Court File No. 40269

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL OF ALBERTA)

B E T W E E N:

ANDREI BYKOVETS

APPELLANT

- AND -

HIS MAJESTY THE KING

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
CANADIAN CIVIL LIBERTIES ASSOCIATION, INTERVENER

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

KAPOOR BARRISTERS
161 Bay Street, Suite 2900
Toronto, ON M5J 2S1

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

Counsel for the Intervener,
Canadian Civil Liberties Association

SUPREME ADVOCACY LLP
340 Gilmour Street, Suite 100
Ottawa ON K2P 0R3

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

Counsel for the Intervener,
Canadian Civil Liberties Association

MCKAY FERG LLP
1800, 639 6th Ave SW
Calgary, AB 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, ON K1P 6B9

Jonathan Laxer
Tel: (613) 907-5652
Fax: (613) 907-5652
Email: jlaxer@powerlaw.ca

Agent for Counsel for the Appellant,
Andrei Bykovets

JUSTICE AND SOLICITOR GENERAL
Alberta Crown Prosecution Service
Appeals, Education & Prosecution Policy Branch
300, 332 - 6th Avenue SW
Calgary, AB 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
2600 - 160 Elgin St
Ottawa, ON K1P 1C3

D. Lynne Watt
Tel.: (613) 786-8695
Fax: (613) 563-9869
Email: lynne.watt@gowlingwlg.com

Agent for Counsel for the Respondent,
His Majesty the King

PUBLIC PROSECUTION SERVICE OF CANADA
Suite 1400, Duke Tower
5251 Duke Street
Halifax, NS B3J 1P3

David W. Schermbrucker
Allyson Ratsoy
Tel: (902) 426-2285
Fax: (902) 426-1351
Email: David.Schermbrucker@ppsc-sppc.gc.ca

Counsel for the Intervener,
Director of Public Prosecutions

DIRECTOR OF PUBLIC PROSECUTIONS OF CANADA
160 Elgin Street, 12th Floor
Ottawa, ON K1A 0H8

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

Agent for Counsel for the Intervener,
Director of Public Prosecutions

ATTORNEY GENERAL OF BRITISH COLUMBIA
Criminal Appeals and Special Prosecutions
3rd Floor, 940 Blanshard Street
Victoria, BC V8W 3E6

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

Counsel for the Intervener,
Attorney General of British Columbia

ATTORNEY GENERAL OF ONTARIO
720 Bay Street, 10th Floor
Toronto, ON 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

PRINGLE CHIVERS SPARKS TESKEY
1720 - 355 Burrard Street
Vancouver, BC V6C 2G8

Daniel J. Song, K.C.
Stephen Chin
Tel: (604) 669-7447
Fax: (604) 259-6171
Email: djsong@pringlelaw.ca

Counsel for the Intervener,
British Columbia Civil Liberties Association

GOWLING WLG (CANADA) LLP
2600 - 160 Elgin Street
Ottawa, ON K1P 1C3

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

Agent for Counsel for the Intervener,
Attorney General of British Columbia

TABLE OF CONTENTS

PART I: STATEMENT OF THE CASE

1. Do the police need a warrant to require a third party to provide an unknown suspect's IP address and information revealing when the user accessed the internet? In deciding this question this Honourable Court has the opportunity to further develop the law of informational privacy, which began with *Spencer*,[1] to consider whether constitutionally protected privacy and liberty interests are implicated by the police obtaining this information without warrant, accepting that an IP address includes information from which the name of the suspect's internet service provider (ISP) along with the location when that suspect accessed the internet can be derived.[2]

2. As society becomes more reliant on the internet for daily tasks and expression, regulating law enforcement's activities in the digital space is essential to preserving freedom and privacy, enabling full participation in our culture and society without fear of unregulated police surveillance.

PART II: POSITION ON THE QUESTIONS IN ISSUE

3. The CCLA advances two related arguments:

   i. Police access to an internet user's unique IP address should be regulated just as police access to other similar private information is regulated. For example, the use of technology to capture International Mobile Subscriber Identity (IMSI) numbers or obtaining cell tower information from telecoms. Both yield information which is comparable to that embedded in an IP address a user's location in geographical range/space and identity of the ISP; and

[1] *R. v. Spencer*, 2014 SCC 43

[2] In this case the police asked the third-party for information fixing the time of accessing the internet which was provided but that is *not* part of the information an IP address contains. Further an IP address is a series of numbers which provides two sets of information, the first identifies the network on which the connection is made (ISP) and the second identifies the device which the user is using to connect to the internet (usually a router). Publicly available web sites allow anyone to identify the location associated with the IP address (see https://whatismyipaddress.com/ip-lookup), for example.

ii. Liberty, as understood in the *Charter*, protects access to the internet. It is an essential way people live a full and dignified life. From a normative perspective, people expect to access the internet without police obtaining a record of their access without warrant. They expect to be free from police post-hoc surveillance unless warranted.

PART III: ARGUMENT

i. IP addresses are similar to other recognized private information

4. Like information obtained by an IMSI catcher or a cell tower dump, an IP address offers two critical pieces of private information:

i. the IP address provides the police with essential information to identify the ISP associated with the IP address in question; and

ii. the IP address also provides the police with essential information to pinpoint the location a user's device accessed the internet. The geographical area is usually identified as the municipality in which the device accessed the internet.

5. The information embedded in an IP address is similar to the information obtained from cell tower data, which can only be accessed by police pursuant to a production order.[3] Cell tower data provides an approximate geographical location, as well as a time at which that location was "pinged" by a user's mobile phone. While an IP Address does not, in and of itself, reveal the time of access it is often accompanied by that information generated by the third-party who has the IP address. Importantly, cell tower data provides a geographic range, not an exact location, just like the information one can learn from an IP address.

6. IMSI catchers capture similar location information by tracking all mobile phones within their vicinity. IMSI catchers do this by pretending to be a user's cell phone tower and by diverting

[3] *R. v. TELUS Communications Co.*, 2013 SCC 16; *R. v. Rogers Communications*, 2016 ONSC 70 (CanLii), paras. 63-65, which sets out guidelines for police obtaining such production orders.

a user's IMSI to the police device which gives police a user's rough location, like the information that a person can learn if they have an IP address.

7. Both police use of IMSI catchers and accessing cell tower data are regulated by the judicial authorisation regime.[4] Both are a means by which the police can force third parties to produce digital records evidencing network (be it mobile or internet) access.

8. The CCLA respectfully submits there is no principled distinction between these various forms of data collection from third parties such that a warrant is required in one circumstance and not the other. Respectfully, the existing doctrine of privacy supports a warrant requirement for each.

9. In this case, the majority of the Alberta Court of Appeal regarded an IP address as merely a series of number separated by a period. However, it is much more than that. As the dissenting reasons of Justice Veldhuis recognized, an IP address provides the basis for the police to identify an internet user. An IP address does in fact provide identifying information in the form of a location and identified ISP, also third-parties often separately generate the time that a user accessed the internet.

10. Having the IP address allows the police to learn the identity of the ISP. With that information, they can then obtain and execute a *Spencer* warrant to obtain the identity of the user. It is useful to underscore that the grounds to believe a crime has been committed, essential for the *Spencer* warrant, exist independently of the acquisition of the IP address from the third-party. However, crucial pieces of information, the location and, in some instances, the time of accessing the internet along with the identity of the ISP are unknown until the IP address is obtained. Understood in this light, the IP address is not neutral information, it provides necessary core identifying information to obtain a *Spencer* warrant – a necessary step along the way to finding the suspect in the digital world. Again, this is an identification step, it does not generate grounds for the belief that a crime has occurred – those have matured. Consequently, with the grounds in hand,

[4] In the case of IMSI catchers, see *R. v. Brewster*, 2016 ONSC 4133 (CanLii); for cell tower data see *R. v. TELUS Communications Co.;* and *R. v. Rogers Communications*, *supra* note 9.

the police have what they need to seek an authorization to compel a third-party to produce the IP address.

ii. Liberty

11. The CCLA respectfully submits that using the internet is an exercise of liberty premised on the expectation that one's use will be free from unregulated police digital surveillance.[5] This includes any of these activities, the fact of being online, when they were online, where they accessed the internet and what they viewed. The police has no right to know where one has been – people expect that their digital footprint would not be available to the police in the absence of judicial oversight.

12. The internet is ubiquitous, everything from shopping to communications to education and participation in our public institutions, such as court proceedings, is mediated through the internet. People expect to transact in society without police monitoring either in real time or after the fact. Unregulated police surveillance (including *post-hoc*) is anathema to a free and democratic society. That said, police can access a person's digital footprint (post-hoc surveillance) where there has been a prior judicial authorisation. To use the language of the *Charter* warranted access represents a fundamentally just limit on liberty. Put slightly differently, one's movements (digitally recorded) are not the business of the police; it only becomes their business if they have grounds that the information will assist in unearthing criminal activity – if they wish access they must subject their grounds to the prior judicial authorization regime in accordance with the Constitution.

13. The internet is a particular and necessary mode of engaging with the world. The generation and disclosure of an IP address is a necessary condition to accessing the internet. One cannot transmit or receive information online without generating an IP address. People expect to transact their activities understanding that the police will only be able to access their internet activities if a judge permits. Having a judge sanction police access ensures that there is a reason to access the information. This normative expectation is reasonable and is reflected in Justice Veldhuis'

[5] Though the surveillance does not occur in real-time as usually understood, given the precision with which the information is preserved, tracking an internet user's digital footprint is a form of *post-hoc* surveillance and should be understood as such.

dissenting reasons.[6] Relying on *R* v *Jones*,[7] she underscored that an individual should not be required to take evasive steps to, such as abstaining from online life, in order to protect their privacy:

> Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives. I therefore conclude that the sender of a text message retains a reasonable expectation of privacy in records of text messages stored in a service provider's infrastructure notwithstanding that he relinquished direct control over those messages. This result comports with contemporary social norms and a purposive approach to s. 8. It also comports with the purpose of PIPEDA, and the approaches adopted by this Court in *Spencer* and *TELUS*.

Similarly, an individual should not have to conceal themselves to protect their liberty to be free from police monitoring by using VPN technology[8] or use internet cafes or other means. Instead, people should be secure in the knowledge that all their private online activities[9] at anytime from anywhere (including their home) cannot be accessed by the police unless they have a warrant.

14. As held by this Honourable Court in *Alberta (Information and Privacy Commissioner)* v *United Food and Commercial Workers, Local 401*:

> The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society.[10]

This equally applies to accessing the internet as an expression of liberty.

15. As Justice Veldhuis held in her dissenting reasons, interpreting constitutional protections necessary to ensure this sort of privacy for citizens requires adopting a normative approach.[11] The

[6] *R. v. Bykovets*, 2022 ABCA 208 (CanLii), para. 93
[7] *R. v. Jones*, 2017 SCC 60, para. 45
[8] In this respect, using these forms of concealment are the preserve of the tech savvy, a small percentage of the population.
[9] Excluding those activities which the person cannot claim a reasonable expectation of privacy.
[10] 2013 SCC 62 (CanLII), [2013] 3 SCR 733 at para. 19.
[11] *R. v. Bykovets*, at paras. 64-65.

normative approach highlighted by this Honourable Court ties privacy to liberty and ultimately to the notion that persons expect to be free from police monitoring.

16. Nestling traditional s. 8 *Charter* considerations within liberty, as understood in s. 7 *Charter*, illuminates privacy is an essential part of one's liberty.

iii. Conclusion

17. The information revealed in an IP Address is like the information accessed by the use of an IMSI catcher or obtained from a cell tower in that it contains geo-location information as well as the time of access and, in some cases, ISP/mobile carrier information. There is no principled reason why one ought to attract the warrant regime and the other not. Moreover, from a normative perspective, liberty includes accessing the internet without fear that the police will obtain a record (their IP Address) of their internet activity post-hoc without a warrant. Instead, people accept that the police would be entitled to that information once a judge has warranted access. Respectfully, the police should be required to obtain a warrant to obtain IP address and time of access information from third-parties.

PARTS IV & V: COSTS AND ORDER SOUGHT

18. The CCLA takes no position on the disposition of this appeal. The CCLA does not seek costs and asks that no costs be awarded against it.

ALL OF WHICH IS RESPECTFULLY SUBMITTED.

DATED at Toronto, Ontario this 20th day of December 2022.

Anil K. Kapoor
Counsel to the Intervener

Cameron Cotton-O'Brien
Counsel to the Intervener

PART VI: TABLE OF AUTHORITIES

Jurisprudence	**Paragraph(s)**
Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62 (CanLII), [2013] 3 SCR 733	14
R. v. Brewster, 2016 ONSC 4133 (CanLii)	7
R. v. Bykovets, 2022 ABCA 208 (CanLii)	13, 15
R. v. Jones, 2017 SCC 60	13
R. v. Rogers Communications, 2016 ONSC 70 (CanLii)	5, 7
R. v. Spencer, 2014 SCC 43	1, 10
R. v. TELUS Communications Co., 2013 SCC 16	5, 7
Secondary Source	
Look up IP Address Location	1
Legislation	**Section(s)**
Constitution Act, 1982, Schedule B to the Canada Act 1982, 1982, c. 11 (U.K) *Loi Constitutionnelle de 1982*, L'annexe B de la Loi de 1982 sur le Canada, 1982, Ch. 11, (R.-U.)	7, 8 7, 8