SCC File No.: 40269

IN THE SUPREME COURT OF CANADA
(ON THE 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,
ATTORNEY GENERAL OF ONTARIO,
ATTORNEY GENERAL OF BRITISH COLUMBIA,
CANADIAN CIVIL LIBERTIES ASSOCIATION,
BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

INTERVENERS

FACTUM OF THE INTERVENER, ATTORNEY GENERAL OF BRITISH COLUMBIA

(Pursuant to Rules 37 and 42 of the *Rules of Supreme Court of Canada*)

Micah B. Rankin
Michael Barrenger
Attorney General of British Columbia
Criminal Appeals and Special Prosecutions
3rd Floor, 940 Blanshard Street
Victoria, BC 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 Estabrooks
Gowling WLG (Canada) LLP
2600 - 160 Elgin Street
Ottawa, ON K1P 1C3
Telephone: (613) 786-0211
Fax: (613) 788-3573
Email: matthew.estabrooks@gowlingwlg.com

Agent for the Intervener,
Attorney General of British Columbia

Sarah Rankin
Ian Mckay
Heather Ferg
McKay Ferg LLP
1800, 639 – 6 Avenue S.W.
Calgary, AB T2P 0M9
Telephone: (403) 984-1919
Fax: (403) 1-844-895-3926
Email: sarah@mckaycriminaldefence.com

Counsel for the Appellant, Andrei Bykovets

Jonathan Lazer
Power Law
Suite 701, 99 Bank Street
Ottawa, ON K1P 6B9
Telephone/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
Gowling WLG (Canada) LLP
2600, 160 Elgin Street
Ottawa, ON K1P 1C3
Telephone: (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, NS 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, ON 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

Jeremy Streeter
Andrew Hotke
Attorney General of Ontario
720 Bay Street, 10th Floor
Toronto, ON M7A 2S9
Telephone: (416) 327-5990
Fax: (416) 326-4656
Email: jeremy.streeter@ontario.ca

Counsel for the Intervener,
Attorney General of Ontario

Anil K. Kapoor
Cameron Cotton O'Brien
Kapoor Barristers
161 Bay Street. Suite 2900
Toronto, ON 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, ON K2P 0R3
Telephone: (613) 695-8855 Ext: 102
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Agent for the Intervener,
Canadian Civil Liberties Association

Daniel J. Song, KC
Stephen Chin
Pringle Chivers Sparks Teskey
1720 - 355 Burrard Street
Vancouver, BC 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

A. Overview

1. The protection of privacy is one of the hallmarks of a free and democratic society. Privacy is not only "at the heart of liberty in a modern state"[1], but it is also essential to human dignity, democracy and self-determination. But like all *Charter* guarantees, the "right to privacy is not absolute."[2] This Court's section 8 jurisprudence has long recognized that "the guarantee of security from unreasonable search and seizure only protects a reasonable expectation."[3] Thus, as La Forest J. remarked in *Dyment*, privacy claims must "be balanced against other societal needs, and in particular law enforcement, and that is what s. 8 is intended to achieve."[4]

2. This appeal raises an important question for the investigation of cybercrime: does s. 8 protect an anonymous Internet Protocol ("IP") address? A majority of the Alberta Court of Appeal concluded the answer was "no".[5] Writing in dissent, Justice Veldhuis held that s. 8 was engaged when police acquired an anonymous IP address from a third party because the IP address could be "linked to a particular, monitored internet activity that could disclose biographical core information."[6] In Veldhuis J.A.'s view, police must obtain prior judicial authorization before they can acquire the decimal digits that constitute an IP address.

3. The Attorney General of British Columbia ("AGBC") intervenes to make three overarching points relevant to the resolution of this appeal.

4. The AGBC's first point is that an overly broad or imprecise characterization of the "subject matter" of a search is apt to produce analytical confusion. Where a search engages informational privacy, it is indeed appropriate to identify the "strong, immediate and direct"[7] inferences that might reveal private or intimate personal information. But that inferential process should not be conflated with consideration of the investigational objectives of police. An IP address does not, as

---

[1] *R. v. Dyment*, [1988] 2 S.C.R. 417 at 427-428.
[2] *R. v. Gomboc*, [2010] 3 S.C.R. 211, at para. 17 [*Gomboc*].
[3] *Hunter et al. v. Southam Inc.,* [1984] 2 S.C.R. 145 at 159-160 [*Hunter*, emphasis original].
[4] *R. v. Dyment*, [1988] 2 S.C.R. 417, at para. 18.
[5] *R v Bykovets*, 2022 ABCA 208, at para. 27 [*Bykovets ABCA*]
[6] *Bykovets ABCA*, at para. 94.
[7] *R. v. Kang-Brown*, [2008] 1 S.C.R. 456, at para. 175 [*Kang-Brown*].

the dissenting justice concluded, engage "a high level of informational privacy"[8] merely because the police hope to use it to eventually identify the suspect of a crime.

5. The AGBC's second and related point is that a raw IP address should not be given s. 8 protection because it reveals nothing about an individual's "biographical core". Section 8 does not extend to all information about a person but only to "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[9] On many occasions, this Court has confirmed the importance of the "biographical core" in defining the boundaries of s. 8 protection.[10] By limiting *Charter* protection to a sphere of intimate and personal information, this Court has struck a principled balance between the needs of law enforcement, on the one hand, and the public's interest in remaining free from state scrutiny on the other.

6. The AGBC's third and final point is that recognition of s. 8 protection over an IP address will have far-reaching consequences for the investigation of cybercrime. By way of example, most child pornography investigations begin when police identify an IP address sharing child pornography online. Police do not obtain judicial authorization when they monitor IP addresses online, or when they receive tips from electronic service providers. If an IP address is subject to s. 8 protection, the stable investigative framework governing child pornography investigations will be disrupted, doing little or nothing to enhance privacy, and leaving police with few tools to investigate many internet-based crimes.

B. Statement of Facts

7. The AGBC takes no position on the facts in this appeal.

PART II – QUESTIONS IN ISSUE

8. The AGBC intervenes to address the following question:

a. Does a reasonable expectation of privacy attach to an IP address?

---

[8] *Bykovets ABCA*, at para. 80 (per Velduis J.A., dissent).

[9] *R. v. Plant*, [1993] 3 S.C.R. 281 at 293 [*Plant*].

[10] See most recently: *Sherman Estate v. Donovan*, 2021 SCC 25, at para. 75 [*Sherman Estate*]; *R. v. J.J.*, 2022 SCC 28, at para. 44.

PART III – STATEMENT OF ARGUMENT

A. Identification of the "subject matter" of the search should not predetermine the outcome of the s. 8 analysis

9. This appeal involves a relatively rare example of a case where the identification of the "subject matter" of a search raises controversy. The trial judge and majority of the Court of Appeal were in agreement that the subject matter of the search was "the IP addresses which [were] sought for the purpose of being able to further the investigation."[11] The dissent, on the other hand, faulted the trial judge for "embark[ing] on an extremely narrow analysis of the subject matter."[12] The dissent held that the true subject matter was the "identity of an internet user which corresponds to a particular IP address that is linked to a particular, monitored internet activity."[13] The dissent concluded that this subject matter "engage[d] a high level of informational privacy."[14]

10. When this Court first recognized the "totality of the circumstances" framework in *Edwards*,[15] it did not identify the "subject matter" as a distinct analytical consideration. The subject matter inquiry first emerged in *Tessling*[16] where this Court considered whether using an infrared camera to capture images of "heat emanations" radiating from a home engaged s. 8. It is no accident that the subject matter inquiry emerged in a case involving informational privacy. In territorial or personal privacy cases, identifying the subject matter usually poses limited controversy. But the same cannot be said of claims involving informational privacy. When informational privacy is at stake, the characterization of the subject matter can radically shift the analysis. Indeed, depending on the identification of the subject matter, a bag of household waste could be considered mere "garbage" or "an opaque and sealed 'bag of information'."[17]

11. The dissenting justice's analysis arguably represents an example of a growing trend where reviewing courts have conflated the identification of the subject matter with the police's objectives in acquiring a piece of data or information.[18] The apparent source of this approach can be traced

---

[11] *R v Bykovets*, 2020 ABQB 70, at para. 44 [*Bykovets ABQB*]; *Bykovets ABCA*, at para. 26.
[12] *Bykovets ABCA*, at para. 66.
[13] *Bykovets ABCA*, at para. 77.
[14] *Bykovets ABCA*, at para. 80 [emphasis added].
[15] *R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 45.
[16] *R. v. Tessling*, [2004] 3 S.C.R. 432, at para. 32 [*Tessling*].
[17] *R. v. Patrick*, [2009] 1 S.C.R. 579, paras. 32, 54 [*Patrick*].
[18] *R. v Flintroy*, 2018 BCSC 1692, at para. 26; *R. v Ali, Boparai & Malonga-Massamba*, 2020 BCSC 1309, at para. 92; *R. v. Latimer,* 2020 BCSC 488, para. 172.

to a misunderstanding of *dicta* in *Spencer*.[19] In *Spencer*, Cromwell J. observed that when identifying the subject matter courts should consider "not only the nature of the precise information sought, but also [the] nature of the information that it reveals."[20] Cromwell J. went on to explain that "the *tendency* of information sought *to support inferences* in relation to other personal information must be taken into account in characterizing the subject matter of the search."[21]

12. Properly understood, *Spencer* should not be interpreted as a direction to consider police investigational objectives when defining the subject matter of a search. Instead, *Spencer* confirms an unbroken line of authority that holds that reviewing courts should consider whether a piece of seemingly innocuous information may inferentially reveal information that falls within the "biographical core" protected by s. 8. This Court's leading informational privacy decisions do not suggest that the overarching investigational objectives of police should be considered when characterizing the subject matter of a search. In *Plant*,[22] the subject matter of the search was electrical consumption records which "reveal[ed] very little about the personal lifestyle or private decisions of the occupant of [a] residence." In *Tessling*,[23] the subject matter was "heat emanations" from a home which supported "extremely limited" inferences. In *Kang-Brown*[24] and *A.M.*[25], the subject matter of a dog sniff search was the "airspace surrounding" a bag (*Kang-Brown*) or backpack (*A.M.*) which permitted police to make "strong, immediate and direct inference[s]" about their contents. In *Cole*,[26] this Court described the subject matter of a computer search as "the data, or *informational content* of the laptop's hard drive, its mirror image, and the Internet files disc — not the devices themselves." In *Marakah*[27] and *Jones*[28], this Court held that the subject matter of a cellphone search was the "electronic conversation" between sender and recipient, as well as "any inferences about associations and activities that can be drawn from that information."[29]

---

[19] *R. v. Spencer*, [2014] 2 S.C.R. 212 [*Spencer*].
[20] *Spencer*, at para. 26.
[21] *Spencer*, at para. 31 [emphasis added].
[22] *Plant*, at 293.
[23] *Tessling*, at para. 35.
[24] *Kang-Brown*, at para. 175.
[25] *R. v. A.M.*, [2008] 1 S.C.R. 569, paras. 66.
[26] *R. v. Cole*, [2012] 3 S.C.R. 34, at para. 41 [emphasis in original].
[27] *R. v. Marakah*, [2017] 2 S.C.R. 608 [*Marakah*].
[28] *R. v. Jones*, [2017] 2 S.C.R. 696, at para. 14 [*Jones*].
[29] *Marakah*, at para. 20; *Jones,* at para. 14.

13. As this brief review demonstrates, the subject matter must be defined with a greater degree of "precision"[30] than was articulated by the dissent in the court below. But more importantly, this Court has not infused the definition of the subject matter of a search with the police's intended use of seized information. Characterizing the subject matter of a search requires a reviewing court to ask "*what* the police were really after"[31] and not "*why* they were after it." There is good reason for this: it is self-evident that police acquire data or information, not for its own sake, but to determine if a crime has been committed and, if so, by whom. Although a broad and functional approach to the subject matter requires courts to consider the tendency of seemingly innocuous information to reveal intimate details about a person's lifestyle, the police's overall investigational objectives do not assist in this analysis.

B. Section 8 protection of the biographical core strikes an appropriate balance between privacy and the needs of law enforcement

14. A key issue dividing the court below was whether the police's receipt of an IP address could yield information that falls within the "biographical core" of information protected by s. 8. The majority, like the trial judge, concluded that a bare IP address "does not reveal intimate details of a person's lifestyle."[32] The dissenting justice, by contrast, appeared to accept that an IP address was a "parallel method" of identifying an internet user comparable to obtaining the internet subscriber information discussed by this Court in *Spencer*.[33]

15. The idea that s. 8 is directed at a "biographical core" of personal information was first proposed by this Court in *Plant*.[34] In his reasons, Sopinka J. rejected the notion that the *Charter* protected all forms of information about a person. Consistent with the purposive approach espoused by this Court in *Hunter*,[35] Sopinka J. reasoned that s. 8 should be construed purposively to foster "the underlying values of dignity, integrity and autonomy" by protecting "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."[36]

---

[30] *Marakah*, para. 16.
[31] *Marakah*, at para. 15 citing *R. v. Ward*, 2012 ONCA 660, at para. 67 [*Ward*].
[32] *Bykovets ABCA*, at para. 21; *Bykovets ABQB*, at para. 56.
[33] *Bykovets ABCA*, at paras. 88-89.
[34] *Plant*.
[35] *Hunter* at 155.
[36] *Plant*, at para. 20.

16. In the roughly 30 years since *Plant* was decided, this Court has confirmed the continued salience of the "biographical core" in defining the inner and outer boundaries of informational privacy protection under s. 8. In *Tessling*, Binnie J. described the "biographical core" as the means this Court has used to respond to the "difficult" question of "where the 'reasonableness' line should be drawn."[37] In *Gomboc*, Deschamps J. referred to the need to assess the "nature and quality of the information" and its "remoteness" from the biographical core.[38] In *Cole,* Fish J. held that "[t]he closer the subject matter of [an] alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy."[39] More recently, in *Sherman Estate,* this Court relied on the "biographical core" to define the limits of the "open court principle"[40] explaining that openness would give way to the protection of individual privacy where information in a court file "is sufficiently sensitive such that it can be said to strike at the biographical core of the individual."[41]

17. The analytical value of the biographical core turns as much on what falls within the core as what falls outside of it. Sopinka J. in *Plant* described the contents of the biographical core as encompassing "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[42] In *Sherman Estate*, this Court contrasted "intimate or personal details about an individual" with "generic information that reveals little if anything about who they are as a person".[43] While it would be "scarcely feasible" (and potentially counterproductive) to itemize a "judicial catalogue" of information falling within the core or periphery of s. 8,[44] this Court's jurisprudence contains helpful guidance on its basic dimensions. Computers and electronic devices like cellphones are protected under s. 8 because they may contain "our most intimate correspondence", as well as "details of our financial, medical, and personal situations."[45] But the same cannot be said of "heat emanations"[46] from a home or "electrical consumption records"[47]

---

[37] *Tessling,* at para. 25.
[38] *Gomboc*, at para. 2.
[39] *R. v. Cole*, [2012] 3 S.C.R. 34, para. 46 [*Cole*]; *R. v. Le*, [2019] 2 S.C.R. 692, at para. 221.
[40] *Sherman Estate*.
[41] *Sherman Estate*, at para. 35.
[42] *Plant* at 293.
[43] *Sherman Estate*, para. 75.
[44] *Tessling*, para. 19.
[45] *R. v. Morelli*, [2010] 1 S.C.R. 253, at para. 105.
[46] *Tessling*, at para. 58.
[47] *Plant*, at 293.

which are forms of information that are simply too generic or too abstract to reveal "activities of an intimate or private nature".[48]

18. By distinguishing between "intimate" and "generic" information, the biographical core defines the normative boundary line where "the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals".[49] This Court has stressed that the protection of privacy under s. 8 "seeks to strike an appropriate balance between the right to be free of state interference and the legitimate needs of law enforcement."[50] That balance is fundamentally disrupted if exaggerated significance is attached to generic information which, viewed objectively, is incapable of revealing anything meaningful about the lifestyle and personal choices of an identifiable individual.

19. Returning to the case at bar, recognition of s. 8 protection for an IP address is difficult to square with a jurisprudentially sound account of the biographical core. An IP address is "a multi-digit numerical identifier that is automatically and randomly assigned by an ISP to a subscriber when the subscriber's computer device connects to the Internet."[51] Unlike a computer, the informational value of an IP address is meaningless on its own. The extent to which that an IP address has the *potential* to reveal information about an identifiable individual is only realized through separate investigational steps, which themselves require judicial authorization.

C. Recognition of s. 8 protection for anonymous IP addresses will frustrate the investigation of cybercrime

20. The AGBC's final point emphasizes the practical implications of extending s. 8 protection to anonymous IP addresses. The dissenting justice was of the view that police actions in acquiring an IP address without a production order was "not driven"[52] by the absence of investigative tools. While the AGBC acknowledges that administrative convenience is not a justification for invading privacy rights, this Court should not underestimate the future impact of requiring judicial authorization to acquire IP addresses.

---

[48] *Gomboc*, para. 36; *Tessling*, para. 62.
[49] *Hunter* at 159-60.
[50] *R. v. Vu*, [2013] 3 S.C.R. 657, at para. 21 [*Vu*]; *Tessling*, at para. 17; *Patrick*, at paras. 14, 20.
[51] *Ward*, at para. 21.
[52] *Bykovets ABCA*, at para. 97.

21. One area of cybercrime that would be adversely impacted by the recognition of s. 8 protection over IP addresses is the investigation of child pornography offences. Child pornography offences, by their nature, involve surreptitious activity hidden from the public eye. Yet, because of advances in technology, child pornography can now be stored (and shared) in virtually unlimited quantities over the internet. Child pornography is occasionally discovered when third parties inadvertently find illicit material when examining an individual's devices.[53] But far more frequently, police detect anonymous IP addresses sharing child pornography over the internet or receive reports from third party agencies such as the National Center for Missing and Exploited Children ("NCMEC").[54]

22. The basic features of most child pornography investigations are reflected in numerous reported decisions including cases such as *Spencer* and *Ward*.[55] Child pornography investigations often begin when police detect an anonymous IP address uploading or downloading known child pornography using peer-to-peer file sharing programs such as Limewire or BitTorrent.[56] Police are able to monitor IP addresses sharing child pornography through web-based platforms that zero in on IP addresses trading in suspected child pornography.[57] Police can use law enforcement peer-to-peer programs to download suspected child pornography and verify its contents.[58]

---

[53] *R. v. Morelli,* [2010] 1 SCR 253; *Cole*; *R. v. Villaroman*, [2016] 1 S.C.R. 1000 [*Villaroman*].

[54] *R. v. Cusick*, 2019 ONCA 524, at para. 6; *R v. Friesen*, 2021 ABPC 223, at para. 6; *R v. Thibodeau*, 2021 BCPC 98, at para. 9 [*Thibodeau*]; *R. c. Laffont,* 2021 QCCQ 4433, at para. 15; *R. v Haire*, 2021 BCSC 1308, at para. 10 [*Haire*]; *R. v Meissner*, 2019 BCSC 1778, at para. 10 [*Meissner*]; *R. v Mollon*, 2017 BCSC 2481 [*Mollon*], at para. 8; *R. v Seguin*, 2015 ONSC 1908, at para. 2; *R. v. Gauthier*, 2021 ONCA 216, at para. 2; *R. v. Noseworthy*, 2017 CanLII 42035 (NL SC), at para. 12 [*Noseworthy*]; *R. v. Pahle*, 2017 ONSC 6164, at para. 14; *R. v. Shokouh*, 2022 ONSC 1451, at para. 3 [*Shokouh*]; *R. v. Wissink*, 2018 ONSC 6787, at para. 2.

[55] *R. v. Spencer*, 2009 SKQB 341, at para. 9; *Ward*.

[56] *Spencer*, at para. 7; *Villaroman*, at para. 9; *R. v. Crump*, 2022 ONCJ 510, at para. 7; *R. v. Owen*, 2017 ONCJ 729, at para. 54 [*Owen*]; *R. v. Collins*, 2017 SKQB 139, at para. 9; *R. v. Rhodes*, 2017 ONSC 4213, at para. 8.

[57] *R. v. Waygood*, 2018 BCCA 409, at para. 3; *R. v. Scopel-Cessel*, 2022 ONCA 316, at paras. 2 – 3; *R v Pratchett*, 2016 SKPC 19, at para. 18; *R. v. Ramlogan*, 2018 ONCJ 805, at para. 8; *R. v. Isaacs*, 2015 CanLII 13350 (NL PC), at para. 3 [*Isaacs*]; *R. v Hoben*, 2016 CanLII 18785 (NL PC), para. 1; *R. v. Gilbert*, 2015 NSSC 69, at para. 4; *R. v. El-Halfawi*, 2021 ONCJ 462, at para. 26; *R. v. Olmstead*, 2021 ONCJ 76, at para. 16; *R. v. Finn*, 2018 ONSC 7191, at para. 8; *R. v. MacDonald*, 2012 NSPC 132, at para. 6; *R. v. McKenzie*, 2017 SKQB 186, at para. 5; *R. v Nguyen*, 2017 ONSC 1341, at para. 7 [*Nguyen*]; *R. v. Collins*, 2017 SKQB 139, at para. 7; *R. c. Veillette*, 2020 QCCQ 8642, [*Veillette*].

[58] *R. v. Mains*, 2022 ONCJ 44, at para. 21; *R. v. El-Halfawi*, 2021 ONCJ 462, at para. 32[*El-Halfawi*]; *Nguyen*, at para. 9; *R. v. M.O.C.*, 2016 BCPC 273, at para. 16; *Veillette*, para. 5; *Isaacs*, at para. 3.

23. Once police have identified a target IP address, they must still pursue further investigational steps to link the IP address to a user or subscriber. Police can use open-source methods to identify the Internet Service Provider ("ISP") associated with a target IP address.[59] After identifying the ISP, police may make a preservation demand under s. 487.012(1) of the *Criminal Code*.

24. The next typical investigative step is to obtain a production order directed at the identified ISP in conformity with *Spencer*. If a production order is granted, police must serve the order on the ISP. Only then will the ISP provide investigators with subscriber information—usually consisting of the subscriber's name, their address, and perhaps associated email addresses.

25. Police must undertake further investigational steps to obtain a search warrant for a residence or any digital storage devices therein. This can include surveillance of the residence or business associated with the target IP address to confirm the identity of subscribers or potential users. Police may then be in a position apply for a search warrant authorizing them to seize and search devices believed to contain evidence of child pornography. To access the data on seized devices, such search warrants must comply with this Court's ruling in *Vu*.[60]

26. To date, the jurisprudence has not suggested that police must have prior judicial authorization when they initially identify a "raw IP address"[61] sharing child pornography online. On the contrary, in *Spencer* itself the investigating police officer had already obtained an IP address before he made a request for subscriber information from the ISP. Cromwell J. explained that police could have applied for "a production order requiring Shaw to release the subscriber information corresponding to the IP address they had obtained."[62] Yet, the dissenting reasons in the court below appear to require police to obtain prior judicial authorization any time an IP address could be "linked to a particular, monitored internet activity".[63]

27. The same would apply *a fortiori* to the receipt of reports from third parties. At present, police receive reports from agencies such as NCMEC that contain identifiable IP addresses without obtaining prior judicial authorization.[64] In *Ward*, for example, the investigation began when

---

[59] *Owen*, at para. 7; *Mollon*, at para. 10.
[60] *Vu*, at paras. 3 and 49.
[61] *Nguyen*, at para 36; *El-Halfawi*, at para 82.
[62] *Spencer*, at para. 49 [emphasis added].
[63] *Bykovets ABCA*, at para. 94.

"German authorities forwarded a list of 229 IP addresses" involved in accessing child pornography to the RCMP.[65] If, in the case at bar, police needed a production order to obtain an IP address from Moneris, then the same would arguably be true of reports identifying IP addresses accessing child pornography that are received from third parties. An added complication for NCMEC reports is that they are often generated by U.S. based electronic service providers such as Google, Microsoft, Facebook and Instagram.[66]

28. Investigations involving child pornography and other cybercrimes require a strong element of preventative and proactive policing. In most cases, the identification of an IP address is the precipitating event that triggers an investigation. If police cannot monitor or receive IP addresses without prior judicial authorization—because they are protected by s. 8—it is difficult to imagine how they will be able to proactively pursue these investigations.

PART IV – COSTS

29. The AGBC does not seek costs and asks that no costs be awarded against it.

PART V – ORDER SOUGHT

30. The AGBC takes no position with respect to the disposition of the appeal but seeks an order to present oral submissions not exceeding five minutes.

ALL OF WHICH IS RESPECTFULLY SUBMITTED,

 for:

Michael Barrenger
Counsel for the Intervener,
Attorney General of British Columbia

 for:

Micah B. Rankin
Counsel for the Intervener,
Attorney General of British Columbia

Dated at Victoria, British Columbia, this 21st day of December 2022.

---

[65] *Ward*, at para. 29.

[66] *Thibodeau*, at para. 9; *R. v. Williams*, 2021 ONCJ 552, at para. 2; *Meissner*, at para. 10; *R. v. Noseworthy*, at para. 12; *R. v Cusick*, 2015 ONSC 6739, at para. 25; *Mollon*, at para. 8; *R. v. Claveria*, 2021 ONCJ 348, at para. 5; *R. v. Neasloss*, 2020 BCPC 161, at para. 7; *Shokouh*, at para. 3; *Haire*, at para. 9.

PART VII – TABLE OF AUTHORITIES

R. v. Wissink, 2018 ONSC 6787	8
Sherman Estate v. Donovan, 2021 SCC 25	2, 5, 6
LEGISLATION	
Canadian Charter of Rights and Freedoms, s. 8 *Loi constitutionnelle de 1982*, Annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11, s. 8	1, 2 3, 4, 5, 6, 7, 9
Criminal Code, R.S.C., 1985, c. C-46, s. 487.012(1) *Code criminel* (L.R.C. (1985), ch. C-46), s. 487.012(1)	8