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
(Interveners)

FACTUM OF THE INTERVENER, BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

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

PRINGLE CHIVERS SPARKS TESKEY
Suite 1720 – 355 Burrard Street
Vancouver, BC V6C2G8
Telephone: 604-669-7447
Facsimile: 604-259-6171
Email: djsong@pringlelaw.ca

DANIEL J. SONG, K.C.
VIBERT M. JACK
Counsel for the Proposed Intervener,
British Columbia Civil Liberties Association

MCKAY FERG LLP
1800, 639 6th Avenue SW
Calgary, Alberta, T2P 0M9
Telephone: 403-984-1919
Facsimile: 1-844-895-3926
Email: sarah@mckayferg.com

SARAH RANKIN
IAN MCKAY
HEATHER FERG
Counsel for the Appellant

POWER LAW
Suite 701, 99 Bank Street
Ottawa, Ontario, K1P 6B9
Telephone: 613-907-5652
Fax: 613-907-5652
Email: jlaxer@powerlaw.ca

JONATHAN LAXER
Ottawa Agent for the Counsel of the Appellant

ALBERTA CROWN PROSECUTION SERVICE - Appeals Branch
300, 332 - 6th Avenue SW
Calgary, Alberta, T2P 0B2
Telephone: 403-297-8444
Facsimile: 403-297-4311
Email: rajbir.dhillon@gov.ab.ca

RAJBIR DHILLON
Counsel for the Respondent

GOWLING WLG (CANADA) INC.
Suite 2600 – 160 Elgin Street
Ottawa, Ontario, K1P 1C3
Telephone: 613-786-8695
Facsimile: 613-788-3509
Email: lynne.watt@gowlingwlg.com

D. LYNNE WATT
Ottawa Agent for the Counsel of the Respondent

PUBLIC PROSECUTION SERVICE OF CANADA
Suite 1400, Duke Tower
5251 Duke Street
Halifax, Nova Scotia, B3J 1P3
Telephone: 902-426-2285
Facsimile: 902-426-1351
Email: david.schermbrucker@ppsc-sppc.gc.ca

DAVID W. SCHERMBRUCKER
ALLYSON RATSOY
Counsel for the Director of Public Prosecutions

DIRECTOR OF PUBLIC PROSECUTIONS
160 Elgin Street
12th Floor
Ottawa, Ontario, K1A 0H8
Telephone: 613-957-4770
Facsimile: 613-941-7865
Email: francois.lacasse@ppsc-sppc.gc.ca

FRANCOIS LACASSE
Ottawa Agent for the Director of Public Prosecutions

KAPOOR BARRISTERS
161 Bay Street, Suite 2900
Toronto, Ontario, M5J 2S1
Telephone: 416-363-2700
Facsimile: 416-363-2787
Email: akk@kapoorbarristers.com

ANIL K. KAPOOR
CAMERON COTTON O'BRIEN
Counsel for the Canadian Civil Liberties Association

SUPREME ADVOCACY LLP
340 Gilmour Street, Suite 100
Ottawa, ON K2P 0R3
Telephone: 613-695-8855
Facsimile: 613-695-8580
E-mail: mfmajor@supremeadvocacy.ca

MARIE-FRANCE MAJOR
Agent for Counsel for the Canadian Civil Liberties Association

ATTORNEY GENERAL OF BRITISH COLUMBIA
Criminal Appeals and Special Prosecutions
3rd Floor, 940 Blanshard Street
Victoria, BC V8W 3E6
Telephone: 778-974-3344
Facsimile: 250-387-4262
Email: micah.rankin@gov.bc.ca

MICAH B. RANKIN
ROME CAROT
MICHAEL BARRENGER
Counsel for the Attorney General of British Columbia

ATTORNEY GENERAL OF ONTARIO
720 Bay Street, 10th Floor
Toronto, Ontario M7A2S9
Telephone: 416-327-5990
Facsimile: 416-326-4656
Email: jeremy.streeter@ontario.ca

JEREMY STREETER
ANDREW HOTKE
Counsel for the Attorney General of Ontario

GOWLING WLG (CANADA) INC.
Suite 2600 – 160 Elgin Street
Ottawa, Ontario, K1P 1C3
Telephone: 613-786-0211
Facsimile: 613-788-3573
Email: matthew.estabrooks@gowlingwlg.com

MATTHEW ESTABROOKS
Ottawa Agent for the Counsel for the Attorney General of British Columbia

TABLE OF CONTENTS

PARTS I & II: OVERVIEW AND INTERVENER'S POSITION ON APPEAL

1. Informational privacy includes both anonymity and the choice to control that anonymity.[1] Without judicial oversight, third-party private corporations have the power to displace individual agency and decide whether and when to uncover anonymity to facilitate police investigations. This Court's normative approach under s. 8 of the *Charter* should broadly protect informational privacy in the digital sphere *because* of the ubiquity of technology.[2] When internet companies indiscriminately store troves of our personal data and wield the discretion to collaborate with the state, it challenges the very limits of how we might participate in a free and open society.

2. Without taking any position on the outcome of this case, the British Columbia Civil Liberties Association (BCCLA) intervenes to offer the following three points on whether there is a reasonable expectation of privacy in an IP address:

a) The European Union classifies IP addresses as "personal data" because it can *indirectly* reveal a person's identity, which is consistent with our normative approach to privacy;

b) The power imbalance between individuals and third-party companies leads to individuals ceding some privacy to gain access to the internet, but without surrendering *control* over their anonymity; and,

c) Third-party companies may have the discretion to provide information to the police, thereby allowing corporate interests to augment police power and delineate the boundaries of privacy.

3. The BCCLA submits that these points militate in favour of this Court finding that an IP address does attract a reasonable expectation of privacy. Only on its surface is an IP address a string of meaningless numbers. In reality, an IP address can be revelatory, tracing a history of exploration, contemplation, and rejection that helped form someone's identity. In a society that

---

[1] ***R. v. Spencer***, 2014 SCC 43 at paras 27, 34, 38-46 (**Book of Authorities ["BOA"], Tab 2**).
[2] Renee Pomerance, "Flirting with Frankenstein: The Battle between Privacy and our Technological Monsters" (2016) 20:2 C.C.L.R. 149 at 156.

values liberty and autonomy, that history should remain free from the unblinking stare of the state.

PART III: STATEMENT OF ARGUMENT

I. THE NORMATIVE APPROACH TO PRIVACY AND ONLINE ANONYMITY

A. Privacy and IP Addresses in Other Jurisdictions

4. Other jurisdictions have diverged in their treatment of IP addresses in their privacy laws. The European Union, for example, considers IP addresses as "personal data" because they are capable identifying individuals, albeit indirectly. On the other hand, appellate courts in the United States have not recognized a privacy interest in IP addresses on account that individuals relinquish control over them to third parties. The European view that IP addresses are personal data is consistent with the normative approach under s. 8, while the categorical application of third-party control in American cases conflicts with this Court's jurisprudence which has consistently rejected a "risk approach."[3]

5. In ***Breyer v. Bundesrepublik Deutschland***,[4] the Court of Justice of the European Union (CJEU) expanded the definition of "personal data" in Article 2(a) of the European Parliament's Directive 95/46/EC to include IP addresses. Article 2(a) defined "personal data" as the following:

> "Personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;[5]

6. Mr. Breyer sought an order preventing Germany (or third parties) from storing dynamic IP addresses after he accessed state-run websites. The CJEU accepted that a dynamic IP address, alone, did not directly reveal the identity of a person. But because Article 2(a) of Directive 95/46

---

[3] See Steven Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014) 67 S.C.L.R. 505 at 517, and Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011) 54 S.C.L.R. 335 at 339-341. See, also, ***R. v. Dyment***, [1988] 2 S.C.R. 417 at 429-30; ***R. v. Marakah***, 2017 SCC 59 at paras 40 and 41.

[4] ***Breyer v. Bundesrepublik Deutschland*** (Case C-582/14), ECLI:EU:C:2016:779.

[5] *Ibid* at para 5 (emphasis added).

defined personal data as including data that *indirectly* allows a person to be identified, it did not matter that additional subscriber information from an Internet Service Provider (ISP) was needed to identify the user.[6]

7. Furthermore, although the Advocate General argued that there would be "a disproportionate effect in terms of time, cost and man-power" to obtain additional data from an ISP, the CJEU held that there were legal means to obtain additional data from the ISP to identify the user.[7] In other words, there were reasonable means through which an IP address could reveal the identity of the user with *the assistance* of the ISP and competent authority (e.g. the police).[8] In the result, a dynamic IP address constituted "personal data" in these circumstances.

8. This broader view of how an IP address can tend to identify a person stands in contrast with the reasons of the majority of the Alberta Court of Appeal. The expert evidence in this case established that companies like Google or Facebook can identify a person by examining an IP address and the internet activity associated to it. But the majority appeared to discount this evidence because it was predicated on the "assumption" that the police could access the information logged in the third-party company's website.[9] Unlike Velduis J.A. in this case[10] or the CJEU in ***Breyer***, the majority did not appear to ask whether an IP address *tends to reveal* personal information.

9. As a result of ***Breyer***, the EU's *General Data Protection Regulation* (*GDPR*) now includes "online identifiers" under the definition of "personal data."[11] And the European Commission specifically lists an IP address as an example of personal data — along with names and surnames, home addresses, and location data.[12]

10. The United Kingdom has yet to specifically address whether a person has a reasonable expectation of privacy in an IP address. But the UK is still bound by the CJEU and has also

---

[6] *Ibid* at paras 40-44.
[7] *Ibid* at paras 46-47.
[8] *Ibid* at paras 47-48.
[9] ***R. v. Bykovets***, 2022 ABCA 208 at para 13 ["***Bykovets*** ABCA"]
[10] *Ibid* at para 74.
[11] *General Data Protection Regulation*, "Definitions," Art. 4(1).
[12] European Commission, *What is personal data?* (n.d.) online: Official Website of the European Union

adopted the EU's *GDPR* in its own *Data Protection Act 2018*. The Act includes a definition of "personal data" under section 3(3) that strongly resembles Article 4 of the *GDPR* by incorporating protection against the *indirect* identification of an individual by reference to an online identifier.[13] And unlike the majority in this case, which disagreed that an IP address was analogous to a house address,[14] the England and Wales Court of Appeal has held that browser generated information (including an IP address) provided insight about "the user's (virtual) address" and "when the user is at his or her (virtual) home."[15]

11. The US Supreme Court has yet to consider whether an individual has a privacy interest in an IP address. However, US appellate courts have repeatedly concluded that the police do not need a search warrant to obtain an IP address *or* ISP subscriber information (unlike this Court's decision in ***Spencer***).[16] Critically, these courts applied the US Supreme Court's "third-party doctrine," where "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," even for limited purposes.[17] Not surprisingly, by applying that logic, the 11th Circuit Court *did* find a reasonable expectation of privacy in an IP address because the person had taken steps to keep his IP address *concealed*.[18]

12. This line of American authorities relying on the third-party doctrine is unhelpful. This Court has rejected such a categorical approach and has not wavered from the view that the lack of control over information is *not* fatal to an individual's privacy claim.[19] The European Court of Human Rights has also held that the failure to "hide" an IP address is not decisive in assessing the reasonableness of a subjective expectation of privacy.[20] And even Justice Sotomayor has

---

[13] *Data Protection Act 2018* (United Kingdom), 2018 c. 12, s. 3(3).
[14] ***Bykovets* ABCA**, *supra* note 9, at para 19.
[15] ***Google Inc. v. Vidal-Hall, et al.***, [2015] EWCA Civ 311 at para 115 (emphasis added).
[16] See, e.g., ***State v. Mixton***, Case No. CR-19-0276-PR (Sup. Ct. Ariz. 2021); ***United States v. Trader***, USCA11 Case: 17-15611 (11th Cir.); ***United States v. Soybel***, No. 19-1936 (7th Cir. 2021); ***United States v. Ulbricht***, No. 15-1815 (2nd Cir. 2017). Australia may also permit access to IP addresses without a warrant: ***R. v. Daly***, [2021] SADC 131; ***Privacy Commissioner v. Telstra Corporation Ltd***., [2017] FCAFC 4.
[17] ***Carpenter v. United States***, 138 S. Ct. 2206 (2018) at p 9.
[18] ***United States v. Taylor***, 935 F.3d 1279 (11th Cir. 2019).
[19] See ***R. v. Cole***, 2012 SCC 53 at paras 54 and 58; ***Spencer***, *supra* note 1, at paras 46 and 62; ***Marakah***, *supra* note 3, at para 38; ***R. v. Jones***, 2017 SCC 60 at paras 40-45.
[20] ***Benedik v. Slovenia***, No 62357/14, [2018] IV ECHR at para 116.

recognized that the third-party doctrine is "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[21]

13. While the Fourth Amendment protects people and not places,[22] given the textual differences in US rights instruments and the distinct history of the United States, courts must exercise "the greatest of caution" before transplanting American decisions into the Canadian context.[23] The *Charter* is, of course, a broad and purposive document "capable of growth and expansion within its natural limits."[24] Adopting the rationale of the American third-party doctrine with respect to informational privacy would not only conflict with this Court's s. 8 jurisprudence, but would also stunt the *Charter*'s potential to meet society's expectations and aspirations as they shift over time.

14. Thus, the EU's acceptance that IP addresses are personal data because they can indirectly identify individuals is consistent with our normative approach to privacy. Justice Pomerance might agree, having said that "[p]rivacy is defined, not only by the information sought by law enforcement, but also by the inferences and uses that flow from that information."[25] Seen from this perspective, an IP address is much more than a string of "meaningless" numbers. It *tends* to reveal a person's identity and associated pattern of online conduct, which are undeniably part of an individual's "biographical core."

B. Power Imbalances and the Privacy Paradox

15. The fact that individuals generally access the internet without attempting to mask their IP addresses should have little bearing on the s. 8 analysis in this case. One of the confounding effects of society's expectations in the digital sphere is the so-called "privacy paradox." This

---

[21] ***United States v. Jones***, 565 U.S. 400 (2012).
[22] ***Katz v. United States***, 389 U.S. 347 (1967).
[23] ***Hunter v. Southam Inc.***, 1984 CanLII 33 (SCC) at 154-55 and 161.
[24] *Ibid* at 156.
[25] Pomerance, *supra* note 2, at 157 (emphasis added).

paradox captures the apparent discrepancy between consumers' desire for strong privacy protections and consumers' actual choices which do not appear to prioritize privacy.[26]

16. Justice Pomerance (writing extra-judicially) has observed that we have willingly conceded our privacy interests in pursuit of convenience, communication, and connection: we *want* the convenience of being able to locate a great cheeseburger, to track and locate our thoughts and movements with our friends on Facebook and Twitter, and to engage with the latest smart technologies in our homes.[27] We embrace technology to fuel our preoccupation with both notoriety and anonymity — our desire to be, at once, visible and hidden.[28]

17. Similarly, Professor Penney frames this in terms of market forces, pointing out that the market would respond accordingly if consumers actually prioritized their privacy.[29] Instead, the current market simply reflects our acquiescence in existing norms.

18. This paradox invites us to consider the apparent erosion of privacy through a *relational* lens, as opposed to focusing strictly on the technology itself (and bits of information). In other words, the issue of whether an expectation of privacy is reasonable should account for the relative power imbalance between the individual consumer and the companies that necessarily facilitate participation in an increasingly virtual society. Informational asymmetries (along with our cravings for convenience) may impair our ability to make truly informed choices during our interactions with digital platforms:

> [I]f consumers are not adequately informed about how their user data is collected, used and disclosed, and if consumers do not have sufficient control in deciding whether to give up their user data, their behaviours in using digital platforms may not accurately reflect consumers' decisions or their individual privacy preferences.[30]

19. For example, companies invariably offer consumers a standard set of contractual terms on a "take-it-or-leave-it" basis, often leaving them with little or no ability to negotiate terms that

---

[26] Australian Competition & Consumer Commission, "Digital Platforms Inquiry: Final Report," (June 2019) at 384 ["Australian Commission Final Report"].
[27] Pomerance, *supra* note 2, at 154-155.
[28] Pomerance, *supra* note 2, at 155.
[29] Penney, *supra* note 3, at 526.
[30] Australian Commission Final Report, *supra* note 27, at 384.

grant platforms extensive rights to collect, use, and disclose user data.[31] Professor Penney has questioned whether consumers have much bargaining power given the uniformity, length, complexity, and frequent amendment of those terms.[32] In ***Ward***, Doherty J.A. recognized that internet service providers could unilaterally set the terms of the agreement and related documents through a "classic" contract of adhesion, leaving the customer no choice but to agree to the terms in order to access the service.[33] And this Court recently observed in ***Ramelson*** that data collection often occurs "without a user's awareness or consent."[34] If consumers are unaware of how their data is collected, used, and disclosed, then these power imbalances deepen and distort their ability to provide any meaningful consent to release information.

20. In this case, contractual (and statutory) privacy frameworks did not factor into the appellant's record or submissions in the courts below.[35] But notably, just as the existence of these frameworks does not defeat an individual's reasonable expectation of privacy, *neither does their absence*.[36]

21. In addition, the inherent imbalance in this case is that individuals *must* use an IP address to access the internet and participate freely in modern society. If our ability to maintain control over access to our personal information is a facet of privacy linked to personal autonomy,[37] then the normative approach requires courts to accept that disclosing one's IP address while surfing the internet is not truly voluntary. Viewed in this way, even after accessing services through the internet, we should expect to decide for ourselves whether IP addresses should be shared with others. We cannot settle for the *illusion* of control.

C. Corporate Interests Augmenting State of Power

22. Even where an individual may have ceded some control over private information for *non-law enforcement* purposes, that individual should reasonably expect that this information will not

---

[31] Australian Commission Final Report, *supra* note 27, at 395 and 397.
[32] Penney, *supra* note 29 at 526.
[33] ***R. v. Ward***, 2012 ONCA 660 at paras 52 and 106.
[34] ***R. v. Ramelson***, 2022 SCC 44 at para 48.
[35] ***R. v. Bykovets***, 2020 ABQB 70 at para 60.
[36] ***Spencer***, *supra* note 1, at para 54; ***Jones***, *supra* note 20, at para 51.
[37] ***R. v. Jarvis***, 2019 SCC 10 at paras 134-135, per Rowe J., in dissent (but not on this point).

be divulged to the police.[38] For instance, Fish J. in ***Cole*** held that the school board's acquisition of Mr. Cole's laptop "*for its own administrative purposes* did not vest in the police a delegated or derivative power to appropriate and search the computer *for the purposes of a criminal investigation*."[39] To hold otherwise, warned La Forest J. in ***Duarte***, would be to "annihilate any expectation that our communications will remain private."[40]

23. In this case, the police simply contacted Moneris and, in turn, Moneris provided two IP addresses. In this way, private corporations have the discretion *to expand state power* by choosing to collaborate with the police. Justice Veldhuis held that the trial judge failed to consider that the police could approach third-parties and obtain IP addresses without a warrant, allowing them to gather "digital breadcrumbs" about an internet user and *disincentivizing* them from obtaining warrants to learn the same information through the ISP.[41]

24. This "disincentivizing" of seeking warrants is a serious risk to individual privacy and civil liberties. These third parties are often large multinational corporations with resources to hold onto information about us indefinitely. They are not community neighbours making fleeting observations from the windows of their homes. Internet companies possess disquieting power because of the exponentially growing volume of data they can store and analyze.[42]

25. It is important to point out that the concern in this context is not simply that technology permits the vast collection of information, but also that technology enables the *exchange, collation, and synthesis* of information to reveal new insights. In this way, an IP address can indeed create an "electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet."[43] An IP address tends to reveal a vivid, enduring, and potentially compromising portrait of an individual.

---

[38] Kate Robertson, Cynthia Khoo, Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto, at pp 75-76.
[39] ***Cole***, *supra* note 20, at para 67 (italics in original).
[40] ***R. v. Duarte***, 1990 CanLII 150 (SCC) at 44.
[41] ***Bykovets*** **ABCA**, *supra* note 9, at para 70.
[42] ***Spencer***, *supra* note 1 at para 46.
[43] ***R. v. Morelli***, 2010 SCC 8 at para 3; See, also, Office of Privacy Commissioner of Canada, "What an IP Address Can Reveal About You," (May 2013)

26. Justice Iacobucci (writing extra-judicially) stressed that, while the collection of information confined to specific uses and isolated databases poses relatively little threat to privacy, it is ultimately the consolidation, augmentation, and pooling of that information by private companies that may produce the greatest negative impacts.[44] This is compounded by the fact that companies not only compile these pervasive histories and profiles for extended periods of time, they also do so at never before seen rates.[45] As Karakatsanis J. recently observed in ***Ramelson***, internet traces "can spread with prodigious speed and reach, making it still more likely those traces will persist. And they can be compiled, dissected and analyzed to lend new insights into who we are as individuals or populations."[46]

27. This is how third-party corporations can influence the scope of police power. Professor Lisa Austin describes these corporate entities as potential "technological tattletales" that cooperate with the police and thereby "augment state power."[47] They are not ordinary citizens that might offer witness accounts to the police: "[t]he nature of the information held by intermediaries is not mediated by the frailties of human memory or individual relationships, and is centralized, digitized, and structured data."[48] As in this case, law enforcement often simply asks these third-party companies for information, such as an IP address. That IP address is connected to unfiltered information capable of directly identifying the internet user through data held by third-party companies. Corporate (rather than individual) choice amplifies the power of the police to obtain *what they are looking for*—by giving them access to "more information, more useful information, and more accurate information than when information is dispersed within a community."[49] And just because this information is in the hands of third parties does not mean the police should freely access it for their own purposes.[50]

---

[44] The Honourable Frank Iacobucci, "Recent Developments Concerning Freedom of Speech and Privacy in the Context of Global Communications Technology" (1999) 48 Law and Social Policy 189 at p 198-199.
[45] Iacobucci, *supra* note 46 at p 200-201; and Pomerance, *supra* note 2 at p 154.
[46] ***Ramelson***, *supra* note 35, at para 48.
[47] Lisa M. Austin, "Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints" (2016) 17:2 Theoretical Inq L 451 (**BOA, Tab 1**).
[48] *Ibid* at p 464.
[49] *Ibid*.
[50] Penney, *supra* note 3, at 518; See, e.g., ***R. v. Telus Communications Co.***, 2013 SCC 16 at para 13, and ***R. v. Gomboc***, 2010 SCC 55 at para 34.

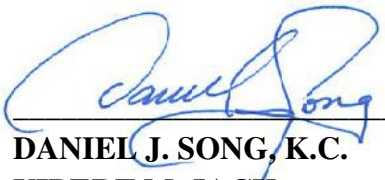
28. If s. 8 of the *Charter* does not protect IP addresses from being disclosed to the police without prior judicial authorization, then the potential identification of an internet user will depend on whether a corporate intermediary *chooses* to cooperate with law enforcement or to safeguard individual privacy.[51] In other words, the envelope of privacy over an IP address would be delineated by corporate interests — interests which should have no bearing on our freedom to control our anonymity.

29. One function of privacy is that it enables us to create a public persona with which we participate in social and political life. If there was no private space, the distinction between the private individual and their public persona would be obliterated, leaving no possibility of distinguishing the two.[52] Given that a person *must* have an IP address to access the internet, there is little choice but to surrender personal histories to third-party corporations in order to participate in modern society. Seen from this perspective, an IP address should be afforded constitutional protection to ensure that our public identities are not distorted by our private activities on the internet. Hence, protecting an IP address under s. 8 of the *Charter* would not only buttress individual control over anonymity. It would also affirm that we value the freedom to leave behind our shortcomings, curiosities, and habits in virtual spaces — so our identities can prosper in public.

PARTS IV & V: COSTS, ORDERS SOUGHT AND CASE SENSITIVITY

30. The BCCLA seeks no costs or orders and makes no submissions on case sensitivity.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 21st day of December 2022.



DANIEL J. SONG, K.C.
VIBERT M. JACK
Counsel for the Intervener, British Columbia Civil Liberties Association

---

[51] Mike Zajko, "Internet Service Providers as Privacy" (2018) 33:3 Can JL & Soc 401 at 405 (**BOA, Tab 3**).
[52] Stewart, *supra* note 3, at 345.

PART VI: TABLE OF AUTHORITIES

CASES

ACADEMIC ARTICLES AND SECONDARY SOURCES

STATUTORY PROVISIONS