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)

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
DIRECTOR OF PUBLIC PROSECUTIONS

Public Prosecution Service of Canada
Suite 1400, Duke Tower, 5251 Duke Street
Halifax, Nova Scotia B3J 1P3

David Schermbrucker
Allyson Ratsoy
Tel: (902) 426-2285 / (613) 612-6657
Fax: (902) 426-1351
Email: david.schermbrucker@ppsc-sppc.gc.ca
allyson.ratsoy@ppsc-sppc.gc.ca

Counsel for the intervener, Director of Public Prosecutions

Kathleen Roussel
Public Prosecution Service of Canada
160 Elgin Street, 12th Floor
Ottawa, Ontario K1A 0H8

Per: François Lacasse
Tel: (613) 957-4770
Fax: (613) 941-7865
Email: francois.lacasse@ppsc-sppc.gc.ca

Agent for the intervener, Director of Public Prosecutions

McKay Ferg LLP
1800, 639 6th Ave SW
Calgary, Alberta T2P 0M9

Sarah Rankin
Ian McKay
Heather Ferg
Tel: (403) 984-1919
Fax: (844) 895-3926
Email: sarah@mckaycriminaldefence.com

Counsel for the appellant, Andrei Bykovets

Power Law
99 Bank Street, Suite 701
Ottawa, Ontario K1P 6B9

Jonathan Laxer
Tel: (613) 902-5652
Fax: (613) 902-5652
Email: jlaxer@powerlaw.ca

Agent for the appellant, Andrei Bykovets

Justice and Solicitor General
Appeals, Education & Prosecution Policy Branch
300, 332 – 6th Avenue SW
Calgary, Alberta T2P 0B2

Rajbir Dhillon
Tel: (403) 297-8444
Fax: (403-297-4311
Email: rajbir.dhillon@gov.ab.ca

Counsel for the respondent, His Majesty the King

Gowling WLG (Canada) LLP
160 Elgin Street, Suite 2600
Ottawa, Ontario K1P 1C3

D. Lynne Watt
Tel: (613) 786-8695
Fax: (613) 788-3509
Email: lynne.watt@gowlingwlg.com

Agent for the respondent, His Majesty the King

Attorney General of Ontario
720 Bay Street, 10th Floor
Toronto, Ontario M7A 2S9

Jeremy Streeter
Andrew Hotke
Tel: (416) 327-5990
Fax: (416) 326-4656
Email: Jeremy.streeter@ontario.ca

Counsel for the intervener, Attorney General of Ontario

Attorney General of British Columbia
Criminal Appeals and Special Prosecutions
3rd Floor, 940 Blanshard Street
Victoria, British Columbia V8W 3E6

Micah B. Rankin
Tel: (778) 974-3344
Fax: (250) 387-4262
Email: micah.rankin@gov.bc.ca

Counsel for the intervener, Attorney General of British Columbia

Gowling WLG (Canada) LLP
2600-160 Elgin Street
Ottawa, Ontario K1P 1C3

Matthew Estabrooks
Tel: (613) 786-0211
Fax: (613) 788-3573
Email: matthew.estabrooks@gowlingwlg.com

Agent for the intervener, Attorney General of British Columbia

Kapoor Barristers
161 Bay Street, Suite 2900
Toronto, Ontario M5J 2S1

Anil K. Kapoor
Cameron Cotton O'Brien
Tel: (416) 363-2700
Fax: (416) 363-2787
Email: akk@kapoorbarristers.com

Counsel for the intervener, Canadian Civil Liberties Association

Supreme Advocacy LLP
100-340 Gilmour Street
Ottawa, Ontario K2P 0R3

Marie-France Major
Tel: (613) 695-8855 Ext: 102
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Agent for the intervener, Canadian Civil Liberties Association

Pringle Chivers Sparks Teskey
1720-355 Burrard Street
Vancouver, British Columbia V6C 2G8

Daniel J. Song, KC
Stephen Chin
Tel: (604) 699-7447
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

Overview

1. The Director of Public Prosecutions ("DPP") intervenes in this appeal, by leave, in order to impress upon the Court the vital need to balance competing interests when determining whether a claimant has a constitutionally protected right of privacy in their IP address. The framework for this balancing is well established. A proper normative approach to the task requires this balancing of interests.

2. An Internet Protocol address ("IP address") does not identify the user, nor in the circumstances of this case tends by itself to reveal any other private information. The police obtained private information only later pursuant to judicial authorization. Assessed in the totality of the circumstances, including a balancing of interests under the normative approach, the IP address of the claimant was not subject to a reasonable expectation of privacy.

3. As crime is increasingly committed online, the police must follow. Obtaining an IP address that provides only a series of numbers related to an unknown computer does not impact any expectation of privacy in a manner that outweighs the interests of law enforcement in investigating crime.

Facts

4. The intervener DPP takes no position on the facts.

PART II – POSITION ON THE QUESTION IN ISSUE

5. The DPP supports the respondent's position that the trial judge and the majority of the Alberta Court of Appeal were correct in finding that no reasonable expectation of privacy attaches to an IP address.

6. The DPP's particular submission is that in determining whether there is a *Charter* protected reasonable expectation of privacy in an IP address, it is critically important to balance the nature of the privacy interest with the duty and ability of the police to investigate cybercrime.

PART III – ARGUMENT

This Court should maintain the balancing of competing interests in assessing privacy

7. "The community wants privacy but it also insists on protection."[1] Justice Binnie's words in *Tessling* (2004) succinctly express the tension between the individual's interest in freedom from state intrusion and the community's interest in effective law enforcement. They also express the sound view that any assessment of whether the *Charter* protects privacy in a particular case must consider and balance these competing interests. A lack of balance on either side potentially favours a police state or, conversely, a society overrun by cybercrime, which police have inadequate powers to investigate.

8. This Court consistently and enduringly looked to balance the competing interests that present between an individual's right to be free from state intrusion and the state's duty to conduct effective law enforcement. Several extracts from this Court's previous judgments illustrate in a vast array of varying circumstances the need for such balancing. The DPP invites the Court to continue its practice of balancing those interests in assessing the expectation of privacy in an IP address.

9. The proper balancing of these interests, in this context, leads to the conclusion that there is no reasonable expectation of privacy in an IP address. To find an expectation of privacy in information which lacks any personal identifying features, while potentially hampering police investigations, would tip the balance much too far to the individual interests of the accused.

10. In *Hunter v Southam* (1984), the original judgment of this Court on privacy under section 8 of the *Charter*, Dickson J (as he then was) discussed the nature of the constitutional right to be free from unreasonable search and seizure: he referred to the English and United States history and jurisprudence; and then—in a clear effort to chart the course going forward for Canada—he wrote:

> The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that **an assessment must be made as**

[1] *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 17.

> **to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement**.[2]

11. Following this original course-setting statement, the balancing of interests has been a recurring and overarching theme in this Court's jurisprudence on assessing privacy under section 8 of the *Charter*. This theme has been consistently evident, even as digital searches of devices have joined physical searches of places, and as traditional investigative techniques such as physical surveillance have been complemented by modern technology.

12. In *Duarte* (1990), balancing privacy interests with law enforcement needs was central to this Court's conclusion that participant wiretapping must be judicially authorized. Justice La Forest wrote:

> Electronic surveillance plays an indispensable role in the detection of sophisticated criminal enterprises. Its utility in the investigation of drug related crimes, for example, has been proven time and time again. But, for the reasons I have touched on, it is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion. The threat this would pose to privacy is wholly unacceptable.
>
> It thus becomes necessary to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in the furtherance of its responsibilities for law enforcement.[3]

13. In *Plant* (1993), this Court determined there was no reasonable expectation of privacy in computer records which tracked electricity consumption, but no details about the lifestyle or private decisions of the occupants of the residence. Justice Sopinka reiterated the need for a balanced analysis in the following terms:

> The purpose of s. 8 is to protect against intrusion of the state on an individual's privacy. The limits on such state action are determined by balancing the right of citizens to have respected a reasonable expectation of privacy as against the state interest in law enforcement.[4]

---

[2] *Hunter v Southam*, [1984] 2 SCR 145 at 159-160 [underlining in original; bold added].
[3] *R v Duarte*, [1990] 1 SCR 30 at 44-45.
[4] *R v Plant*, [1993] 3 SCR 281 at 291-292.

14. In *Tessling* (2004), Binnie J restated the need to strike a balance between individual privacy and suppression of criminality, leading to his conclusion that there was no reasonable expectation of privacy in heat signatures emanating from a residence:

> Safety, security and the suppression of crime are legitimate countervailing concerns. Thus s. 8 of the *Charter* accepts the validity of reasonable searches and seizures. A balance must be struck, as held in *Hunter v Southam*…[5]

15. In *Reeves* (2018), Karakatsanis J wrote, early on in paragraph 2 of her reasons, that: "In assessing whether s. 8 has been infringed, courts consider whether an individual's privacy interests must give way to the state's interest in law enforcement."[6]

16. In *Mills* (2019), Karakatsanis J observed that: "as technology evolves, the ways in which crimes are committed—and investigated—also evolve."[7] Thus, the tension between unauthorized online intrusion by the state and the protection of vulnerable children had to be addressed. In the circumstances of *Mills*, requiring police to obtain judicial pre-authorization before even launching an electronic undercover investigation would effectively "hamstring" the police from proactively investigating child luring offences and, therefore, "simply does not strike an appropriate balance between individual privacy and the safety and security of our children."[8]

17. These authorities show that the balancing exercise cannot be all one sided. The Court cannot simply focus on the interests of the accused. It is necessary to consider the need of law enforcement, and balance that against the interests of the accused. To fail to do so risks losing the balance that this Court has always strived to include in the section 8 analysis.

Balancing digital privacy and law enforcement concerns

18. The wide scope of personal information stored on cell phones and computers and the high privacy interests that attach to such information have been noted by this Court in many decisions.[9] However, the reality is that when criminals operate online, police have no choice but to follow.

---

[5] *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 17 [underlining in original].
[6] *R v Reeves*, 2018 SCC 56, [2018] 3 SCR 531 at para 2 (Karakatsanis J).
[7] *R v Mills*, 2019 SCC 22, [2019] 2 SCR 320 at para 39 (Karakatsanis J).
[8] *R v Mills*, 2019 SCC 22, [2019] 2 SCR 320 at para 52 (Karakatsanis J).
[9] *R v Morelli*, [2010] 1 SCR 253 at paras 1-2; *R v Vu*, [2013] 3 SCR 657 at para 24; *R v Cole*, [2012] 3 SCR 34 at paras 2-3.

This Court should not lose sight of the difficulties that would arise in investigating online crime if even the most benign piece of information, such as an IP address, benefits from *Charter* protection.

19. Police most often seek an IP address at the early stages of an investigation, as illustrated by the instant case. Credit card data had been stolen and used for fraudulent online purchases. To discover the identity of the thief, police had to follow the online path. That path started with Moneris, the financial service provider who identified an IP address associated to the individual making the online transactions. Once in possession of the IP address, through open source information, the police identified Telus as the Internet Service Provider that had assigned that IP address. At that stage of their investigation, the police were certainly not getting a treasure trove,[10] but only the minimal information required to obtain judicial authorization to lead them to the subscriber using that particular IP address.

20. In the absence of any information about who fraudulently used the credit cards, all the police knew at the beginning of the investigation was that an offence had been committed and that Moneris would have an IP address linked to the fraudulent transactions. That IP address was the starting point investigators needed. This will be the case in many cybercrime scenarios.

21. The question then becomes how many hurdles should the police face in pursuing their online investigations and how will this affect their ability to protect the safety and security of the community? Requiring judicial authorization for police to obtain an IP address would, at the very least, result in delaying any law enforcement response until grounds for a production order emerge from some other source. At worst, it will allow the most dangerous online offences, such as child luring, to continue while law enforcement remains paralyzed.

22. This was the risk that Karakatsanis J found unacceptable in *Mills*, in the context of online police undercover investigations. Her analysis applies here. Requiring police to obtain judicial pre-authorization to obtain an IP address does not strike an appropriate balance between individual privacy and the safety and security of our community.

[10] *R v Otto*, 2019 ONSC 2473 at para 60.

The normative assessment of *Charter*-protected privacy requires a proper balancing of the competing interests

23. It is well understood that the constitutional protection of a reasonable expectation of privacy is normative, not descriptive: what privacy **should** we have, not what privacy **do** we have.[11] It is equally clear that the normative approach to privacy reflects the original assessment of interests pronounced in *Hunter v Southam*.[12]

24. The normative approach to privacy protection emerged in *Wong* (1990)[13] and gained essential traction in *Tessling* (2004)[14] as a response to the proposition that persons only have constitutional protection of the privacy that in fact they do have.[15] However, a normative approach to privacy protection must remain balanced, not absolute, as explained by professor Hamish Stewart:

> Put another way, the ultimate normative question is whether, in light of the impact of an investigative technique on privacy interests, it is right that the state should be able to use that technique without any legal authorization or judicial supervision. **Does our conception of the proper relationship between the investigative branches of the state and the individual permit this technique without specific legal authorization?**[16]

25. The answer to the question as to what privacy should one have in an IP address is not total privacy, but as much as is reasonably needed for individual liberty and autonomy in our modern democracy, subject to society's reasonable need for law enforcement and public safety.

---

[11] *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 42; *R v Mills*, 2019 SCC 22, [2019] 2 SCR 320 at paras 20-26 (Brown J), para 59 (Karaktsanis J), para 80 (Martin J); *R v Jarvis*, 2019 SCC 10, [2019] 1 SCR 488 at para 68 (Wagner CJ); *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 at para 14.
[12] *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 at para 14.
[13] *R v Wong*, [1990] 3 SCR 36 at 45-48, as discussed by Renee Pomerance, "Flirting With Frankenstein: The Battle Between Privacy and Our Technological Monsters", (2016) 20 Can Crim L Rev 149 at 156-157.
[14] *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 42.
[15] Renee Pomerance, "Flirting With Frankenstein: The Battle Between Privacy and Our Technological Monsters", (2016) 20 Can Crim L Rev 149 at 157-159.
[16] Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy", (2011) 54 SCLR (2d) 335 at 342 [bold added], quoted in *R v Mills*, 2019 SCC 22, [2019] 2 SCR 320 at para 59 (Karakatsanis J). See also *R v Orlandis-Habsburgo*, 2017 ONCA 649 at para 41.

The "totality of the circumstances" approach also invokes a balancing of competing interests

26. In *Tessling* this Court established that whether there is a constitutionally protected reasonable expectation of privacy within section 8 of the *Charter* depends on assessing the "totality of the circumstances."[17] In the informational privacy sphere, which is at stake in this appeal, this engages four basic and well recognized[18] lines of inquiry:

> (1) What was the subject matter of the search?
>
> (2) Did the claimant have a direct interest in the subject matter of the search?
>
> (3) Did the claimant have a subjective expectation of privacy in the subject matter of the search?
>
> (4) Was that expectation of privacy objectively reasonable?

27. Evaluating the totality of the circumstances logically requires a balancing of the person's interests and the state's interests in responding to questions 1 and 4.

What was the subject matter of the search?

28. The principal parties diverge widely on this first line of inquiry. The appellant says the subject matter of the search was the police obtaining the IP address along with any further use to which the police could put that information. The respondent says the IP address is just a series of numbers.

29. The appropriate and useful question to ask, when assessing the subject matter of the search, is: "What were the police really after?" In *Marakah* (2017), McLachlin CJ explained that:

> The subject matter of a search must be defined functionally, not in terms of physical acts, physical space, or modalities of transmission. As Doherty J.A. stated in *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 65, a court identifying the subject matter of a search must not do so "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action". In *Spencer*, at para. 26, Cromwell J. endorsed these words and

---

[17] *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at paras 19, 31-32, citing *R v Edwards*, [1996] 1 SCR 128.

[18] *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608 at para 11 (McLachlin CJ); *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34 at para 40 (Fish J); *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 at para 18; *R v Mills*, 2019 SCC 22, [2019] 2 SCR 320 at para 13 (Brown J); *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 at para 18.

> added that courts should take "a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake" and should look at "not only the nature of the precise information sought, but also at the nature of the information that it reveals". The court's task, as Doherty J.A. put it in *Ward*, is to determine "what the police were really after".[19]

30. What the police were really after and obtained in this case was the IP address somebody's computer used in order to conduct a fraudulent credit card transaction. Moneris had that IP address, so the police asked Moneris for it. That was "the subject matter of the search."

31. The point remains that in assessing "the subject matter of the search" this Court must balance the competing interests of individual privacy and law enforcement. It is not enough to simply assume that a person does not wish their computer's IP address to be shared with the police on the theory that it is a breadcrumb in a possible trail of technological breadcrumbs.[20] In a case involving a technological trail of "breadcrumbs"—as this appeal is—sometimes a breadcrumb is just a breadcrumb. As a result, the search in this case does not amount to a search for *Charter* purposes.

The claimant's expectation of privacy in their IP address is not objectively reasonable

32. Assuming, for the sake of argument, that the claimant has a direct interest in the police obtaining their IP address, and they subjectively have an expectation of privacy in that information, that expectation is objectively unreasonable.

33. When an internet user goes online, their computer's IP address is employed in order for the user to browse a webpage, conduct online banking, or otherwise communicate with the host or administrator of the webpage. The uncontroverted evidence of Mr Musters describes this.[21] Here, the host or administrator can "see" the user's IP address but nobody else can. This is the scenario in the present appeal, where Moneris had the user's IP address but others did not. It is also the scenario in cases like *Ward*,[22] where the host of a forum webpage provided users' IP addresses to German police. Otherwise, law enforcement would not have the IP address.

---

[19] *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608 at para 15 (McLachlin CJ); *R v Reeves*, 2018 SCC 56, [2018] 3 SCR 531 at para 29 (Karakatsanis J).
[20] *R v Bykovets*, 2022 ABCA 208, dissenting reasons of Veldhuis JA at paras 69-70 [Appellant's Record, Tab 1D, p 50].
[21] Affidavit of Matthew Musters, Ex VD-1 [Appellant's Record, Tab 4B, pp 309-310].
[22] *R v Ward*, 2012 ONCA 660 at paras 27-29; *R v Ward*, 2008 ONCJ 355 at paras 10-13.

34. Returning to the balancing of interests originally expressed in *Hunter v Southam*, the public's interest in being left alone by the State must give way to the government's interest in intruding on the individual's privacy in order to advance its legitimate law enforcement goal. As a result, there is no expectation of privacy, and thus no search for *Charter* s. 8 purposes, in obtaining a mere IP address.

PART IV – SUBMISSIONS AS TO COSTS

35. The DPP does not seek any costs and makes no submissions as to costs.

PART V – ORDER SOUGHT

36. The DPP takes no position on the relief to be granted in these appeals.

All of which is respectfully submitted this 21st day of December 2022.

David Schermbrucker
Allyson Ratsoy
Counsel for the Intervener
Director of Public Prosecutions of Canada

PART VI – TABLE OF AUTHORITIES

Jurisprudence	**Paragraphs Cited**
Hunter v Southam, [1984] 2 SCR 145	10, 14, 23, 34
R v Cole, 2012 SCC 53, [2012] 3 SCR 34	18, 26
R v Duarte, [1990] 1 SCR 30	12
R v Edwards, [1996] 1 SCR 128	26
R v Jarvis, 2019 SCC 10, [2019] 1 SCR 488	23,
R v Marakah, 2017 SCC 59, [2017] 2 SCR 608	26, 29,
R v Mills, 2019 SCC 22, [2019] 2 SCR 320	16, 22, 23, 24, 26
R v Orlandis-Habsburgo, 2017 ONCA 649	24
R v Otto, 2019 ONSC 2473	19
R v Patrick, 2009 SCC 17, [2009] 1 SCR 579	23
R v Plant, [1993] 3 SCR 281	13
R v Reeves, 2018 SCC 56, [2018] 3 SCR 531	15, 29
R v Spencer, 2014 SCC 43, [2014] 2 SCR 212	26, 29
R v Tessling, 2004 SCC 67, [2004] 3 SCR 432	7, 14, 23, 24, 26
R v Ward, 2008 ONCJ 355	33
R v Ward, 2012 ONCA 660	29, 33
R v Wong, [1990] 3 SCR 36	24

Secondary Sources	**Paragraphs Cited**
Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy", (2011) 54 SCLR (2d) 335 at 342	24
Renee Pomerance, "Flirting With Frankenstein: The Battle Between Privacy and Our Technological Monsters", (2016) 20 Can Crim L Rev 149 at 156-159	24