SCC File No.: 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*)

-and-

DIRECTOR OF PUBLIC PROSECUTIONS
CANADIAN CIVIL LIBERTIES ASSOCIATION,
ATTORNEY GENERAL OF BRITISH COLUMBIA,
ATTORNEY GENERAL OF ONTARIO
BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

INTERVENERS

FACTUM OF THE INTERVENER, ATTORNEY GENERAL OF ONTARIO

(Pursuant to r. 37 of the *Rules of Supreme Court of Canada*)

Ministry of the Attorney General of Ontario
Crown Law Office – Criminal
720 Bay Street, 10th Floor
Toronto Ontario

Jeremy Streeter
Andrew Hotke

Tel: (416) 326-4600
Fax: (416) 326-4656
Email: jeremy.streeter@ontario.ca
andrew.hotke@ontario.ca

Counsel for the Intervener,
Attorney General of Ontario

Sarah Rankin
Ian Mckay
Heather Ferg
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

Counsel for the Appellant,
Andrei Bykovets

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

Agent for the Appellant,
Andrei Bykovets

Rajbir Dhillon
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

Counsel for the Respondent

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

Agent for the Respondent

David W. Schermbrucker
Allyson Ratsoy
Public Prosecution Service of Canada
Suite 1400, Duke Tower
5251 Duke Street
Halifax, Nova Scotia
B3J 1P3
Telephone: (902) 426-2285
FAX: (902) 426-1351
Email: David.Schermbrucker@ppsc-sppc.gc.ca

Counsel for the Intervener,
Public Prosecution Service of Canada

François Lacasse
Director of Public Prosecutions of Canada
160 Elgin Street
12th Floor
Ottawa, Ontario
K1A 0H8
Telephone: (613) 957-4770
FAX: (613) 941-7865
Email: francois.lacasse@ppsc-sppc.gc.ca

Agent for the Intervener,
Public Prosecution Service of Canada

Anil K. Kapoor
Cameron Cotton O'Brien
Kapoor Barristers
161 Bay Street
Suite 2900
Toronto, Ontario
M5J 2S1
Telephone: (416) 363-2700
FAX: (416) 363-2787
Email: akk@kapoorbarristers.com

Counsel for the Intervener,
Canadian Civil Liberties Association

Marie-France Major
Supreme Advocacy LLP
100- 340 Gilmour Street
Ottawa, Ontario
K2P 0R3
Telephone: (613) 695-8855 Ext: 102
FAX: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Agent for the Intervener,
Canadian Civil Liberties Association

Micah B. Rankin
Michael Barrenger
Attorney General of British Columbia
Criminal Appeals and Special Prosecutions
3rd Floor, 940 Blanshard Street
Victoria, British Columbia
V8W 3E6
Telephone: (778) 974-3344
Fax: (250) 387-4262
Email: micah.rankin@gov.bc.ca

Counsel for the Intervener,
Attorney General of British Columbia

Matthew Estabrook
Gowling WLG (Canada) LLP
2600 - 160 Elgin Street
Ottawa (Ontario) K1P 1C3
Téléphone : 613 786-0211
Télécopieur : 613 788-3573
matthew.estabrooks@gowlingwlg.com

Agent for the Intervener,
Attorney General of British Columbia

Daniel J. Song, KC
Stephen Chin
Pringle Chivers Sparks Teskey
1720 - 355 Burrard Street
Vancouver, British Columbia
V6C 2G8
Telephone: (604) 669-7447
FAX: (604) 259-6171
Email: djsong@pringlelaw.ca

Counsel for the Intervener,
British Columbia Civil Liberties Association

Table of Contents

PART I: OVERVIEW AND STATEMENT OF FACTS

[1] The important legal question raised on this appeal is whether a reasonable expectation of privacy exists in an IP address used by an unknown internet user to engage in particular online activity. If the answer is yes, law enforcement in Canada will not be able to receive, access or seek out IP addresses of unknown internet users to investigate crime unless they have legal authority.

[2] The Attorney General for Ontario has intervened to urge the Court to say the answer is no: the IP address of an unknown internet user does not engage a reasonable expectation of privacy. This is the state of the law after *R. v. Spencer*, 2014 SCC 43, as explained in *R. v. Nguyen*, 2017 ONSC 1341, by Fairburn J., as she then was.[1]

[3] In reaching the opposite conclusion, the dissenting Justice of the Alberta Court of Appeal focused on the fact that the investigating police who requested and received two IP addresses of then unknown internet users were ultimately after the identity of the users.

[4] It is undeniable that this Court has said that courts should focus on "what the police were really after" when assessing whether electronic data obtained by police engages a reasonable expectation of privacy.[2] But this does not mean the assessment turns on what the police were *ultimately* after in their investigation.

[5] Police investigating online crime will almost invariably be after the identities of persons who have committed crimes at each stage of the investigation. It cannot be that any piece of evidence police obtain that furthers an investigation into the identity of an unknown suspect

---

[1] *Nguyen*, at para. 36. See also *R. v. El-Halfawi*, 2021 ONCJ 462, at paras. 82-83
[2] *R. v. Marakah*, 2017 SCC 59, at para. 15; *R. v. Reeves*, 2018 SCC 56, at para. 29

engages a reasonable expectation of privacy. Instead, focusing on "what the police were really after" means that for electronic data courts cannot treat the subject matter of an alleged search as the physical acts of the police, or the physical spaces intruded upon in obtaining the data.[3] The subject matter of the alleged search must include the information the particular data can reveal, on its face and through "immediate and direct" inferences that arise from the data itself or in combination with other available non-private information.[4]

[6] Ontario agrees with the respondent that an IP address reveals nothing that can reasonably be expected to be private. An IP address of an unknown internet user does not link a specific individual to specific online activity.[5] Subscriber information can provide such a link. This reality compelled this Court in *Spencer* to hold that subscriber information can engage a reasonable expectation of privacy. Extending *Spencer* to IP addresses is not necessary to advance the privacy interests *Spencer* now protects. Moreover, extending *Spencer* to IP addresses will unduly hamper the ability of law enforcement to protect Canadians against online crime.

[7] Ontario takes no position on the facts of the case.

PART II: POINTS IN ISSUE

[8] Ontario advances two points on this appeal:

A. This Court should not adopt the dissenting Justice's approach to the reasonable expectation of privacy analysis for electronic data. The dissenting Justice focused on the ultimate goal of the police investigation, rather than what an IP address can reveal.

B. This Court should give consideration to the consequences of the dissenting Justice's conclusion for effective criminal law enforcement for online crime.

---

[3] *Marakah*, at para. 15; *Reeves*, at para. 29
[4] *R. v. Kang-Brown*, 2008 SCC 18, at para. 175
[5] A reality animating issues considered recently by this Court in *Rogers Communications Inc. v. Voltage Pictures, LLC*, 2018 SCC 38

PART III: STATEMENT OF ARGUMENT

A. The subject matter of an alleged search involving electronic data should be characterized by reference to what the data can reveal, not what the police are ultimately after

[9] In *R. v. Marakah*, 2017 SCC 59, Chief Justice McLachlin emphasized that the subject matter of an alleged search involving electronic data must be defined with care and precision at the first step of the reasonable expectation of privacy analysis.[6] The focus cannot be merely on the physical space intruded upon by police when they obtained the data, or the physical acts of police in obtaining the data. Rather, focus must be placed on the information the data reveals and gives access to through immediate and direct inferences.[7]

[10] It was in this context that the Chief Justice endorsed the language of Doherty J.A. in *R. v. Ward*, 2012 ONCA 660, where, in determining the proper characterization of the subject matter of a search of internet subscriber information, Doherty J.A. rejected a characterization that did not capture "what the police were really after".[8] This phrase was not meant to imply that the subject matter of an alleged search is equal to *what the police investigation is ultimately after*. Doherty J.A. was simply identifying a fact that helped show that the characterization he was rejecting was too narrow; it did not capture the information the police really wanted and could potentially glean from the data in question.[9]

---

[6] *Marakah*, at paras. 14, 16
[7] *R. v. Cole*, 2012 SCC 53, at para. 34; *Marakah*, at para. 10; *Kang-Brown*, at para. 175; *Spencer*, at para. 31
[8] *Ward*, at paras. 66-67
[9] See *R. v. Dosanjh*, 2022 ONCA 689, at paras. 115-116

[11] Because "what the police are really after" can help identify the information particular electronic data is capable of giving access to, Justice Karakatsanis in *R. v. Reeves,* 2018 SCC 56, identified it as a guiding question for defining the subject matter of an alleged search.[10]

[12] In her analysis of the subject matter of the alleged search, the dissenting Justice of the Alberta Court of Appeal focused on what the police investigation was ultimately after. She focused on the fact that the police were ultimately after "the identity of an internet user" connected to particular internet activity, and she reasoned that because the IP addresses were sought to "further the investigation" into the identity of an internet user, the subject matter of the alleged search (i.e., the subject matter of IP addresses) should be defined as just that: the identity of an unknown internet user.[11]

[13] Ontario urges this Court not to adopt this way of reasoning. The focus for courts tasked with defining the subject matter of an alleged search involving electronic data should be the information directly revealed by the data; standing alone, and in combination with other non-private data available to law enforcement.[12] The analysis should not focus on the ultimate goal of the police investigation for which the data was obtained. To do so invites a flawed reasonable expectation of privacy analysis, by inviting consideration of privacy implications that are not actually engaged by the data in question. And in the context of investigations into online crime, where the identity of an unknown person who engaged in online activity is almost invariably the ultimate goal of any investigation, such an approach could make nearly any investigative step a search for the purposes of s. 8.

---

[10] *Reeves,* at para. 29
[11] *R. v. Bykovets,* 2022 ABCA 208, at paras. 76-77
[12] *Marakah,* at para. 15; *Spencer,* at paras. 25-31; *R. v. Trapp,* 2011 SKCA 143, at para. 37

[14] Examples help to illustrate the point. Consider an instance where police use publicly available resources to ascertain the Internet Service Provider who issued an IP address used by an unknown internet user. This happened in the case at bar: see *R. v. Bykovets*, 2022 ABCA 208, at para. 9.[13] Clearly, this investigative step can further an investigation into the identity of an unknown internet user connected to particular internet activity. But it would be wrong to say that because the police had as their ultimate goal the discovery of the identity of the user, the subject matter engaged by police obtaining the Internet Service Provider information is the identity of the unknown user. That would only be true if knowledge of the Internet Service Provider, standing alone or combined with other non-private information, could reveal the user's identity to police.[14]

[15] As a second example, consider an instance where police have a username used by an unknown internet user connected to particular online activity. Publicly available internet searches for platforms or services with an account operating under the same username could reveal information capable of furthering an investigation into the identity of the internet user operating under the username.[15] But again, it would be wrong to say that, because the police had as their ultimate goal the discovery of the identity of the user and they uncovered information that furthered that goal, the subject matter of their conduct is the identity of the user.

[16] For these reasons, Ontario urges the Court to affirm the direction of the Chief Justice in *Marakah* regarding the proper way to characterize the subject matter of an alleged search involving

---

[13] See also *Nguyen*, at para. 10; *Rochefort c. R.*, 2022 QCCS 3100, at para. 23

[14] A similar argument could be made about using an IP address to determine an unknown internet user's general geographic location. See *Nguyen*, at para. 10: "Publicly available, online databases allow IP addresses to be geographically located".

[15] See, for example, *R. v. Jonat*, 2019 ONSC 415, at paras. 5-7

electronic data. The focus has to be on the information the data can reveal, standing alone and in combination with other available non-private information, using direct and immediate inferences.

B. The dissenting Justice's conclusion would have negative consequences for effective law enforcement against online crime

[17] Since *Hunter v. Southam Inc.*, [1984] 2 SCR 145, this Court has emphasized that interpreting s. 8 of the *Charter* requires a balancing of societal interests.[16] Society's interest in privacy and being left alone by the state must be balanced against "legitimate countervailing concerns" of "safety, security and the suppression of crime".[17]

[18] This balancing is not limited to assessments of the reasonableness or proper scope of laws permitting intrusions into spheres that have been recognized as engaging a reasonable expectation of privacy.[18] It also applies to determinations of whether a reasonable expectation of privacy should be said to exist at all. This is because the question of whether a reasonable expectation of privacy exists is a normative one. It turns on what is reasonable and what Canadians *ought* to expect, given the relevant considerations, including the legitimate needs of law enforcement.[19] As Watt J.A. said in *R. v. Atkinson*, 2012 ONCA 380:

> The right to be secure from unreasonable search or seizure protects only a "reasonable expectation of privacy". The limiting term "reasonable" implies that, in each case, the court must assess whether, in the circumstances, the public's interest in being left alone by the state must give way to the state's interest in intruding on the individual's privacy to advance its goals, such as law enforcement: *R. v. Edwards* (1996), 1996 CanLII 255 (SCC), 26 O.R. (3d) 736, [1996] 1 S.C.R. 128, [1996] S.C.J. No. 11, at para. 30; *Hunter v. Southam Inc.*, 1984 CanLII 33 (SCC), [1984] 2 S.C.R. 145, [1984] S.C.J. No. 36, at pp. 159-60

---

[16] See *R. v. Dyment*, [1988] 2 SCR 417, at para. 18; *R. v. Edwards*, [1996] 1 SCR 128, at para. 30; *R. v. Patrick*, 2009 SCC 17, at para. 20; *R. v. Vu*, 2013 SCC 60, at para. 21; *R. v. Mills*, 2019 SCC 22, at para. 59. See also *Trapp*, at para. 92; *R. v. Felger*, 2014 BCCA 34, leave ref'd [2014] S.C.C.A. No. 120, at para. 50

[17] *R. v. Tessling*, 2004 SCC 67, at para. 17

[18] See *Edwards*, at para. 30; *Marakah*, at paras. 89, 179, 187-188; *Reeves*, at para. 113

[19] See *Mills*, at para. 20

> S.C.R. The assessment must take into account all the circumstances of the case: *Edwards*, at paras. 31 and 45.[20]

[19] Ontario submits that the Court should give consideration to the impact the dissenting Justice's decision would have for law enforcement if it were accepted. In Ontario's respectful submission, recognizing a reasonable expectation of privacy in the IP address of an unknown internet user would have significant implications for effective law enforcement for online crime in Canada, without a corresponding benefit to the legitimate privacy interests of Canadians.[21]

[20] Recognizing a reasonable expectation of privacy in the IP address of an unknown internet user could undermine the ability of law enforcement to investigate online sharing of child pornography. In the expert report filed at trial, the expert referred to peer-to-peer file sharing software. On such platforms, the IP addresses of participants are "broadcast to all others using the same software to facilitate file sharing".[22] *Spencer*, as well as *Nguyen,* dealt with instances of child pornography being shared on peer-to-peer file sharing platforms. One need not look far to find other examples in the case law.[23]

[21] If a reasonable expectation of privacy is said to exist in an IP address of an unknown internet user, police will need common law authority or judicial authorization before they can scan peer-to-peer file sharing programs to look for IP addresses of users sharing child pornography. But what lawful authority can be relied on to carry out such investigative action, where the police operate with general knowledge that peer-to-peer file sharing is used to share child pornography,

---

[20] See also *Mills*, at paras. 20 and 80
[21] See *R. v. July*, 2020 ONCA 492, at para. 70
[22] *R. v. Bykovets*, 2020 ABQB 70, at para. 13
[23] Examples from decisions of this year: *R. v. Scopel-Cessel*, 2022 ONCA 316 (see paras. 2-5); *R. v. Zahor*, 2022 ONCA 449 (see paras. 14-15); *R. v. Reid*, 2022 ONSC 2987 (see para. 5); *R. v. Crump*, 2022 ONCJ 510 (see paras. 7-8); *R. v. Mains*, 2022 ONCJ 44 (see paras. 20-26)

but without grounds pertaining to any particular target or particular offence?[24] The law does not provide any clear route. A search warrant requires reasonable and probable grounds to believe that an offence has been committed and that the search of a specified place will afford evidence of that offence.[25] A general warrant – in addition to other requirements – requires reasonable grounds to believe that an offence has been committed and that "information concerning the offence will be obtained by use of the warrant.[26] A production order for transmission data requires a third party target, and reasonable suspicion that the third party has possession or control of data that will assist in the investigation of a suspected offence.[27]

[22] Furthermore, if prior judicial authorization is required before police can receive, access or seek out IP addresses of unknown internet users, that will consume law enforcement and court resources and delay investigations. Preparing applications for search warrants and production orders takes time.[28] And further delays can be predicted for the trial stage, where accused persons will be able to challenge applications and resulting authorizations.[29] These practical consequences are necessary where, as with subscriber information, there are privacy interests to be protected that justify them. But this is not true of IP addresses. IP addresses reveal nothing private – not without access to subscriber information that *Spencer* already protects.

[23] Recognizing a reasonable expectation of privacy in the IP address of an unknown internet user could also call into question the validity of *An Act Respecting the Mandatory Reporting of*

---

[24] See *Spencer,* at paras. 8-9
[25] See *R. v. Morelli*, 2010 SCC 8, at paras. 39-40
[26] See *R. v. Brown*, 2021 ONCA 540, at para. 31
[27] See Magotiaux, Susan. "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015), 71 S.C.L.R. (2d) 501, at n. 52
[28] See *Marakah,* at para. 185
[29] See *Marakah*, at para. 186

Internet Child Pornography by Persons Who Provide an Internet Service, S.C. 2011, c. 4. This Act imposes reporting duties on persons who provide internet services. In conjunction with the *Internet Child Pornography Reporting Regulations*, SOR/2011-292, section 2 of the Act requires service providers to report any IP addresses that may be making child pornography available to the Canadian Centre for Child Protection (the "Centre"). The Centre, under s. 4 of the Regulations, is required to investigate reports made by service providers under the Act.[30] If the investigation determines that "any material found at the reported Internet address" appears to constitute child pornography, the Centre must "make available to every appropriate Canadian law enforcement agency": (i) the reported IP address[31], (ii) the geographic location of the server associated with the IP address, and (iii) "any other information" the Centre possesses that might assist an investigation.[32]

[24] If there is no reasonable expectation of privacy in an IP address, the receipt of an IP address by police under the scheme described above is not a search or seizure for the purpose of s. 8. Conversely, if an IP address engages a reasonable expectation of privacy, the scheme is subject to the requirements of s. 8, which means the scheme must afford reasonable privacy protection to IP addresses.[33] Again, striking a balance between privacy and the needs of law enforcement is a justifiable and unobjectionable requirement where there are legitimate privacy interests to protect. But IP addresses do not engage them. They cannot reveal anything private without the tools to link online activity to a person – and that link is already protected by *Spencer*.

---

[30] See Cybertip.ca, "Mandatory Reporting" ("www.cybertip.ca/en/about/mandatory-reporting")
[31] The Regulations refer to an "Internet address" which is defined in s. 1 to mean "an Internet Protocol address or Uniform Resource Locator".
[32] Per Regulations s. 4(b)
[33] *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46, at paras. 55-57

C. Conclusion

[25] In *Spencer,* this Court recognized a reasonable expectation of privacy in internet subscriber information associated to an IP address. It did so in light of the reality that subscriber information can link a particular individual to particular online activity associated with an IP address, thereby revealing information in respect of which there can be a "high level" of informational privacy.[34]

[26] *Spencer* achieved a fine balance between privacy interests in online activity and the ability of law enforcement to take steps to investigate online crime. Police can look for and gather evidence of online crime related to unknown internet users, including IP addresses, without first seeking judicial authorization, up to the point where they will take the step of obtaining subscriber info to link an individual to anonymous online activity. At that point, *Spencer* requires police to demonstrate grounds before the privacy interests inherent in anonymous online activity are obliged to yield to those of law enforcement.

[27] Extending *Spencer* to IP addresses does not advance the privacy interests *Spencer* now protects and will upset the fine balance *Spencer* has achieved.

PART IV: SUBMISSIONS CONCERNING COSTS

[28] Ontario makes no submissions as to costs.

Jeremy Streeter
Counsel for the Intervener
Attorney General of Ontario

Andrew Hotke
Counsel for the Intervener
Attorney General of Ontario

DATED at Toronto this 20th day of December, 2022

[34] *Spencer,* at para. 51

PART VII: TABLE OF AUTHORITIES

Cases:	Paragraphs:
Hunter v. Southam Inc., [1984] 2 SCR 145	17
Goodwin v. British Columbia (Superintendent of Motor Vehicles), 2015 SCC 46	24
Rochefort c. R., 2022 QCCS 3100	14
Rogers Communications Inc. v. Voltage Pictures, LLC, 2018 SCC 38	6
R. v. Atkinson, 2012 ONCA 380	18
R. v. Brown, 2021 ONCA 540	21
R. v. Cole, 2012 SCC 53	9
R. v. Crump, 2022 ONCJ 510	20
R. v. Dosanjh, 2022 ONCA 689	10
R. v. Dyment, [1988] 2 SCR 417	17
R. v. Edwards, [1996] 1 SCR 128	17, 18
R. v. El-Halfawi, 2021 ONCJ 462	2
R. v. Felger, 2014 BCCA 34	17
R. v. Jonat, 2019 ONSC 415	15
R. v. July, 2020 ONCA 492	19
R. v. Kang-Brown, 2008 SCC 18	5, 9
R. v. Mains, 2022 ONCJ 44	20
R. v. Marakah, 2017 SCC 59	4, 5, 9, 13, 16, 22
R. v. Mills, 2019 SCC 22	18
R. v. Morelli, 2010 SCC 8	21
R. v. Nguyen, 2017 ONSC 1341	2, 14, 20
R. v. Patrick, 2009 SCC 17	17
R. v. Reeves, 2018 SCC 56	4, 5, 11, 18
R. v. Reid, 2022 ONSC 2987	20
R. v. Scopel-Cessel, 2022 ONCA 316	20
R. v. Spencer, 2014 SCC 43	2, 9, 13, 21, 25, 26
R. v. Tessling, 2004 SCC 67	17
R. v. Trapp, 2011 SKCA 143	13, 17
R. v. Vu, 2013 SCC 60	17
R. v. Ward, 2012 ONCA 660	10
R. v. Zahor, 2022 ONCA 449	20

Secondary sources:	**Paragraphs:**
Magotiaux, Susan. "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015), 71 S.C.L.R. (2d) 501	21

Statutory Provisions and Regulations	**Paragraphs:**
An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons Who Provide an Internet Service, S.C. 2011, c. 4	23
Internet Child Pornography Reporting Regulations, SOR/2011-292	23