SCC Court File No: 37676

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO)

B E T W E E N:

THOMAS REEVES

APPELLANT
(Respondent)

- and -

HER MAJESTY THE QUEEN

RESPONDENT
(Appellant)

- and -

DIRECTOR OF PUBLIC PROSECUTIONS OF CANADA, DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES, ATTORNEY GENERAL OF BRITISH COLUMBIA, CRIMINAL LAWYERS' ASSOCIATION (ONTARIO) AND SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC (CIPPIC)

INTERVENERS

FACTUM OF THE INTERVENER, SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Presser Barristers
116 Simcoe Street, Suite 116
Toronto, Ontario, M5H 4E2

Jill R Presser

Tel: (416)586-0330
Fax: (416) 596-2597
Email: presser@presserlaw.ca

Markson Law Professional Corporation
390 Bay Street, Suite 1000
Toronto, Ontario, M5H 2Y2

Kate Robertson

Tel: (416) 800-0502
Fax: (416) 601-2514
Email: krobertson@marksonlaw.com

Counsel for the Intervener

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tamir Israel

Tel: (613) 562-5800 x 2914
Fax: (613) 562-5417
Email: tisrael@cippic.ca

Agent for the Intervener

TO: THE REGISTRAR

COPY TO: GREENSPAN PARTNERS LLP
144 King Street E.
Toronto, ON M5C 1G8

Brad Greenshields

Tel: (416) 366-3961
Fax: (416) 366-7994
Email: bgreenshields@144king.com

Counsel for the Appellant, Thomas Reeves

AUGER HOLLINGSWORTH
1443 Woodroffe Ave.
Ottawa, ON k2G 1W1

Richard Auger

Tel: (613) 233-4529
Fax: (613) 822-5096
Email: richard.auger@ottawalawfirm.ca

Agent for the Appellant, Thomas Reeves

AND TO: ATTORNEY GENERAL OF ONTARIO
10th Floor, 720 Bay Street
Toronto, ON M5G 2K1

Michelle Campbell

Tel: (416) 326-2411
Fax: (416) 326-4656
Email: michelle.campbell@ontario.ca

Counsel for the Respondent, Her Majesty the Queen

BORDEN LADNER GERVAIS LLP
World Exchange Plaza
100 Queen Street, suite 1300
Ottawa, ON, K1P 1J9

Nadia Effendi

Tel: (613) 237-5160
Fax: (613) 230-8842
Email: neffendi@blg.com

Agent for the Respondent, Her Majesty the Queen

AND TO: BRAUTI THORNING ZIBARRAS LLP
161 Bay Street, Suite 2900
Toronto, ON M5J 2S1

Michael W Lacy

Tel: (416) 360-2776
Fax: (416) 362-8410
Email: mlacy@btzlaw.ca

Counsel for the Intervener, Criminal Lawyers' Association (Ontario)

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

Marie-France Major

Tel: (613) 695-8855 x 102
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Agent for the Intervener, Criminal Lawyers' Association (Ontario)

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

PUBLIC PROSECUTION SERVICE OF CANADA
160 Elgin Street
Suite 1200
Ottawa, ON K2P 2C4

	James C Martin	**François Lacasse**
	Tel: (902) 426-2484 FAX: (902) 426-1351 E-mail: james.martin@ppsc-sppc.gc.ca	Tel: (613) 957-4770 FAX: (613) 941-7865 Email: flacasse@ppsc-sppc.gc.ca
	Counsel for the Intervener, Director of Public Prosecutions of Canada	**Agent for the Intervener, Director of Public Prosecutions of Canada**
AND TO:	**DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES DU QUÉBEC** 2050, rue Bleury, bureau 6.00 Montréal, QC H3A 2J5	**DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES DU QUÉBEC** 17, rue Laurier, bureau 1.230 Gatineau, QC J8X 4C1
	Ann Ellefsen-Tremblay Nicolas Abran	Sandra Bonanno
	Tel: (514) 873-6493 x 53021 FAX: (514) 873-6475 Email: ann.ellefsen-tremblay@dpcp.gouv.qc.ca	Tel: (819) 776-8111 x 60446 FAX: (819) 772-3986 Email: sandra.bonanno@dpcp.gouv.qc.ca
	Counsel for the Intervener, Directeur des poursuites criminelles et pénales	**Counsel for the Intervener, Directeur des poursuites criminelles et pénales**
AND TO:	**ATTORNEY GENERAL OF BRITISH COLUMBIA** 3rd Floor - 940 Blanshard Street Victoria, BC V8W 3E6	**GOWLING WLG (CANADA) LLP** 160 Elgin Street Suite 2600 Ottawa, ON K1P 1C3
	Daniel M Scanlan	Robert E Houston, QC
	Tel: (250) 387-0284 FAX: (250) 387-4262	Tel: (613) 783-8817 FAX: (613) 788-3500 E-mail: robert.houston@gowlingwlg.com
	Counsel for the Intervener, Attorney General of British Columbia	**Agent for the Intervener, Attorney General of British Columbia**

TABLE OF CONTENTS

PART I. OVERVIEW AND STATEMENT OF FACTS

1. This case considers whether individuals retain a reasonable expectation of privacy in a home, even when cohabiting. The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic ("CIPPIC") submits that they do. In *R. v. Cole*, this Honourable Court unanimously rejected the authority of a third party employer to consent to a search of a work-owned laptop, notwithstanding the employer's shared access to the information on the computer.[1] Even more so than the employer issuing a laptop in *Cole*, cohabitants share access to an array of intimate information regarding each others' private lives. Section 8 mandates a contextual and normative approach to privacy, particularly in relation to a dwelling home.[2] This approach recognizes that individuals may share private information on a limited basis or for particular purposes only, while retaining a freedom to be secure from unreasonable state intrusion. Where the subject matter of a search intrudes an individual's reasonable expectation of privacy, a third party cannot speak on behalf of the right holder. The right holder's *subsisting* expectation of privacy in the home is not for the third party to waive.

2. Even though, in the instant appeal, the Appellant's computer was not searched by the police on the authority of third party consent, the implications of the Court of Appeal's analysis may affect all constitutionally-protected informational privacy interests in a shared home, including household electronic information. Indeed, the Respondent now argues before this Court that certain third party "consent" searches of a home computer should be permissible, despite *Cole*'s application to computers at work and at home.[3] CIPPIC intervenes to request that this Court reaffirm that a third party <u>cannot</u> waive another individual's right to protection against unreasonable state intrusion upon the unique privacy interests found in household electronic information.

3. CIPPIC makes no submissions on the facts of this appeal.

---

[1] *R. v. Cole*, 2012 SCC 53, at paras. 66-79.
[2] *R. v. Law*, 2002 SCC 10 at para. 16; *R. v. Jones*, 2017 SCC 60, at para. 20.
[3] *Cole*, *supra* at para. 2.

PART II. POSITION ON QUESTIONS IN ISSUE

4. CIPPIC submits the following:

i. The Court of Appeal for Ontario erred in extinguishing an individual's reasonable expectation of privacy in a home on the basis of an imputed assumption that a co-resident would have the power to consent to a search of commonly accessible space;

ii. This Honourable Court should reject a "risk analysis" basis for the warrantless search of a shared home. This position is grounded in the extensive informational privacy interests in a home, including the sea of electronic information that is commonly accessible to cohabitants through electronic devices and a shared home Internet connection;

iii. Extinguishing a reasonable expectation of privacy within the home on the basis of common access may have unintended deleterious consequences for victims of technology-facilitated abuse, which should be avoided; and

iv. In the absence of an arrest or exigent circumstances, sections 489(1) and (2) of the *Criminal Code* remain the lawful bases upon which an electronic device may be seized.

PART III. STATEMENT OF ARGUMENT

A. The Court of Appeal's approach to the relevance of shared access to a dwelling home and third party consent is inconsistent with s. 8 jurisprudence

5. CIPPIC submits that the Court of Appeal erred in defining the reasonable expectation of privacy in a home by reference to whether an accused would reasonably expect that a co-resident would have the power to consent to police search of a common space.[4] This approach is inconsistent with *Cole*, and with the purposive approach to s. 8 that led to the rejection of third party consent.

6. With respect, stating that a right holder's reasonable expectation of privacy is cancelled out by an imputed assumption that a third party *could* consent is precisely the same as concluding that third party consent should be valid. According to LaForme J.A., it is unreasonable for *any* individual to expect that a cohabitant would not invite an agent of the state to search the common area of the home.[5] In effect, this holding means that anyone who chooses to cohabitate—whether for financial, romantic, or other reasons—assumes the risk that the state may conduct a warrantless search of the home on the basis of third party consent.

---

[4] *R v Reeves*, 2017 ONCA 365, (*Reeves*, CA Decision), at para. 50.
[5] *Reeves*, CA Decision, at para. 48.

7. This approach is at fundamental odds with the essential character of an informed waiver. It asks whether an individual would *expect* a cohabitant could "consent" to the invasion of privacy, without the right holder ever receiving the informational prerequisites to a valid consent.[6]

8. The rejection of the "risk" of third party consent in *Cole* confirms that shared access to a zone of privacy does not quash the right to s. 8 protection.[7] Individuals who share private information for limited purposes are not deprived of constitutional protection under s. 8.[8] If this is true of a work laptop or a hotel room,[9] it must also be true for a shared home.

9. Contrary to the alternative approach taken by the Manitoba Court of Appeal—which is relied upon by the Respondent—a third party's waiver of her own privacy has no bearing on the right holder's entitlement to constitutional protection.[10] Where the subject matter of the search—*what the police were really after*—targets the right holder's reasonable expectation of privacy, the fact that a third party has her own privacy interests in the zone of privacy says nothing about their authority to waive another individual's s. 8 protection.

10. Respectfully, the alternative approach adopted by the Manitoba Court of Appeal overlooks the most important question of all: Did the *individual asserting the s. 8 claim* have a reasonable expectation of privacy in the subject matter of the search? The approach in *R.M.J.T.* simply asks: did the third party who consented to the search have his or her own privacy in the place? If so, the consent was valid. No inquiry need be made into the accused's s. 8 right at all.[11] This cannot be right. Section 8 requires consideration of the *totality* of the circumstances, not just the circumstances of a third party.

---

[6] *R. v. Borden*, [1994] 3 S.C.R. 145, at p. 162; *R. v. Cole*, *supra*, at para. 78.
[7] *R. v. Dyment*, [1988] 2 S.C.R. 417 at p. 429-430; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wong*, [1990] 3 S.C.R. 36 at pp. 44-49; *Cole*, *supra*, at paras. 58, 75-79; *R. v. Marakah*, 2017 SCC 59, at para 40.
[8] *Dyment*, *supra* at p. 429-430, at para 22; *R v Tessling*, 2004 SCC 67 at para. 23; *R. v. Patrick*, 2009 SCC 17, at para. 26, *R. v. Spencer*, 2014 SCC 43 paras. 17-18, 40; *Cole*, *supra*, at para. 42; *Marakah*, *supra*, at paras. 10, 41.
[9] *R. v. Buhay*, [2003] 1 S.C.R. 631, at paras. 23-24; *R. v. Mercer* (1992), 7 O.R. (3d) 9 (C.A.); *Cole*, *supra*.
[10] See *R. v. R.M.J.T.*, 2014 MBCA 36.
[11] *R.M.J.T.*, *supra*, at para. 46.

11. *Cole* stands for the proposition that, as a third party, the school board could not authorize a search because even though the school shared access and knew the computer's contents, the employee still "retained a reasonable and 'continuous' expectation of privacy in the personal information on his work-issued laptop."[12] The case does not stand for the proposition that the school could not consent to the search because it had no overlapping expectation of privacy. The police required Mr. Cole's consent because the school board's expectation of privacy did not extinguish or replace that of Mr. Cole.

12. The true issue to be determined is not whether someone has "veto power" over the exercise of a cohabitant's common law property rights, as put by the Respondent. This distorts the nature of the constitutional inquiry. Section 8 protects people, not property rights. Rather, the *true issue* is whether individuals retain a reasonable expectation of privacy, even when a cohabitant may waive his or her own protection under s. 8. CIPPIC submits that they do. This flows expressly from *Duarte*, from *Marakah*, and most significantly, from *Cole*. The privacy interests of cohabitants may be overlapping in the place they are found, but their privacy interests are not coextensive. A waiver for one is not a waiver for all. Neither are they mutually exclusive: recognition of the privacy interest of one (even one who is waiving theirs) does not extinguish the expectation of privacy of the others.

13. The rationale supporting the constitutionality of first party consent does not extend to third party consent, even where privacy interests overlap. In *R. v. Buhay*, this Court adopted the reasoning of Arbour J.A. (as she then was) in *R. v. Mercer*, holding that the rationale for a consent search falls away unless the consent comes from the person whose privacy interest is engaged in the subject matter of the search.[13] It was for this reason that in *R. v. Feeney*, this Honourable Court declined even to permit third party consent to *mitigate* the seriousness of a s. 8 breach under section 24(2):

> *Hunter*, *supra*, was clear that an ownership interest is unnecessary in invoking s. 8; what is required is a reasonable expectation of privacy. It would be inconsistent with this emphasis on the expectation of privacy to mitigate the seriousness of the violation based on the consent of the owner of the premises ***rather than the person with the***

[12] *Cole*, *supra*, at para. 72.
[13] *Buhay*, *supra*; *Mercer*, *supra*.

profound expectation of privacy associated with his dwelling house.[14]

14. Affirming this Court's holding in *Cole* would not interfere with the exigencies of policing. No one contests that cohabitants can cooperate with and inform the police of the discovery of contraband in a home.[15] Information provided to police by a co-resident may itself authorize warrantless entry and/or search in exigent circumstances.[16] Section 489(2) also allows for the warrantless seizure (not search) of an item with reasonable grounds to believe that it contains criminal evidence.[17] Further, in *R. v. Godoy*, this Court also addressed the circumstances in which safety concerns will provide the police with a common law power to conduct a warrantless entry and search of a dwelling home.[18] The Respondent asserts that these powers are insufficient because they require more than mere reasonable suspicion. However, CIPPIC submits that third party consent should not be resuscitated just to circumvent the limits of *Criminal Code* powers for warrantless entry into a dwelling home.[19]

B. Shared access must not quash an individual's reasonable expectation of privacy in household electronic information

15. A search of a dwelling home engages informational privacy interests.[20] As a result, the Court of Appeal's reasoning regarding the relevance of joint access is not easily confined to the purely territorial context. As this Court recently reaffirmed in *Marakah*, in determining whether a reasonable expectation of privacy is engaged under section 8, one does not look only at the information revealed in the particular case, but to the search's "potential for revealing private information."[21] The implications of the Court of Appeal's analysis for all informational privacy interests in a home, including household electronic information, may therefore be broad indeed. CIPPIC urges caution.

---

[14] *R. v. Feeney*, [1997] 2 S.C.R. 13, at para. 78.
[15] *Cole*, *supra*, at para. 73.
[16] *R. v. Brilhante* (2001), 83 C.R.R. (2d) 349 at para. 27 (Ont. S.C.J.); *R. v. Paterson*, [2017] 1 S.C.R. 202, at para. 32.
[17] Notably, the provision does not allow for entry into a private place to seize an item.
[18] *R. v. Godoy*, [1999] 1 S.C.R. 311.
[19] See *R. v. Paterson*, [2017] 1 S.C.R. 202 at para. 32.
[20] *Tessling*, *supra*, at para 24; *Patrick*, *supra*, at para 42; *R v. Gomboc*, 2010 SCC 55, at para. 49 per Deschamps J.; *Spencer*, *supra*, at para. 37.
[21] *Marakah*, *supra*, at para. 31-32.

16. CIPPIC submits that an individual's significant privacy interest in household electronic information is not extinguished when they (either knowingly or unknowingly) share access to their private electronic information with a cohabitant or spouse. As this Honourable Court recognized in *R. v. Vu*, household computers engage unique privacy interests.[22] In romantic and cohabiting relationships, individuals have routine access to intimate electronic information about each other that is at the heart of the biographical core of one's private life. Importantly, this "shared" access may occur unbeknownst to one or both parties. Due to the uneven nature of computer literacy, electronic devices are full of cyberspaces that are meaningfully expected to be private, but which are jointly accessible with ease. Whether sharing a computer, a "smart" home device, or a home wireless network, individuals often lack appreciation of the *scope* of their digital footprint, and the ease with which it may be *accessed* by other individuals living under the same roof and sharing the same home network.

17. In *R. v. Wong*, this Court held that the section 8 right must develop along with existing technology at the disposal of law enforcement authorities so as to remain relevant.[23] The proliferation of smart home devices—a ballooning market referred to as 'the internet of things'—also has enormous implications for the amount of information now available in private homes regarding the identities of the individual occupants, their expressive activities and habits, and their comings and goings from the home.[24] These electronic devices have been likened to "extensions to the human body and mind."[25] The expanding use of such devices presents unique privacy issues, as users are unfamiliar with how much data is collected, and expectations of anonymity in the data gathered may be a false hope.[26]

18. In addition to not appreciating the scope of electronic records created, individuals may be even less aware of the ways in which the *anonymity* of their electronic footprint may be undermined

---

[22] *R. v. Vu*, 2013 SCC 60, at para. 1.
[23] [1990] 3 S.C.R. 36 at p. 43-44.
[24] Office of the Privacy Commissioner of Canada, "The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments", February 2016, at p 20
[25] *Ibid*, at pp 16-20.
[26] *Ibid*.

or extinguished. Household electronic information includes not only the *content* of electronic activity (such as the content of a private communication or files saved on a computer), but also *metadata* (data that provides information about other data). This data has the potential to reveal a detailed mosaic of an individual's daily activities, associations, political or religious beliefs, or even an individual's uncommunicated thoughts.[27] The unregulated collection of metadata and other electronic records (recognized by this Honourable Court in *Vu*) may provide through the backdoor what *Spencer* says cannot be gained through the front:

> A computer is, as A. D. Gold put it, a "fastidious record keeper." Word-processing programs will often automatically generate temporary files that permit analysts to reconstruct the development of a file and access information about who created and worked on it. Similarly, most browsers used to surf the Internet are programmed to automatically retain information about the websites the user has visited in recent weeks and the search terms that were employed to access those websites.[28]

19. Metadata forms trails of information revealing even of an individual's thoughts:

> …metadata can sometimes be more revealing than content itself. In the digital age, almost every online activity leaves some sort of a personal trace…. This information represents, in aggregate form, a place holder for the intentions of humankind – a massive database of desires, needs, wants, and likes that can be discovered, subpoenaed, archived, tracked, and exploited to all sorts of ends.[29]

20. The absence (or imbalance) of familiarity with technology thus has important implications for articulating an individual's reasonable expectation of privacy. Individuals may have no appreciation of the extent of the data trails they are leaving behind them, or the extent to which their electronic life is easily accessible to a computer savvy roommate. Due to the Court of Appeal's focus on <u>shared access</u>, in conjunction with a blanket assumption of risk of third party consent, it appears that the state could obtain from a consenting co-resident highly sensitive electronic data in circumstances wholly unforeseen and unforeseeable to the individual right holder. Such records could include, for example: intimately private electronic files that the right holder deleted from a shared home computer, but were

---

[27] *Spencer*, *supra*, at paras. 26, 46.
[28] *Vu*, *supra* at paras. 42-43.
[29] Office of the Privacy Commissioner of Canada, "Metadata and Privacy A Technical and Legal Overview", October 2014, at p. 4.

recovered from the hard drive by a knowledgeable co-resident; or any amount of electronic data that was readily accessible from a *separate* computer by virtue of a shared home network connection.[30]

21. Take the hypothetical of a cohabitant who agrees to act as an informant, and "consent" to the release of his roommate's internet browsing history on their shared computer. Should the right-holder reasonably be expected to assume the risk that their roommate would have the authority to "consent" to provide the state with a running feed of electronic records and metadata about the individual's innermost thoughts, simply because they lived in the same apartment and share a computer? CIPPIC submits that the normative purposes of section 8 are discordant with such a proposition.

22. Anonymous and intimately personal electronic life occurs on a metamorphically new level since *Duarte* was decided. The erosion of privacy that would be occasioned by unregulated electronic surveillance is thus markedly more dangerous to a free and democratic society than it was in 1990. In participating in electronic life, individuals often do not know when records are created, who has access to the records, and whether they are personally identifiable in relation to the records. To deny s. 8 protection because a roommate has shared access does not accord with the expectations of Canadians in the digital age. If the state exercises an unregulated authority to access the sea of electronic information in digital life purely on the basis of third party consent, it leaves individuals unknowing as to when the state will be watching through the electronic walls of their life. This is a risk of precisely the same magnitude that *Duarte* held was wholly unacceptable.

C. The Court of Appeal's approach could have detrimental implications for victims of technology-facilitated abuse perpetrated by domestic partners

23. CIPPIC submits that adopting an approach that extinguishes expectations of privacy within the home on the basis of joint access and third-party consent may diminish the security of persons (including women in particular) who are victimized by technology-facilitated abuse by their intimate partners.[31] Such abuse may arise in the very context of the breakdown of a romantic relationship.

---

[30] *Vu*, *supra*, at paras. 42-43.

[31] Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the

Current legal mechanisms for protection against this form of abuse will inevitably be premised on the principle underlying informational privacy: "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit."[32] Section 162.1 of the *Criminal Code* criminalizes the non-consensual distribution of intimate images, and in so doing, recognizes that an individual may have a reasonable expectation of privacy in images accessible to a domestic partner.[33]

24. If section 8 does not recognize a reasonable expectation of privacy *even against state intrusion* on the basis of common access in a home and third party consent,[34] this would set an unworkable precedent when it comes to policing the borders of privacy vis-à-vis private citizens when things go south in a domestic relationship. As the phenomenon of technology-facilitated abuse becomes better understood by policy makers, the adoption of further legal mechanisms for protection may also require recognition of an individual's reasonable expectation of privacy in relation to their electronic information and devices that are accessible to domestic partners. To adopt an approach that fundamentally limits the scope of that right inside all homes and intimate partnerships risks undermining the dignity and autonomy of persons who are vulnerable to this form of abuse.

D. Third party consent does not authorize the warrantless seizure of an electronic device

25. Individuals have a privacy interest in personal items in their home, including a residual privacy interest in items taken from their home and retained by the state.[35] Depriving an individual of access to his or her electronic device—even without searching the computer prior to judicial

---

United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović, November 7, 2017, accessed online on March 9, 2018; "Technology-facilitated abuse: the new breed of domestic violence", The Conversation, March 26, 2017, accessed online on March 9, 2018.

[32] *Spencer*, *supra*, at para 40; *Dyment*, *supra*, at p 429.

[33] *Criminal Code*, RSC 1985, c C-46, at s 162.1.

[34] In *Duarte*, *Wong*, and *Marakah*, *supra*, this Court recognized that in a free and democratic society, citizens may in fact face risks to privacy from their fellow citizens that they do not reasonably expect from the state. The intrusion upon reasonable expectations of privacy by the *state* uniquely endangers a free and democratic society.

[35] *Law*, *supra* at para. 16; *R v. Garcia-Machado*, 2015 ONCA 569, at paras. 45 and 54.

authorization—can have meaningful consequences for the individual's *Charter*-protected interests. Services available through electronic devices are multiplying prolifically to support mental health; improve the accessibility of cities; and support a range of motor, visual, speech, and auditory impairments. Further, many electronic devices have external screens such that real-time private communications and other information would be easily visible through pop-up notifications to an officer in possession of the device.

26. In *R. v. Vu*, this Court held that while executing a search warrant, the police may seize a computer, pending specific authorization for a search.[36] The Court of Appeal erred in extending *Vu* on the basis of third party consent.[37] It is unclear even on the Court of Appeal's test why one must expect a spouse to give away joint family property. The application of ss. 489(1) **or** (2) of the *Criminal Code* are the lawful bases upon which to authorize the seizure of an electronic device, pending specific authorization to search.[38] Both provisions require reasonable grounds to believe the computer has criminal evidence—as the Court in *Vu* affirmed.[39] LaForme J.A. concluded that such a belief was not available here.[40]

PART IV. SUBMISSIONS ON COSTS

27. CIPPIC does not seek costs and asks that no costs be awarded against it.

PART V. ORDER REQUESTED

28. CIPPIC makes no submission on the ultimate order to be made.

---

[36] *Vu*, *supra* at para 49 [emphasis added].
[37] *Reeves*, CA Decision, at paras. 56-57.
[38] S. 489(1) authorizes the seizure of an item found in executing a search warrant. S. 489(2) permits a warrantless seizure of an item where an officer is lawfully present in a place. Note, this provision cannot be used in a way that constitutes an unconstitutional search. As DiLuca J. held in *R. v. Riccardi*, s. 489(2) is not to be misused as a "roving search warrant": 2017 ONSC 2105, at para 44.
[39] *Vu*, *supra* at para. 49.
[40] *Reeves*, CA Decision, at paras. 92-95.

ALL OF WHICH IS RESPECTFULLY SUBMITTED, this 3rd day of May, 2018.

Jill R. Presser

Presser Barristers
116 Simcoe Street, Suite 116
Toronto, ON M5H 4E2

Tel: (416) 586-0330
Fax: (416) 596-2597
Email: presser@presserlaw.ca

Counsel for the Proposed Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

Kate Robertson

Markson Law Professional Corp
390 Bay Street, Suite 1000
Toronto, ON M5H 2Y2

Tel: (416) 800-0502
Fax: (416) 601-2514
Email: krobertson@marksonlaw.com

Counsel for the Proposed Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

PART VI. TABLE OF AUTHORITIES

Authority		Reference in Argument
	Cases	**para**
1	*R. v. Borden*, [1994] 3 S.C.R. 145, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1174/index.do	7
2	*R. v. Brilhante* (2001), 83 C.R.R. (2d) 349, https://www.canlii.org/en/on/onsc/doc/2001/2001canlii28325/2001canlii28325.html	14
3	*R. v. Buhay*, [2003] 1 S.C.R. 631, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2062/index.do	8, 13
4	*R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/12615/index.do	1-2, 5, 7-8, 11-12, 14
5	*R. v. Duarte*, [1990] 1 S.C.R. 30, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/559/index.do	8, 12, 22, 24
6	*R. v. Dyment*, [1988] 2 S.C.R. 417, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do	8, 23
7	*R. v. Feeney*, [1997] 2 S.C.R. 13, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1508/index.do	13
8	*R. v. Garcia-Machado*, 2015 ONCA 569, https://www.canlii.org/en/on/onca/doc/2015/2015onca569/2015onca569.html	25
9	*R. v. Godoy*, [1999] 1 S.C.R. 311, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1682/index.do	14
10	*R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7898/index.do	15
11	*R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16897/index.do	1
12	*R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1947/index.do	1, 25
13	*R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16896/index.do	8, 12, 15, 24
14	*R. v. Mercer* (1992), 7 O.R. (3d) 9 (C.A.), https://www.canlii.org/en/on/onca/doc/1992/1992canlii7729/1992canlii7729.html	8, 13
15	*R. v. Paterson*, 2017 SCC 15, [2017] 1 S.C.R. 202, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16484/index.do	14

16	*R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7611/index.do	8, 15
17	*R. v. R.M.J.T.*, 2014 MBCA 36, https://www.canlii.org/en/mb/mbca/doc/2014/2014mbca36/2014mbca36.html	9-10
18	*R v Reeves*, 2017 ONCA 365, https://www.canlii.org/en/on/onca/doc/2017/2017onca365/2017onca365.html	5, 6, 26
19	*R. v. Riccardi,* 2017 ONSC 2105, https://www.canlii.org/en/on/onsc/doc/2017/2017onsc2105/2017onsc2105.html	26
20	*R. v. Spencer*, 2014 SCC 43, [2014] 2 SCR 212, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do	8, 15, 18, 23
21	*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2183/index.do	8, 15
22	*R. v. Vu*, 2013 SCC 60. [2013] 3 S.C.R. 657, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13327/index.do	16, 18, 20, 26
23	*R. v. Wong*, [1990] 3 S.C.R. 36, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/683/index.do	8, 17, 24
	Additional Sources	
24	Office of the Privacy Commissioner of Canada, "Metadata and Privacy A Technical and Legal Overview", October 2014, https://www.priv.gc.ca/media/1786/md_201410_e.pdf	19
25	Office of the Privacy Commissioner of Canada, "The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments", February 2016, https://www.priv.gc.ca/media/1808/iot_201602_e.pdf	17
26	Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović, November 7, 2017, accessed online on March 9, 2018, https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf	23
27	"Technology-facilitated abuse: the new breed of domestic violence", The Conversation, March 26, 2017, accessed online on March 9, 2018, http://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683	23