasonable expectation of privacy are 75.156.161.143 and 75.158.6.122 – numbers that expose nothing about the appellant's core biographical details, private life, or online browsing habits. As this Court held in *Spencer*, a privacy interest is raised when the police try to *link* an IP address to subscriber information.[1]

2. This link was *Spencer's* lynchpin. There, once the police had an IP address, their request for subscriber information was a request to link a specific person to specific anonymously undertaken online activities. Thus, to protect a person's interests under s 8 of the *Charter*, this Court held that subscriber information engages a reasonable expectation of privacy.

3. Here, the police complied with *Spencer.* A defrauded company's payment processor gave the police IP addresses used to commit fraud. The police then lawfully obtained a production order for the subscriber information. Before the police got the subscriber information, they knew only that an unknown person using a known IP address was committing fraud from an unknown location. The police compliance with *Spencer* meant the appellant's s 8 interests were protected.

4. The appellant's argument that the police needed a warrant to get the IP addresses from the payment processor serves no reasonable privacy interests. He bases his argument on speculative possibilities about what the police might be able to learn from IP addresses. But as established by this Court, whether a reasonable expectation of privacy exists depends on the totality of circumstances, which admits neither speculative concerns nor predictions about future technology.[2] Here, the totality of circumstances leads to one conclusion: the police did not need a warrant to receive the IP addresses from the payment processor.

---

[1] *R v Spencer*, 2014 SCC 43 at paras 33, 42, 46, 47, 50, 67
[2] *R v Tessling*, 2004 SCC 67 at paras 28-29, 55; *R v Gomboc*, 2010 SCC 55 at para 40

The Fraud Investigation

5. Stolen credit cards were used to make online transactions. A Calgary liquor store, Co-Op Wine Spirits Beer ("Co-Op"), sold gift cards that a customer could buy online with a credit card and then use in physical stores. The lead police investigator, Detective Kendra Laustsen, learned that a person or persons had used the credit card data of people, without their permission, to buy and then use thousands of dollars worth of Co-Op gift cards. Co-Op told Det. Laustsen that Moneris Solutions Corporation ("Moneris") processed the fraudulent transactions. Det. Laustsen assigned another officer, Constable Nelson, to obtain the IP addresses associated to the transactions.[3]

6. Det. Laustsen testified she wanted the IP addresses to find out, relative to these transactions, "if there was an opportunity for investigation." She agreed ultimately she wanted to link the IP addresses to a street address so she could determine where the activity was occurring. But to do this, she first had to find out which Internet Service Provider ("ISP") had issued the IP addresses. She explained that an IP address can be associated to an ISP, who can then provide the subscriber's address. She was clear she could not track a person's location or movements from an IP address.[4]

7. Moneris gave Cst. Nelson the two IP addresses used to make the fraudulent transactions: 75.156.161.143 and 75.158.6.122. Cst. Nelson then conducted a publicly available internet search. From this, he learned that Telus had issued the IP addresses. He then applied for and received a production order for the IP addresses' subscriber information. The appellant does not challenge the lawfulness of this production order.[5]

8. In response to the production order, Telus provided the names and addresses of the subscribers, who turned out to be the appellant and his father. Telus had assigned one IP address

---

[3] *R v Bykovets*, 2020 ABQB 70 ("*Bykovets* ABQB") at paras 5-6, 17 [Appellant's Record ("AR") Tab 1C]; Exhibit 1: Agreed Statement of Facts at paras 3-6, 8-15, 17-19 [AR Tab 4A]; Transcript Testimony of Det. Laustsen at 55/33-56/27 [AR Tab 3A]

[4] *Bykovets* ABQB, *supra* note 3 at paras 16-17 [AR Tab 1C]; Transcript Testimony of Det. Laustsen at 53/35-57/1 [AR Tab 3A]

[5] *Bykovets* ABQB, *supra* note 3 at paras 7-9 [AR Tab 1C]; Exhibit VD-2: Agreed Statement of Facts at paras 2-4 [AR Tab 4C]

to Anatoli Bykovets (the appellant's father), at a specified Calgary address. Telus assigned the other IP address to Andrei Bykovets (the appellant), at a different Calgary address.[6]

9. After the police learned the subscriber information, they obtained another warrant and lawfully searched both addresses. At the appellant's house, they seized instruments of forgery, fraudulent identification documents, and the card data of innocent victims.[7]

***Charter* Issues**

10. At trial, the appellant argued the police violated his s 8 *Charter* rights when they received the IP addresses associated to the fraudulent transactions from Moneris without a court order. He also argued the police breached his s 10(b) *Charter* rights when they delayed his right to counsel while they searched his house. The trial judge agreed with the appellant that his s 10(b) rights were breached, but declined to exclude evidence under s 24(2). The majority of the Court of Appeal upheld the trial judge's s 24(2) ruling; the dissenting justice found it unnecessary to consider the s 24(2) ruling given her s 8 decision. Since this ruling is not a subject of this appeal, the respondent will not address it further.[8]

11. In the s 8 *voir dire*, the appellant filed the report of a computer expert, Matthew Musters, whose opinions, summarized by the trial judge, included:

- An external IP address is used in transferring information across the internet from one source to another.
- An ISP assigns external IP addresses to a subscriber.
- External IP addresses may be dynamic or static, but typical residential subscribers would receive a dynamic external IP address from their ISP.
- An ISP can change a dynamic external IP address without notice to the subscriber.
- The ISP keeps a record of to whom they assign external IP addresses and for what period, and the ISP determines how long it keeps these records.

---

[6] *Bykovets* ABQB, *supra* note 3 at para 9 [AR Tab 1C]
[7] *Bykovets* ABQB, *supra* note 3 at para 10 [AR Tab 1C]; Exhibit 1: Agreed Statement of Facts at paras 20-23 [AR Tab 4A]
[8] *R v Bykovets*, 2022 ABCA 208 ("*Bykovets* ABCA") at paras 3-6, 31-37, 55 [AR Tab 1D]

- An external IP address is distinctly associated with one subscriber during its lease period.
- Without an external IP address, a user cannot send or receive data.
- External IP address information is not typically broadcast publicly, and, in the example of online shopping, the external IP address would be known by the destination server only (excluding any hops it went through on its way).
- A person may choose to share their external IP address using peer-to-peer sharing software, where internet users share files with one another and have their IP address broadcast to all others using the same software to facilitate file sharing.
- In most cases, the ISP who owns a particular external IP address can be determined by entering the IP address into an IP lookup website, but this will not disclose the subscriber information.[9]

12. In his report, Mr. Musters also asserted that a third-party company like Google or Facebook could potentially determine the identity of a person using the internet by tracking an external IP address and examining the internet activity of that user on their site. In turn, another individual (like the police) could "take steps" to determine the identity of an internet user. But, he stated, this was "predicated on the assumption that the individual [i.e., the police] seeking to learn the identity of a particular internet user, is able to access the information logged by the third-party company's website." [i.e., Google or Facebook].[10]

Trial judge's ruling

13. The trial judge found the appellant had no reasonable expectation of privacy in the IP addresses, thus the police did not need a warrant to get them from Moneris. To make this finding, she considered the issues identified in *Spencer*:[11]

---

[9] *Bykovets* ABQB, *supra* note 8 at para 13 [AR Tab 1C]; Exhibit VD-1: Affidavit of Matthew Musters [AR Tab 4B]

[10] *Bykovets* ABQB, *supra* note 8 at para 15 [AR Tab 1C]; *Bykovets* ABCA, *supra* note 3 at para 13 [AR Tab 1D]

[11] *Spencer*, *supra* note 1 at para 18

(i) The subject matter of the alleged search

14. The trial judge found the subject matter of the "search" were IP addresses, which the police wanted to further the investigation. She accepted Det. Laustsen's testimony that she wanted the IP addresses so she could take the next steps in the investigation: look up what ISP assigned the IP addresses and then serve them with a production order for the subscriber information.[12]

15. The trial judge noted that IP addresses do not reveal intimate details about a person's life. She rejected the appellant's argument that with an IP address alone, the police could identify the user of that IP address without having to serve a court order on the ISP. The appellant likened an IP address to the mobile phone data at issue in two trial decisions: *R v Jennings*, and *X (Re)*. In those cases, the courts found the accused had a reasonable expectation of privacy in international mobile subscriber identity ("IMSI") and international mobile equipment identity ("IMEI") numbers that the police obtained with a mobile device identifier ("MDI") or cellular-site simulator ("CSS").[13]

16. The trial judge found those cases were inapt comparators. She noted that unlike here, "the subject or identity of the target is often already known when the MDI or CSS technology is used." More importantly, 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. She found that Mr. Musters' statement that a third party (like Google or Facebook) could "attempt" to identity a user by examining the internet activity of that user on their website, did not show that such parties did this. She also noted that Mr. Musters' statement that a person (like a police officer) could identify a user from an IP address alone was speculative: he predicated it on the assumption that the person "is able to access the information logged by a third party's website." Here, no evidence suggested the police had or sought such access.[14]

---

[12] *Bykovets* ABQB, *supra* note 3 at paras 35-45 [AR Tab 1C]
[13] *R v Jennings*, 2018 ABQB 296; *X (Re)*, 2017 FC 1047
[14] *Bykovets* ABQB, *supra* note 3 at paras 39-42 [AR Tab 1C]

17. The trial judge found the bare IP addresses revealed no meaningful personal information to the police. It was only when the police linked the IP addresses to ISP subscriber information – which they did here through a production order – that meaningful information was revealed:

> In the end, I must define the subject matter of the search functionally and consider the question, "what are the police really after?" I conclude that the subject matter of the search was, as the Primary Investigator testified, the IP addresses which she sought for the purpose of being able to further the investigation. She knew that with the IP addresses, she would be able to take the next investigative step which was to access an open source, described by Mr. Musters as an "IP lookup website", to find out which ISP had control over those IP addresses. But the IP addresses, on their own, did not provide a link to, or provide any other information about, a street address or a person. The IP addresses were used by the CPS to subsequently seek subscriber information from the ISP, which was done by obtaining judicial pre-authorization[15]

(ii) The claimant's interest in the subject matter, and (iii) the claimant's subjective expectation of privacy in the subject matter

18. For the sake of analysis, the trial judge accepted the appellant had as much interest in his father's IP address as his own. For the same reason, she accepted the appellant met the low threshold for establishing a subjective expectation of privacy in the IP addresses.[16]

(iv) Whether the subjective expectation of privacy was objectively reasonable

19. By analyzing the factors identified by the majority in *R v Marakah*, the trial judge found the appellant's subjective expectation of privacy was objectively unreasonable.[17]

- Place the "search" occurred. The trial judge found the place searched was Moneris' database. She rejected the appellant's claim that acquiring the IP addresses was like searching his home.[18]
- Private nature of the subject matter. The trial judge found that IP addresses revealed no private information. Mr. Musters stated the police might be able to use an IP address to "take steps" to identify a person using the internet. But she found this was speculative: "the police would first need to know what third party website to access, and then gain

---

[15] *Bykovets* ABQB, *supra* note 3 at para 44 [AR Tab 1C]
[16] *Ibid* at paras 46-48 [AR Tab 1C]
[17] *R v Marakah*, 2017 SCC 59 at para 24
[18] *Bykovets* ABQB, *supra* note 3 at paras 52-54 [AR Tab 1C]

access to such third-party website in order to attempt to identify a specific user." No evidence suggested this was a reality. Thus, she found an IP address was a "collection of numbers" that "does not, in itself, reveal intimate details of a claimant's lifestyle."[19]

- Control over the subject matter. Though she noted it was not determinative, she found the appellant had no control over the IP addresses.[20]

20. All the *Marakah* factors lined up against the appellant's claim. The trial judge found it was "not objectively reasonable to recognize a subjective expectation of privacy in an IP address used by an individual."[21]

Conclusion: no reasonable expectation of privacy

21. The trial judge concluded the appellant had no reasonable expectation of privacy in an IP address. Thus, the police did not breach the appellant's s 8 rights when, without a warrant, they asked for and received from Moneris the IP addresses used in the fraudulent transactions. Because *Spencer* already protected a person's s 8 interests, the trial judge would not make police get judicial authorization earlier in the investigation:

> In reaching this conclusion, I am heavily influenced by the analysis regarding the subject matter of the search. In my view, an IP address in itself does not reveal information about a subscriber that should be protected in a free and democratic society. While I acknowledge that the police might be able to obtain information about a user's identity, there are significant limitations on this. Obtaining an IP address is an important investigative step for police, but privacy interests are not triggered by mere police investigation. The Courts must continually ask the question, "what are the police really after?", including where electronic devices, technology and digital information are concerned. There must continue to be a balancing of interests in determining the scope of section 8 of the *Charter*.
>
> Based on ***Spencer***, police must seek judicial authorization prior to requesting subscriber information from an ISP. The Court in ***Spencer*** was particularly concerned about linking internet activity to a particular user, which cannot easily be done with an IP address alone. While Mr. Musters' evidence indicated that one could take steps to ascertain an individual's identity with an IP address, this position was predicated on the assumption that an investigator could gain access to a third-party website. I question why an investigator would do that when they are able to access a public resource listing IP addresses to identify an ISP. The

[19] *Ibid* at paras 55-56 [AR Tab 1C]
[20] *Ibid* at paras 57-60 [AR Tab 1C]
[21] *Ibid* at para 61 [AR Tab 1C]

> investigator can then seek judicial authorization before obtaining specific subscriber information from that ISP.
>
> In my view, the balance that is achieved by the ruling in ***Spencer*** remains appropriate. I see little to be gained from a normative perspective, requiring the police to seek judicial authorization earlier in the investigation process, particularly since an IP address may not reveal much information to police at all. Fundamentally, defence counsel asks me to find a reasonable expectation of privacy in any IP address used by an individual, not just his or her own. But accepting defence counsel's position could lead to a strange result in different contexts.
>
> Consider, for example, a scenario where an individual uses a public computer to engage in a fraudulent online transaction. Does that individual have a reasonable expectation of privacy in an IP address in those circumstances? In such a case, the IP address alone would reveal even less from a personal information perspective, and would presumably be less helpful from an investigatory perspective. I conclude that finding a reasonable expectation of privacy in an IP address would not advance the protection of privacy interests expected in a free and democratic society.[22]

22. After the *Charter* rulings, the parties submitted a statement of admitted facts. From this, the trial judge found the appellant used the credit card data of nine people, without their consent, to buy gift cards worth $1,000.00 each. The appellant then used the gift cards to make in-store purchases of alcohol, which store CCTV footage corroborated. She also found the appellant possessed the contraband the police found in his house. She convicted the appellant of fourteen counts: six counts of fraudulent use of named complainants' credit cards (*CC* s 342(3)); five counts of laundering the proceeds of crime by using gift cards knowing they were obtained by crime (*CC* s 462.31); one count of possession of a forged credit card (*CC* s 342(1)(c)); one count of possession of a fraudulent identity document (*CC* s 56.1); and one count of possession of instruments used to forge credit cards (*CC* s 342.01(1)(b)). [23]

Alberta Court of Appeal

23. The majority of the Court of Appeal agreed with the trial judge that the appellant had no reasonable expectation of privacy in the IP addresses provided by Moneris. They found an IP address is an "abstract number that reveals none of the core biographical information the issuer

---

[22] *Ibid* at paras 62-65 [AR Tab 1C]

[23] Exhibit 1: Agreed Statement of Facts [AR Tab 4A]; Reasons for Judgment, Transcript at 223-229 [AR Tab 3A]

of that IP address attaches to it." They observed that an IP address can tell the police something about a person only if they comply with *Spencer* and get a production order for subscriber information.[24]

24. The majority rejected the appellant's analogy between an IP address and a physical address. "An IP address does not tell police where the IP address is being used or, for that matter, who is using it. Nor is there a publicly available resource from which the police can learn this or other subscriber data."[25]

25. Like the trial judge, the majority rejected the appellant's comparison of IP addresses to mobile phone data. They found the reason that a reasonable expectation of privacy exists in IMSI and IMEI numbers that police obtain with MDIs or CSSs, is because in those cases, the identity of the target is generally known when the MDI or CSS is used. They also agreed with the trial judge that in those situations, unlike here, 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]

26. The majority found the trial judge interpreted the subject matter of the search functionally as she needed to. "She understood what the police were 'really after' - IP addresses to further the investigation, hoping the authorized further investigation would reveal names and addresses associated with the IP addresses provided." The majority agreed no privacy interest was protected by requiring the police to obtain a warrant when they make initial inquiries. They noted, "Obtaining an IP address is an important investigative step for police, but privacy interests are not triggered by mere police investigation."[27]

27. Ultimately, the majority found this case was opposite to *Spencer*. In *Spencer*, this Court addressed a situation when, without a warrant, police learned the name and address of an IP address user along with their online tendencies. Here, there was no link between a specific person and their online habits. Rather, the police learned without a warrant only that an

---

[24] *Bykovets* ABCA, *supra* note 8 at para 21 [AR Tab 1D]
[25] *Ibid* at paras 19-20 [AR Tab 1D]
[26] *Ibid* at para 18 [AR Tab 1D]
[27] *Ibid* at paras 22-26 [AR Tab 1D]

"unknown person using a known IP address was committing fraud from an unknown address." This did not engage a reasonable expectation of privacy.[28]

28. The dissenting justice would have held that police need judicial authorization at the start of the investigation before they obtained the IP addresses.[29] She found the trial judge interpreted the subject matter of the police request too narrowly because "the police did not want the IP address for its own sake, rather they wanted the IP address to identify who was involved in the internet activity to purchase the gift cards, which were alleged to be fraudulent." She concluded the subject matter of the search was "the identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity."[30]

29. The dissenting justice found that even though the police complied with *Spencer* and got a production order to learn the IP addresses' subscriber information, the trial judge's analysis reflected "a failure to consider the broader context and long-term consequences of government action." She relied on a "digital breadcrumbs" analogy, stating, "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." She believed the trial judge should have considered possible and unspecified technological advances, stating, "Depending on technological advances, this [gathering of digital breadcrumbs] could disincentivize the police from following the existing practice of obtaining warrants to learn the same or similar information through the ISP."[31]

30. Based on the majority's decision, the appellant's convictions were upheld. The appellant now appeals as of right.

---

[28] *Ibid* at para 17 [AR Tab 1D]
[29] *Ibid* at para 73 [AR Tab 1D]
[30] *Ibid* at paras 76-77 [AR Tab 1D]
[31] *Ibid* at paras 69-70 [AR Tab 1D]

PART II – ISSUES

Question in Issue: Does a reasonable expectation of privacy attach to an internet protocol address?

Respondent's Position: No. A reasonable expectation of privacy attaches to linked subscriber information or other specific identifying information, but not to the IP address itself logged by a third party.

PART III – ARGUMENT

31. An IP address alone provides no window into anyone's private life. An IP address does not tell the police the name, address, or phone number of the user. Untethered to subscriber information, an IP address is an abstract number that reveals neither core biographical details nor the online habits of an identifiable person.

32. The trial judge and majority of the Court of Appeal properly found that the appellant had no reasonable expectation of privacy in the IP addresses logged by Moneris, and that the police compliance with *Spencer* protected his s 8 interests.

Governing law

33. Under s 8 of the *Charter*, "Everyone has the right to be secure against unreasonable search or seizure."[32] Whether this protection was engaged here starts with an examination of whether the appellant had a reasonable expectation of privacy in the subject matter at issue, considering the totality of circumstances. A person's expectation of privacy must be subjectively held and objectively reasonable. If a claimant fails to establish that a reasonable expectation of privacy existed in the subject matter, there is no "search or seizure" under s 8.[33]

34. The reasonable expectation of privacy standard is normative. Thus, while the analysis is sensitive to the factual context, it is "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".[34]

35. Privacy is generally broken down into three categories for analysis – personal, territorial, and informational. Here, only the latter is at issue. Informational privacy engages the rights of people to control when, how, and to what extent information about them is made available to other people.[35] In *Spencer*, this Court recognized that anonymity, though not a right, is a basic

---

[32] *Canadian Charter of Rights and Freedoms,* Part 1 of the *Constitution Act, 1982*, being Schedule B of the Canada Act 1982 (UK), 1982, s 8
[33] *Spencer*, *supra* note 1 at paras 16-17; *R v Mills*, 2019 SCC 22 at paras 12-13
[34] *Spencer*, *supra* note 1 at para 18; *R v Patrick*, 2009 SCC 17 at para 14
[35] *Tessling*, *supra* note 2 at paras 20-24; *Patrick*, *supra* note 34 at para 42

state of privacy, which can lead to a reasonable expectation of privacy depending on the circumstances.[36]

36. When "a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information".[37]

No link, no need for a warrant

37. *Spencer* holds that a reasonable expectation of privacy exists when the police try to link an IP address with subscriber information. The *Spencer* Court did not find that an IP address alone led to a reasonable expectation of privacy. Rather, the link between the IP address and its subscriber information was the tipping point. Justice Cromwell, writing for the unanimous Court stated, "subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating not simply to the person's name or address but to his or her identity as the source, possessor or user of that information."[38] He found the police request that the ISP disclose the subscriber information was "in effect a request to link Mr. Spencer with precise online activity that had been the subject of monitoring by the police". Thus, the request engaged a significant privacy interest.[39]

38. Because *Spencer* answers the issue raised by the appellant, it is important to recap its facts and this Court's reasoning. Mr. Spencer lived with his sister and used her internet account. He used a peer-to-peer file sharing program to download child pornography to his computer. Meanwhile, as part of an undercover operation, a police officer searched for people sharing child pornography online. The officer found people using a peer-to-peer file sharing program to download child pornography into a shared folder, making it accessible to other users. The file-sharing program displayed two numbers: the suspect users' IP addresses, and the globally unique identifier (GUID) numbers assigned to each computer using the same peer-to-peer file sharing software.[40]

---

[36] *Spencer*, *supra* note 1 at para 49
[37] *Ibid* at para 67
[38] *Ibid* at para 47
[39] *Ibid* at para 67
[40] *Ibid* at paras 7-8

39. The officer then ran the IP addresses in a database and found that one of the IP addresses was suspected to be in Saskatoon, with Shaw as the ISP. The officer made a request under the *Personal Information Protection and Electronics Document Act (PIPEDA)* to Shaw for the name, address, and phone number of the customer using that IP address at the relevant time. Shaw provided the information. Police then used that information to get a warrant to search the home of the customer – Mr. Spencer's sister. An examination of seized computers led to Mr. Spencer's arrest and conviction.[41]

40. Mr. Spencer said the police needed a warrant for his subscriber information from Shaw. Just as here, the dispute between Mr. Spencer and the prosecution turned on the subject matter of the search and whether Mr. Spencer's subjective expectation of privacy was reasonable.[42]

41. To determine the subject matter of the search, this Court considered "not only the nature of the precise information sought, but also the nature of the information that it reveals."[43] Within this framework, this Court also considered the tendency of the subject matter to support inferences about a person's private life.[44]

42. In the context of Internet usage, Justice Cromwell stated that anonymity was a "particularly important" conception of privacy. He noted "the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users" through things like browsing logs, search histories, and cookies. "The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous - by guarding the link between the information and the identity of the person to whom it relates - the user can in large measure be assured that the activity remains private".[45]

43. Justice Cromwell found that linking an IP address to its subscriber information engaged a privacy interest in the same way a sniffer dog provides information about the contents of a bag,

---

[41] *Ibid* at paras 9-13; *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5
[42] *Spencer*, *supra* note 1 at paras 14, 20
[43] *Ibid* at para 26
[44] *Ibid* at para 31
[45] *Ibid* at paras 45-46

or an electric meter reading provides information about what is occurring inside a home.[46] So the police request to link a given IP address to subscriber information was "in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities." Thus, the police request engaged "a high level of informational privacy."[47]

44. Applying the reasoning from *Spencer* to the facts here leads to the conclusion the appellant had no reasonable expectation of privacy in the IP addresses. Unlike *Spencer*, there was no link between the IP address and the appellant nor anyone else. The police could not infer anything about a specific person from the IP addresses. The appellant's anonymous online activities were not revealed to the police because they had no idea who he was. To learn who he was, they needed the subscriber information, which they obtained lawfully.

45. That there was no link between a specific person and specific online activities is the key to why the appellant had no reasonable expectation of privacy. In *Spencer,* the IP address told the police the user was interested in child pornography. Then, the subscriber information told the police where that user lived. In most cases, the subscriber information would also tell the police the name of the user, though in *Spencer* it was the accused's sister. This is unlike here. The majority of the Court of Appeal correctly observed that based on the information received from Moneris, the police only knew that "an unknown person using a known IP address was committing fraud from an unknown address."[48]

46. The trial judge and majority of the Court of Appeal correctly found that standing alone, the IP addresses were abstract numbers that revealed no private information or indeed identified anyone. To link the IP address to a person, the police got a production order as *Spencer* directs. Thus, police had lawful authorization to obtain the subscriber information - the point when the appellant's s 8 interests were engaged.

47. Justice Fairburn (as she then was) reached a finding like that of the trial judge and the majority of the Court of Appeal in *R v Nguyen*. That case concerned the reasonable expectation

---

[46] *Ibid* at para 47
[47] *Ibid* at paras 50-51
[48] *Bykovets* ABCA, *supra* note 8 at para 17 [AR Tab 1D]

of privacy in a GUID. To Justice Fairburn, *Spencer* established that an IP address standing alone does not give rise to a reasonable expectation of privacy: she used a bare IP address as a standard for the kind of data in which there is no reasonable expectation of privacy.[49]

48. Like *Spencer*, *Nguyen* related to peer-to-peer file sharing. The police used software to track and investigate peer-to-peer trading and distribution of child pornography. The software used by police logged two numbers: the IP address and GUID associated to suspected child pornography. Justice Fairburn noted that a GUID is a unique alphanumeric reference code that peer-to-peer software uses as an identifier.[50]

49. Justice Fairburn applied *Spencer* and found there was no reasonable expectation of privacy in a GUID. She likened the limited information a GUID provides to an IP address. She observed that *Spencer* resolved whether the police need a warrant to get an IP address:

> We know from *Spencer* that, standing on its own, an IP address does not trigger a reasonable expectation of privacy. It is the unveiling of otherwise anonymous Internet activity, by connecting an IP address to a name and or address that triggers s. 8 protection.[51]

50. As the trial judge did here, Justice Fairburn noted that no evidence showed a GUID revealed a person's biographical data or anonymous activity. Rather, she said, a GUID, "like a raw IP address" was just a number:

> Based on the factual record before the court, there is no evidence that a GUID provides any window into private information about an individual. There is no database that collects GUIDs and no one keeps track of them. While this long alphanumeric number, associated to the software application, facilitates the movement of files to and from the user's shared folder on the P2P [peer-to-peer] network, **like a raw IP address, it is just a number and tells the state nothing about a specific individual.**[52] [Emphasis added.]
>
> …
>
> The subject matter of the alleged search here is a long 30 plus digit number that is detached from subscriber information. **It tells us nothing about a particular individual. In this sense, it is exactly like an IP address.**[53] [Emphasis added.]

---

[49] *R v Nguyen*, 2017 ONSC 1341
[50] *Ibid* at paras 8-11
[51] *Ibid* at para 36
[52] *Ibid* at para 37
[53] *Ibid* at para 40

51. Justice Fairburn concluded that while it was possible for the police to use a GUID to learn about a person's anonymous activities, they could do so only if they matched that information to subscriber data, which, under *Spencer*, they could only get by court order. "As such, all s. 8 concerns are properly and constitutionally attended to."[54]

52. The same reasoning applies here. The trial judge and the majority of the Court of Appeal found the appellant's privacy was only intruded upon when the police matched the IP addresses to subscriber information. And because the police got the subscriber information by complying with *Spencer*, they did not breach the appellant's s 8 rights.

The subject matter cannot be reduced to the investigation's purpose

53. As was her right, the trial judge accepted Det. Laustsen's uncontradicted testimony that she wanted the IP addresses to further her investigation by first, running an open-source search to find out which ISP assigned the IP addresses, and second, by serving the ISP with a production order for the subscriber information.[55]

54. The dissenting justice's reasoning framed the subject matter circularly. In her view, when the police asked Moneris for the IP addresses, they really asked for "the identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity." In other words, the dissenting justice's description of the subject matter is simply a description of the police investigation's overall purpose. Critical to the dissenting justice's analysis was that obtaining the IP addresses helped the police investigation:

> By identifying the five specific transactions of interest and seeking from a third-party, without prior judicial authorization, the IP addresses used for those specific transactions, the CPS obtained information to further the investigation as to the identity of the user.[56]

55. Naturally, the police's goal was to identify the user. But the dissenting justice ignored that to do this, the police had to take an intervening step – they had to lawfully get a production order for the subscriber information.

---

[54] *Ibid* at para 45
[55] *Bykovets* ABQB, *supra* note 3 at para 44 [AR Tab 1C]
[56] *Bykovets* ABCA, *supra* note 8 at para 76 [AR Tab 1D]

The totality of circumstances should not include speculation

56. The trial judge rightly refused to accept the appellant's claim that the subject matter of the search was the identity of the person who used the IP addresses. The appellant based this argument on conjectures. These conjectures related to Mr. Musters' evidence that a third party like Google or Facebook could "attempt" to identify a user on their website by tracking that user's activity across the internet and that the police could then access that data. But neither Mr. Musters nor anyone else gave evidence that third parties tried to find users' identities this way, or whether such efforts succeeded.[57] Moreover, even if this data existed, nothing in the record suggested that police could access it – and not without judicial authorization. The appellant did not even ask Det. Laustsen if she knew some way to get such hypothetical data. Properly, the trial judge rejected the appellant's conjecture.

57. The trial judge's refusal to speculate fits with *Spencer*. Justice Cromwell did not engage in speculative reasoning. He noted the IP address told the police the user was interested in child pornography. The subscriber information then told the police the address of that user and in most cases would also provide the user's name. Thus, to Justice Cromwell, it was "straightforward" that the police request to link a given IP address to subscriber information was a request to link a specific person to specific online activities.[58] Speculative reasoning played no part in his straightforward finding.

Future predictions do not establish a breach of s 8

58. Proven facts should govern the s 8 analysis, not what might be possible in the future. The dissenting justice erred when she considered possible and unspecified "technological advances" that might permit future police to piece together "breadcrumbs" to intrude on a person's privacy.

59. The dissenting justice's approach contradicts the approach endorsed by this Court. The "totality of circumstances" means the privacy interest is determined by considering the facts as a whole.[59] But it does not mean a court should determine the privacy interest based on a prediction of the future. So as noted in *Spencer*, in *R v Tessling*, this Court found no reasonable expectation

---

[57] *Bykovets* ABQB, *supra* note 3 at paras 15, 41, 63 [AR Tab 1C]
[58] *Spencer*, *supra* note 1 at para 50
[59] *Spencer*, *supra* note 1 at para 17

of privacy in Forward Looking Infra-Red (FLIR) imaging of heat emanations from a house because "the heat emanations were, on their own, meaningless because they did not permit any inferences about the precise activity giving rise to the heat".[60] But had the technology in *Tessling* been different, this Court's ruling might have been different.

60. In *Tessling*, this Court based its s 8 analysis on "the quality of information that the FLIR imaging can actually deliver", not its "theoretical capacity".[61] Justice Binnie, writing for the unanimous Court, rejected reasoning that finds a reasonable expectation of privacy based on a prediction that the technology involved is "almost Orwellian in its theoretical capacity". Rather, he said the "technology must be evaluated according to its *present* capability. Whatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed as they truly arise." [62]

61. After *Tessling*, this Court again rejected the futurist approach in *R v Gomboc*, which dealt with the information provided by a digital meter that recorded a household's electricity use. Writing for herself and three others (including Justice Cromwell), Justice Deschamps found the analysis had to consider the technology as it was, not as it might be. She left the privacy implications of more evolved technology to be decided when it was a reality:

> We are cautioned by the intervener the CCLA about the looming prospect of smart meters being deployed across the country and the possibility of data they record revealing how electricity is being used in homes.… The CCLA's submissions about smart meters raise concerns about theoretical capabilities and potential future uses of technology rather than realistic privacy concerns applicable in the present case.[63]

62. As *Tessling* and *Gomboc* show, the dissenting justice erred by considering future technological possibilities.

The totality of circumstances cannot presume bad faith

63. The police acted lawfully, and this Court should reject any argument that presumes otherwise. Even under the appellant's speculative argument in which third-party companies

---

[60] *Spencer*, *supra* note 1 at para 28, citing *Tessling*, *supra* note 2 at paras 35-36
[61] *Tessling*, *supra* note 2 at paras 28-29
[62] *Ibid* at paras 34-36, 55 (Emphasis in original.)
[63] *Gomboc*, *supra* note 2 at para 40

successfully learn the identity of users of their websites by tracking those users' IP address activity across the internet, and the police discover this is happening and what third parties are doing it, the police would still need to lawfully comply with *Spencer* to get the data. The appellant argues that if this decision stands, nothing stops the police from engaging in "mass data collection" and "building an IP Address equivalent of a facial recognition database for internet activity."[64] But one thing *would* stop the police from this Orwellian vision: *Spencer* would require they get judicial authorization to do this lawfully, since such a hypothetical database would pierce a person's online anonymity.

64. Thus, the appellant's argument assumes the police would simply ignore *Spencer*. Not only is this argument not grounded in the facts, but it unfairly presumes the police would act in bad faith. Bad faith is a factual issue, decided by a trial judge on the evidence, and considered under a s 24(2) analysis.[65] The trial judge correctly refused to be drawn into reasoning that presumed illegal conduct:

> I question why an investigator would do that [i.e., gain access to a third-party website] when they are able to access a public resource listing IP addresses to identify an ISP. The investigator can then seek judicial authorization before obtaining specific subscriber information from that ISP.[66] [Parenthesis added.]

65. The appellant's reliance on speculative possibilities does not end with a presumption of bad faith. He then says that if the police have an IP address in hand, and then the user of that IP address logs onto a social media site like Facebook, LinkedIn, or Twitter, then "Police now have an IP address connected to a name, geographical area, professional skillset and a myriad of other information."[67] Nothing in the record supports this or the appellant's conclusory statement that "Obtaining the identity of the user in such a circumstance is a one-step process". Mr. Musters' evidence depended on a series of steps and assumptions, not a one-step process.

---

[64] Appellant's Factum at paras 42-47
[65] *R v Le*, 2019 SCC 34 at para 146
[66] *Bykovets* ABQB, *supra* note 3 at para 63 [AR Tab 1C]
[67] Appellant's Factum at para 59

No objectively reasonable expectation of privacy

66. Based on the *Marakah* factors, the trial judge found the appellant had no objectively reasonable expectation of privacy. The dissenting justice substituted her own opinion and disagreed with each of the trial judge's findings by engaging in results oriented reasoning. Her analysis of the *Marakah* factors amounted to simply finding the appellant had an objectively reasonable expectation, because, in her view, the subject matter of the police request was the identity of a person matched to their online habits.[68] On the other hand, the trial judge applied a fact based analysis. She found the place of the search was Moneris' logbooks since the police got the IP addresses by asking Moneris to check their logs. She found the private nature of the subject matter was minimal since an IP address alone reveals no core biographical information. She found the appellant had no control over the subject matter since the IP addresses were assigned by Telus. The trial judge's *Marakah* analysis reveals no palpable and overriding error.

67. Another factor weighs against the appellant having an objectively reasonable expectation of privacy - no contractual or statutory relationship exists between the appellant and Moneris. In *Spencer*, this Court stated that though the contractual and statutory framework was not determinative, it was relevant. There, the ISP's collection, use, and disclosure of the personal information of its subscribers was subject to *PIPEDA*, which prevents personal information held by organizations engaged in commercial activities from being disclosed without the knowledge or consent of the person to whom the information relates.[69]

68. Justice Cromwell noted the confusing and circular interplay between (a) the contract between the ISP and the subscriber, and (b) *PIPEDA*, which permitted the ISP to give the police subscriber information only if the police had "lawful authority". In Justice Cromwell's analysis, the contractual and statutory framework "narrowly circumscribes Shaw's right to disclose the personal information of subscribers." Justice Cromwell found the police had no lawful authority to request subscriber information since they lacked a warrant, and so he found the framework supported the reasonableness of Mr. Spencer's expectation of privacy.[70] Here, there is no

---

[68] *Bykovets* ABCA, *supra* note 8 at paras 83-93 [AR Tab 1D]
[69] *Spencer*, *supra* note 1 at paras 54, 61
[70] *Spencer*, *supra* note 1 at paras 55-65

evidence of any contract between the appellant and Moneris.[71] Nor does the appellant point to *PIPEDA* or any other legislation as stopping Moneris from providing the IP addresses to the police.[72]

69. Yet there is legislation that supports Moneris providing the IP addresses to the police. As Justice Cromwell noted in *Spencer*, s 487.014(1) of the *Criminal Code* provided that a peace officer did not need judicial authorization "to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing." This section has since been replaced by s 487.0195(1), which states that a production order is unnecessary for a person "to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing."[73] Here, no law prohibited Moneris from providing the IP addresses to the police. Thus s 487.0195(1), along with the common law power of police officers to make inquiries, weighs against finding the appellant had an objectively reasonable expectation of privacy in the IP addresses.

Conclusion: the police did not need a warrant

70. When the police asked for and received from Moneris the IP addresses associated to fraudulent transactions, it did not identify a specific user with specific online activities. To make that link, the police complied with *Spencer* and got a production order. Thus, the police did not intrude on the appellant's privacy by receiving the IP addresses from Moneris.

71. The trial judge rooted her analysis in proven facts, not speculation and predictions about future possibilities. Because this case might have broad implications, this Court should endorse her approach.

PART IV – COSTS

72. The respondent asks that no party be awarded costs.

---

[71] *Bykovets* ABQB, *supra* note 3 at para 60 [AR Tab 1C]
[72] *Spencer*, *supra* note 1 at paras 54-57, 65
[73] *Criminal Code*, RSC 1985, c C-46, s 487.0195; "document" defined in s 487.011 as "a medium on which data is registered or marked".

PART V – ORDER SOUGHT

73. The respondent asks this Court to dismiss the appeal.

PART VI – SUBMISSIONS ON CASE SENSITIVITY

74. There are no restrictions in Rule 42(2)(f) of the *Rules of the Supreme Court of Canada* that affect this Court's reasons.

All of which is respectfully submitted, October 14, 2022.

Rajbir Dhillon
Counsel for the respondent

RD/lc

PART VII – TABLE OF AUTHORITIES AND LEGISLATION

Authorities	**Cited at Paragraph No.**
R v Bykovets, 2020 ABQB 70 at paras 5-10, 15-17, 35-48, 52-65	5, 6, 7, 8, 9, 11, 12, 14, 16, 17, 18, 19, 20, 21, 53, 56, 64, 68
R v Bykovets, 2022 ABCA 208 at paras 3-6, 13, 17-21, 22-26, 31-37, 55, 69-70, 73, 76-77, 83-93	10, 12, 23, 24, 25, 26, 27, 28, 29, 45, 54, 56, 66
R v Gomboc, 2010 SCC 55 at para 40	2, 61, 62
R v Jennings, 2018 ABQB 296	15
R v Le, 2019 SCC 34 at para 146	64
R v Marakah, 2017 SCC 59 at para 24	19, 20, 66
R v Mills, 2019 SCC 22 at paras 12-13	33
R v Nguyen, 2017 ONSC 1341 at paras 8-11, 36-37, 40, 45	47, 48, 49, 50, 51
R v Patrick, 2009 SCC 17 at paras 14, 42	34, 35
R v Spencer, 2014 SCC 43 at paras 7-14, 16-18, 20, 26, 28, 31, 33, 42, 45-47, 49-51, 54-65, 67	1, 2, 3, 13, 21, 23, 27, 29, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 57, 59, 63, 64, 67, 68, 69, 70
R v Tessling, 2004 SCC 67 at paras 20-24, 28-29, 34-36, 55	4, 35, 59, 60, 61, 62
X (Re), 2017 FC 1047	15
Legislation	**Cited at Paragraph No.**
Canadian Charter of Rights and Freedoms, Part 1 of the *Constitution Act, 1982*, being Schedule B of the Canada Act 1982 (UK), 1982, s 8	2, 3, 10, 11, 21, 32, 33, 46, 49, 51, 52, 58, 60

Charte Canadienne des droits et Libertés, Part 1 de la *Loi Constitutionnelle De*, 1982, s 8	
Canadian Charter of Rights and Freedoms, Part 1 of the *Constitution Act, 1982*, being Schedule B of the Canada Act 1982 (UK), 1982, s 10(b) *Charte Canadienne des droits et Libertés*, Part 1 de la *Loi Constitutionnelle De, 1982*, s 10(b)	10
Canadian Charter of Rights and Freedoms, Part 1 of the *Constitution Act, 1982*, being Schedule B of the Canada Act 1982 (UK), 1982, s 24(2) *Charte Canadienne des droits et Libertés*, Part 1 de la *Loi Constitutionnelle De, 1982*, s 24(2)	10, 64
Criminal Code, RSC 1985, c C-46, s 56.1 *Code criminal*, LRC (1985), ch C-46, s 56.1	22
Criminal Code, RSC 1985, c C-46, s 342(1)(c) *Code criminal*, LRC (1985), ch C-46, s 342(1)(c)	22
Criminal Code, RSC 1985, c C-46, s 342.01(1)(b) *Code criminal*, LRC (1985), ch C-46, s 342.01(1)(b)	22
Criminal Code, RSC 1985, c C-46, s 342(3) *Code criminal*, LRC (1985), ch C-46, s 342(3)	5, 22
Criminal Code, RSC 1985, c C-46, s 462.31 *Code criminal*, LRC (1985), ch C-46, s 462.31	22
Criminal Code, RSC 1985, c C-46, s 487.0195(1) *Code criminal*, LRC (1985), ch C-46, s 487.0195(1)	69
Criminal Code, RSC 1985, c C-46, s 487.014(1) *Code criminal*, LRC (1985), ch C-46, s 487.014(1)	69
Criminal Code, RSC 1985, c C-46, s 487.011 *Code criminal*, LRC (1985), ch C-46, s 487.011	69
Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5 Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5	39, 67, 68