SCC Court File No: 37194

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

B E T W E E N:

TRISTIN JONES

APPELLANT

- and -

HER MAJESTY THE QUEEN IN RIGHT OF CANADA AND HER MAJESTY THE QUEEN IN RIGHT OF ONTARIO

RESPONDENT

- and -

ATTORNEY GENERAL OF BRITISH COLUMBIA, BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION, CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO, DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES DU QUÉBEC, AND SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

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

Counsel for the Intervener

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
FTX102, 57 Louis Pasteur Street
Ottawa, Ontario, K1N 6N5

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
FTX102, 57 Louis Pasteur Street
Ottawa, Ontario, K1N 6N5

Tamir Israel

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

Agent for the Intervener

Tamir Israel
David A. Fewer

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

Counsel for the Intervener

TO: **THE REGISTRAR**

COPY TO:

Fasken Martineau
55 Metcalfe Street, Suite 1300
Ottawa, ON, K1P 6L5

Patrick McCann
Peter Mantas
Ewan Lyttle

Tel: (613) 696-6906
Fax: (613) 230-6423
Email: pmccann@fasken.com

Counsel for the Appellant, Tristin Jones

Supreme Advocacy LLP
340 Gilmour Street, Suite 100
Ottawa, ON, K2P 0R3

Marie-France Major

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

Agent for the Appellant, Tristin Jones

AND TO:

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

Randy Schwartz

Tel: (416) 326-4586
Fax: (416) 326-4656
Email: Randy.Schwartz@ontario.ca

Counsel for the Respondent, Her Majesty the Queen (Ontario)

Burke-Robertson
441 MacLaren Street, Suite 200
Ottawa, ON, K2P 2H3

Robert E. Houston, Q.C.

Tel: (613) 236-9665
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Agent for the Respondent, Her Majesty the Queen (Ontario)

AND TO:

Public Prosecution Service of Canada
130 King Street West
Suite 3400, Box 36
Toronto, ON, M5X 1K6

Nicholas E. Devlin

Tel: (416) 952-6213

Director of Public Prosecutions of Canada
160 Elgin Street, 12th Floor
Ottawa, ON, K1A 0H8

François Lacasse

Tel: (613) 957-4770

	Fax: (416) 952-2116 Email: nick.devlin@ppsc-sppc.gc.ca	Fax: (613) 941-7865 Email: francois.lacasse@ppsc-sppc.gc.ca
	Counsel for the Respondent, Her Majesty the Queen (Canada)	**Agent for the Respondent, Her Majesty the Queen (Canada)**
AND TO:	**Attorney General of British Columbia** 3rd Floor, 940 Blanshard Street Victoria, BC, V8W 3E6	**Burke-Robertson** 441 MacLaren Street, Suite 200 Ottawa, ON, K2P 2H3
	Daniel M. Scanlan	Robert E. Houston, Q.C.
	Tel: (250) 387-0284 Fax: (250) 387-4262	Tel: (613) 236-9665 Fax: (613) 235-4430 Email: rhouston@burkerobertson.com
	Counsel for the Intervener, Attorney General of British Columbia	**Agent for the Intervener, Attorney General of British Columbia**
AND TO:	**Ursel Phillips Fellows Hopkinson LLP** 555 Richmond Street West, Suite 1200 Toronto, ON, M5V 3B1	**Supreme Advocacy LLP** 340 Gilmour St, Suite 100 Ottawa, ON, K2P 0R3
	Susan M. Chapman	Marie-France Major
	Tel: (416) 969-3061 Fax: (416) 968-0325 Email: schapman@upfhlaw.ca	Tel: (613) 695-8855 Ext 102 Fax: (613) 695-8580 Email: mfmajor@supremeadvocacy.ca
	Counsel for the Intervener, Criminal Lawyers' Association of Ontario	**Agent for the Intervener, Criminal Lawyers' Association of Ontario**
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** Palais de justice, 17 rue Laurier, Bureau 1.230 Gatineau, QC, J8X 4C1
	Ann Ellefsen-Tremblay	Emily K. Moreau
	Tel: (514) 873-6493 Ext 53021 Fax: (514) 873-6475 Email: ann.ellefsen-tremblay@dpcp.gouv.qc.ca	Tel: (819) 776-8111 Ext 60412 Fax: (819) 772-3986 Email: emily-k.moreau@dpcp.gouv.qc.ca
	Counsel for the Intervener, Directeur des poursuites criminelles et pénales du Québec	**Agent for the Intervener, Directeur des poursuites criminelles et pénales du Québec**

AND TO:

Stockwoods LLP TD North Tower, Toronto-Dominion Centre 77 King Street West, Suite 4130 Toronto, ON, M5K 1H1	**Power Law** 130 Albert Street, Suite 1103 Ottawa, ON, K1P 5G4
Gerald Chan Nader R. Hasan	David Taylor
Tel: (416) 593-1617 Fax: (416) 593-9345 Email: geraldc@stockwoods.ca	Tel: (613) 702-5563 Fax: (613) 702-5563 Email: dtaylor@powerlaw.ca
Counsel for the Intervener, British Columbia Civil Liberties Association	**Agent for the Intervener, British Columbia Civil Liberties Association**

AND TO:

McCarthy Tétrault LLP Toronto Dominion Bank Tower Box 48, Suite 5300 Toronto, ON, M5K 1E6	**Conway Baxter Wilson LLP** 400-411 Roosevelt Avenue Ottawa, ON, K2A 3X9
Christine Lonsdale	Colin S. Baxter
Tel: (416) 601-8019 Fax: (416) 868-0673 Email: clonsdale@mccarthy.ca	Tel: (613) 780-2012 Fax: (613) 688-0271 Email: cbaxter@conway.pro
Counsel for the Intervener, Canadian Civil Liberties Association	**Agent for the Intervener, Canadian Civil Liberties Association**

TABLE OF CONTENTS

PART I – OVERVIEW

1. In the instant appeal, this Honourable Court is called upon to ensure that privacy protections are not left behind by changes in communications technologies and digital interactions.

PART II – POSITION ON APPELLANTS' QUESTIONS

2. The Intervener respectfully submits that the Courts below erred in underestimating the high expectations of privacy that individuals retain in text-based communications sent to other individuals.

PART III – STATEMENT OF ARGUMENT

3. Reasonable expectations underpinning constitutional protections must be assessed in a normative manner to secure privacy protections in light of rapidly evolving communications technologies.[1] As elaborated below, control, risk exposure, confidentiality and access are inter-related concepts that require a careful, contextual and purposive application to modern communications technologies.

A. The normative approach must be applied to fully realize the objectives of section 8

4. This Court has repeatedly recognized that the reasonable expectation of privacy standard is normative, not descriptive or empirical. The normative inquiry into privacy expectations is "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[2] The normative approach is flexible and purposive, keeping the values underpinning section 8 as its focus and avoiding "narrow legalistic classifications.[3] Fundamentally, this requires asking what individuals *should* be able to expect in a free and democratic society, not what they currently *can* expect, as a question of fact.

B. Normative analysis recognizes privacy in text-based communications

5. Electronic communications have always engaged a high level privacy, and this has only become more so as digital interactions have been placed at the core of our daily lives. In finding no subjective or objective expectation of privacy, emphasis has been placed on the lack of testimony by the accused on his relationship to the communications in question,[4] the fact that the text messages were under TELUS'

---

[1] *R v Wong*, [1990] 3 SCR 36, p 44, "... the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take."; See also *R v Tessling*, 2004 SCC 67, paras 54-55.

[2] *R v Patrick*, 2009 SCC 17, para 14; *R v Spencer,* 2014 SCC 43, para 18; *R v Tessling,* 2004 SCC 67, para 42.

[3] *R v Duarte*, [1990] 1 SCR 30, para 19; *R v Spencer,* 2014 SCC 43, para 15: "This court has long emphasized the need for a purposive approach to s.8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfillment and autonomy as well as the maintenance of a thriving democratic society."

[4] *R v Jones*, [2012] OJ No 6508 (ONCJ), para 24. Canada Respondent, para 23: (defendant erroneously advances "a right to challenge the admissibility of the texts without having to admit the texts were his.").

control and produced from TELUS' office without "intrusion upon the property of the Applicant[]", the lack of a proven contractual relationship between the defendant and TELUS or the unknown recipient of the text messages, the lack of proactive measures adopted by the defendant for the purpose of protecting his privacy,[5] and the view that the subject matter in question was not "deeply personal", particularly so where such messages pertain to criminal matters.[6]

6. If adopted, this framework would erode privacy in electronic communications by undermining key principles that are integral to constitutional protections in advanced communications networks.

(i) Text-based communications constitute deeply private subject matter

7. Respectfully, the courts below mis-identified the subject matter that is at issue in this appeal. As a result, the decisions below fail to account for the sensitive nature of SMS text communications, and of electronic communications more generally. The characterization of electronic SMS communications as 'mundane' is simply insupportable in light of the 'deeply private' manner in which individuals use text messaging. Treatment of such communications as less private is inconsistent with this Court's historic jurisprudence and can result in an undesirable 'chill' on the use of communications technologies.

8. Properly characterizing the subject matter is integral to "identify[ing] ... the privacy interests that were engaged" in a given context and, by extension, what privacy expectations a particular search might implicate.[7] In characterizing implicated text messages as mundane in character, the courts below focused on the criminal character of the particular exchanges captured in the specific text messages captured by the search.[8] Doing so inappropriately characterizes the subject matter of a search by the criminal nature of the specific communications placed in evidence, in contravention of long-standing section 8 principles.[9] It further erroneously adopts a reductionist assessment of the subject matter at issue which obscures the broader social value of text messaging and electronic communications implicated by the search. The subject matter of the search must look beyond the specific information obtained as a result of a particular search to encompass what such searches are

[5] *R v Jones*, [2012] OJ No 6508 (ONCJ), para 31.

[6] *R v Marakah*, 2016 ONCA 542, para 63 ("We are also not dealing with deeply personal, intimate details going to the appellant's biographical core. Here, we are talking about text messages ... that reveal no more than what the messages contained – discussions regarding the trafficking of firearms."), adopted by reference in *R v Jones*, 2016 ONCA 543, para 18.

[7] *R v Spencer*, 2014 SCC 17, para. 22.

[8] *R v Marakah*, 2016 ONCA 542, para 63.

[9] A principle recently affirmed in *R v Spencer*, 2014 SCC 43, para 36: "The nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. ... the issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes."

generally likely to reveal.[10] It is simply incorrect to classify the subject matter at issue as "discussions regarding the trafficking of firearms" while ignoring all the other implicated information that individuals send to others by means of text messaging.

9. While not every single text message sent will disclose sensitive information, many will.[11] This can, and often does, regularly include intimate text-based exchanges between individuals,[12] extensive interactions comprising dozens of exchanges – in essence a 'running conversation,[13] and even intimate images.[14] Text messaging is increasingly used to transmit often sensitive medical information,[15] for suicide crisis management,[16] and even to provide secondary authentication as a supplement to password-based access to accounts and devices.[17] Mobile commerce, including m-Payments and m-Banking and donations to charitable programs, are also carried out over text-messaging.[18] An increasingly sophisticated ecosystem of 'chat bots' are bringing computing-like functionality to SMS messaging by allowing users to issue instructions to computer programs by means of SMS.[19]

10. Prior to obtaining 'sent' text messages from a recipient's account, law enforcement will not know whether the content of these messages includes these sensitive and private communications. A decision affecting the constitutional privacy protections available to senders of text messages would affect *all* text messaging, chilling the use of this entire sub-set of private communications.[20] It is for this reason that the private

---

[10] *R v Spencer*, 2014 SCC 17, paras 25-26: "[I]n characterizing the subject matter of the alleged search, it is important to look beyond the "mundane" subscriber information such as name and address. The potential of that information to reveal intimate details of the lifestyle and personal choices of the individual must also be considered."; *R v Vu*, 2013 SCC 60, para 41: "computers store immense amounts of information, some of which ... will touch the 'biographical core of personal information' referred to by this Court in *R v Plant*." (emphasis added)

[11] *R v Rogers Communications*, 2016 ONSC 70, para 20; *R v Vye*, 2014 BCSC 93, para 6.

[12] *R v Vye*, 2014 BCSC 93, paras 6, 50-51.

[13] *R v Mann*, 2014 BCCA 231, paras 70-71; *R v TELUS Communications Co*, 2013 SCC 16, per Abella, J, paras 1, 5 ("...text messaging has become an increasingly popular form of communication. Despite technological differences, text messaging bears several hallmarks of traditional voice communication: it is intended to be conversational, transmission is generally instantaneous, and there is an expectation of privacy in the communication. ... Text messaging is, in essence, an electronic conversation. The only practical difference between text messaging and the traditional voice communications is the transmission process.")

[14] *JS v MM*, 2016 ONSC 3072, para 3. Canadian Wireless Telecommunications Association, Canadian Common Short Code – Application Guidelines, Ver 3.0, March 2015, p 7: "MMS means Multi Media Service, which is a standard for telephony messaging systems that enable the sending of messages between mobile devices that includes multimedia objects (images, audio, video)."

[15] World Health Organization, "mHealth: New Horizons for Health Through Mobile Technologies", *Global Observatory for eHealth Series*, Vol 3, (World Health Organization, 2011), p 23-24 and 26: ("The United States reported an SMS-based initiative to promote HIV/AIDS testing as well. By sending their zip code to the SMS shortcode3 KNOWIT, users receive a text message with the address to the nearest HIV/AIDS testing centre.").

[16] Sofian Berrouiguet, *et al*, "Post-acute crisis text messaging outreach for suicide prevention: A pilot study", (2014) 217(3) *Psychiatry Research* 154; Brian Rinker, "Meeting Teens Where They Are: Suicide Prevention by Text Message", September 16, 2014, *Oakland North*.

[17] United States Department of Commerce, National Institute of Standards and Technology, "Digital Identification Guidelines: Authentication and Lifecycle Management", DRAFT NIST Special Publication 800-63B.

[18] CWTA, Canadian Common Short Code – Application Guidelines, V3.0, March 2015, pp 27-31.

[19] Sarah Mitroff, "No Download Needed: The Rise of Chatbots", May 3, 2016, CNET.com.

[20] *R v Taylor*, [1990] 3 SCR 892, paras 76-77: "... s. 13(1) works to suppress private communications, demonstrating an extensive and serious intrusion upon the privacy of the individual. ... I do not disagree with the view that telephone conversations are usually intended to be private; it is

communications which constitute the subject matter of this appeal have enjoyed a high measure of protection. This is reflected in the criminalization of unauthorized interception of such private communications.[21] CIPPIC therefore respectfully submits that a proper identification of the implicated subject matter as 'text messaging' as opposed to 'criminal communications' leads to the inevitable conclusion that, other factors being equal, the search in question implicated deeply private subject matter.

(ii) Search in question compromises a significant informational privacy interest

11. In the instant appeal, the Court is being called upon to adopt an inflexible 'all or nothing' approach to informational privacy interests which is inconsistent with its historic jurisprudence and threatens to leave significant amounts of deeply private activity outside the protective scope of section 8. By focusing on narrow technical elements of the search, the approach in question additionally obscures the extent to which the values and interests underpinning section 8 are compromised by the search in question. Information privacy values and interests include examinations of confidentiality or secrecy, control and anonymity.[22] The normative approach advocated below ensures these values are appropriately realized and, as a result, favours recognition of a significant and high information privacy interest in sent text messages obtained from a service provider.

12. Secrecy and confidentiality in digital contexts are informed by norms of practice, not exposure to risk. As this Court recently summarized in *Quesnelle*: "privacy is not an all or nothing concept; rather, '[p]rivacy interests in modern society include the reasonable expectation that private information will remain confidential to the persons to whom and restricted to the purposes for which it was divulged.'"[23] In *Quesnelle*, this Court further confirmed that a relationship of formal confidentiality might heighten, but is

---

surely reasonable for people to expect that these communications will not be intercepted by third persons. ... The connection between s. 2(b) and privacy is thus not to be rashly dismissed, and I am open to the view that justifications for abrogating the freedom of expression are less easily envisioned where expressive activity is not intended to be public, in large part because the harms which might arise from the dissemination of meaning are usually minimized when communication takes place in private, but perhaps also because the freedoms of conscience, thought and belief are particularly engaged in a private setting." *Bennett v Lenovo*, 2017 ONSC 1082, para 27 ("The risk of unauthorized *access* to private information is itself a concern even without any *actual* removal or actual theft. For example, if a landlord installs a peephole allowing him to look into a tenant's bathroom, the tenant would undoubtedly feel that her privacy had been invaded even if the peephole was not being used at any particular time.") UNGA, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/29/32, May 22, 2015 ("Surveillance systems ... may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information."; Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31(1) *Berkeley T L J* 117; Human Rights Watch & American Civil Liberties Union, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law & American Democracy", July 2014, *Human Rights Watch*; Cindy Cohn, "Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt", (2016) *126 Yale LJ 107*; Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", (2016) 93(2) *Journalism & Mass Communication Q* 296; PEN America, "Global Chilling: The Impact of Mass Surveillance on International Writers", *Pen.org*, January 5, 2015.

[21] *R v Duarte*, [1990] 1 SCR 30, para 47.

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

[23] *R v Quesnelle*, 2014 SCC 46, para 37.

not a pre-requisite to, privacy expectations.[24] Text-based messaging is prevalent in modern communication. A central feature of these is that the sender of a message must expose herself to the risk that a copy of the message might be retained by the recipient or created by the recipient's service provider. It is also common for individuals to use other person's devices and service providers, such as a sister's Internet connection or a wife's telephone.[25] In doing so, they disclose information (often deeply private information), under certain circumstances, to certain persons and for specific purposes, while expecting contextual integrity to be maintained.[26] Normative privacy protections should respect these expectations.

13. Control is another concept that informs the section 8 analysis, but must be applied in a purposive and contextual manner. Informational control is the notion that individuals must be able to retain privacy expectations *even where* they are compelled by modern practicalities to expose information to various third parties for various purposes.[27]

14. Much as with the concepts of secrecy and confidentiality, ceding informational control to one entity for one purpose is not synonymous with ceding control in general. An individual provides a blood sample for medical reasons without ceding control over that sample for state investigative purposes;[28] an individual that cedes control of her Internet activity to her service provider for routing purposes but not for marketing purposes;[29] an individual entrusting intimate details to a partner for personal reasons, to police in order to facilitate a criminal investigation, or to the courts for adjudication does not cede control to the public at large.[30] Focusing on notions of physical control or access to information and the facilities in which information is stored simply misunderstands the nature of informational control.[31]

15. Indeed, this Court has recognized that where, as here, records of electronic interactions are created outside

---

[24] *R v Quesnelle*, 2014 SCC 46, para 38.

[25] *R v Spencer*, 2014 SCC 43, paras 37; *R v MacInnis*, [2007] O.J. No. 2930, 163 C.R.R. (2d) 111 (ONSC).

[26] *R v Quesnelle*, 2014 SCC 46, para 37; *R v Dyment*, [1988] 2 SCR 417, para 22; Helen Nissenbaum, "Privacy in Context: Technology, Policy and the Integrity of Social Life" (2010) Stanford University Press, pp 233-4.

[27] *R v Dyment*, [1988] 2 SCR 417, para 22: "Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it: "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected."

[28] *R v Dyment*, [1988] 2 SCR 417.

[29] PIPEDA Report of Findings #2015-001, *Bell's Relevant Ads Program*, April 7, 2015, (OPC); Telecom Regulatory Policy CRTC 2009-657, *Review of the Internet traffic management practices of Internet service providers*, CRTC File No 8646-C12-200815400, October 21, 2009, (CRTC), paras 96-105.

[30] *R v Quesnelle*, 2014 SCC 46; *Doe 464533 v ND*, 2016 ONSC 541; *AT v Globe24h.com*, 2017 FC 114.

[31] *R v Jones*, [2012] OJ No 6508 (ONCJ), para 31 ("There is no evidence that the Applicants had any control over the records themselves or the Telus offices where they were located."). By contrast, *R v Vu*, 2013 SCC 60, para 39, 41 (authority to search a location and physical receptacles within that location does not extend to electronic data stored within the area being searched); *R v Edwards*, [1996] 1 SCR 128, para 44 (lack of control over the apartment and over access to it is *distinct* from the privacy interest that may persist in goods stored in that apartment).

the sender's control, this can *strengthen* rather than *weaken* privacy expectations as it is all the more important to maintain privacy norms where these are put at risk by the enhanced retention capabilities of modern technologies.[32] Communications intermediaries can record and retain communications and provide a ready point of mass access to the state.[33] If such storage removed 'sent' communications from protection, the state could bypass section 8 altogether by simply directing queries at recipient accounts held by an increasingly small number of intermediaries.[34] Individuals must not fully shoulder the burdens inherent in maintaining privacy expectations in light rapidly evolving technological developments. Individuals need not 'structure their affairs to maintain privacy' by adopting increasingly rigorous privacy countermeasures such as the use of passwords to safeguard devices.[35] The normative approach protects privacy individuals *should* be able to expect, not that which they empirically *can* expect in light of evolving technologies or the capabilities of communications intermediaries.[36] Given the central importance of interconnectivity to modern life,[37] individuals retain a robust interest in ensuring changes in modern communications mechanisms do not wholly erode privacy protections.

(iii) Subjective expectation in private communications should be presumed

16. The Respondents argue that a subjective privacy expectation must be established on the basis of testimony from the accused or, at minimum, cannot be advanced on an 'alternative' basis while repudiating attribution of a private communication.[38] Subjective privacy expectations are often viewed as 'self evident' in contexts that engage deeply private subject matter such as the text messaging at issue here.[39] In *Spencer*, for example, this Court allowed the defence to rely on the Crown's theory and evidence that the defendant

---

[32] *R v Vu*, 2013 SCC 60, para 42 (the manner in which computers auto-generate information and facilitate reconstruction of deleted documents leads to enhanced privacy interests). *R v TELUS Communications Co*, 2013 SCC 16, para 40 "The communication process used by a third-party service provider should not defeat Parliament's intended protection for private communications."

[33] *R v Hoelscher*, 2016 ABQB 44, paras 114-115: ("... when police intercept text messages from a service provider, they acquire every message sent and received for the phone number, for a specific period of time. The owner of the cell phone has no control over the storage or disposition of the messages by the service provider. ... This loss of control of a private communication in the hands of the service provider, and the serious level of intrusion justify the protections of Part VI."); *R v Craig*, 2016 BCCA 154, para 64: "Millions, if not billions, of emails and "messages" are sent and received each day all over the world. Email has become the primary method of communication. When an email is sent, one knows it can be forwarded with ease, printed and circulated, or given to the authorities by the recipient. But it does not follow, in my view, that the sender is deprived of all reasonable expectation of privacy."

[34] *R v Craig*, 2016 BCCA 154, paras 101-102 ", a server is often a repository for vast amounts of highly personal communications and information about the account holder and *also his or her acquaintances*." In Canada, 90% of mobile subscribers market are concentrated in three service providers: CRTC, Communications Monitoring Report 2016, (Ottawa, CRTC, 2016), Figure 5.5.5.

[35] *R v Fearon*, 2014 SCC 77, para 53: "An individual's decision not to password protect his or her cell phone does not indicate any sort of abandonment of the significant privacy interests one generally will have in the contents of the phone."

[36] *R v Tessling*, 2004 SCC 67.

[37] *R v Craig*, 2016 BCCA 154; *R v Hoelscher*, 2016 ABQB 44.

[38] Respondent, Her Majesty the Queen in Right of Canada, paras 38-41; Respondent, Her Majesty the Queen in Right of Ontario, paras 28-29; *R v Jones*, 2016 ONCA 543, paras 15-16; *R v Jones*, [2012] OJ No 6508 (ONCJ), para 21 and para 31 point (vi).

[39] *R v Cole*, 2012 SCC 53, para 43 (subjective expectation can be inferred by use of device to transmit personal information).

accessed the Internet by means of his sister's Internet account.[40] Given the deeply private nature of private communications, the purported sending of such a message is sufficient to establish an implicit subjective expectation of privacy.[41]

17. Further, compelling the accused to confirm authorship of private communications as a pre-condition to asserting a section 8 right at trial undermines anonymity, the right to silence and the right against self-incrimination.[42] The automatic standing rule this Court rejected in *Edwards* was historically intended to prevent a situation where individuals are compelled to choose between self-incrimination in pre-trial testimony or asserting their privacy rights.[43] CIPPIC does not advocate return to the automatic standing rule, but an avenue for individuals to assert privacy rights without sacrificing their right to silence must be retained. One such avenue is to allow individuals to accept crown theories (and evidence)[44] as alternative theories when advancing section 8 rights without compelling these individuals to present incriminating pre-trial testimony regarding attribution of otherwise anonymous text messages.[45] Preventing defendants from accepting the Crown's theories and evidence of ownership and attribution as *alternative* theories in the context of a section 8 *voir dire* would undermine the anonymity protected by section 8, in a heightened context that engages self-incrimination values.[46]

---

[40] *R v Spencer*, 2014 SCC 43, paras 11-12 and 19 ("On the proper understanding of the scope of the search, Mr. Spencer's subjective expectation of privacy in his online activities can readily be inferred from his use of the network connection to transmit sensitive information. Mr. Spencer's direct interest in the subject matter of the search is equally clear. Though he was not personally a party to the contract with the ISP, he had access to the Internet with the permission of the subscriber and his use of the Internet was by means of his own computer in his own place of residence.")

[41] *R v Siniscalchi*, 2010 BCCA 354; *R v Ley*, 2014 BCSC 2108, paras 32-34; *R v Pelucco*, 2015 BCCA 370, para 53: "[i]t would strain credulity to suggest that a reasonable person would have engaged in such a conversation if they thought that the messages would be shared with others."

[42] Respondent, Her Majesty the Queen in Right of Canada, para 41. *R v Farrah*, 2011 MBCA 49, paras 18-21.

[43] *US v Salvucci*, (1980) 448 US 83 (SCOTUS), pp *87-89 ("First, the Court found that in order to establish standing at a hearing on a motion to suppress, the defendant would often be "forced to allege facts the proof of which would tend, if indeed not be sufficient, to convict him," since several Courts of Appeals had "pinioned a defendant within this dilemma" by holding that evidence adduced at the motion to suppress could be used against the defendant at trial. The Court declined to embrace any rule which would require a defendant to assert his Fourth Amendment claims only at the risk of providing the prosecution with self-incriminating statements admissible at trial. The Court sought resolution of this dilemma by relieving the defendant of the obligation of establishing that his Fourth Amendment rights were violated by an illegal search or seizure.")

[44] Respondent, Her Majesty the Queen in Right of Canada, para 38, footnotes 36.

[45] *Gardner v US*, (2012) 680 F.3d 1006 (US, 7th Circuit, Court of Appeals): "If we were to adopt the government's view, a defendant who truthfully contends that police stopped him unlawfully and planted a gun on him during a suspicionless search would be able to challenge the search only by perjuring himself at a suppression hearing by falsely stating that he possessed the gun. It should go without saying, however, that perjury is never required--it is not even permitted. Such lies could also expose a defendant to impeachment at trial if he later truthfully denied possession. To avoid perjury and impeachment, the defendant's only alternative would be to forfeit a challenge to the search and rest his hopes on the jury's believing his testimony that the police planted a gun. The law is not that harsh. A defendant with two legitimate defenses to a possession charge is not forced to pick just one--indeed, he is entitled to present inconsistent positions if he wishes." [citations omitted] See also *US v Salvucci*, (1980) 448 US 83 (SCOTUS), pp *93-97 (evidence presented at pre-trial fourth amendment suppression hearing cannot be used in trial unless to impeach defendant).

[46] *R v Boudreau-Fontaine*, 2010 QCCA 1108, paras 39 and 46.

(iv) Expectations of privacy in text-based digital messages are objectively reasonable

18. The contractual and legal framework guiding interactions in this context supports the already high privacy expectations engaged, rather than detracting from it. While specific contractual provisions can enhance or diminish the reasonableness of privacy expectations,[47] the absence of a contractual relationship between the sender of a text message and the recipient or the recipient's communications provider cannot undermine otherwise robust privacy expectations and is, at best, a neutral factor.[48]

19. It is simply incorrect to conclude that the receipt of a text message by an individual fully exhausts the sender's legal privacy interest.[49] An individual who has disclosed private information to another can rely on tort law to prevent the recipient from recklessly or intentionally disclosing that information in a manner that a reasonable person would consider highly offensive.[50] As noted above, deeply private information including medical conditions, explicit or intimate communications, crisis support interactions and financial information is often communicated by means of text messaging. Senders of such private information by means of text messaging can legally prevent recipients from disclosing it,[51] further strengthening the already high expectations of privacy associated with private correspondence. While the framework for tortious privacy invasion continues to evolve in a manner that is informed by reasonable privacy expectations, it would be generally reasonable for the recipient of harassing, extortionate, or otherwise victimizing text messaging to voluntarily disclose it to law enforcement on the recipient's own initiative.[52] In addition, even where it is legal for a recipient of private communications to voluntarily disclose their

---

[47] *R v Gomboc*, 2010 SCC 55, per Deschamps, J, para 32 and 43 (permissive contractual or legislative scheme is "one factor amongst many" and not necessarily "sufficient ... to dissolve any expectation of privacy" alone, but can, in the totality of circumstances, defeat an otherwise low expectation of privacy). *R v Cole*, 2012 SCC 53, paras 53 and 58 ("written policies are not determinative of a person's reasonable expectation of privacy. ... The nature of the information heavily favours recognition of a constitutionally protected privacy interest.").

[48] *R v Spencer*, 2014 SCC 43, paras 61 and 65 (statutory and contractual provisions essentially 'neutral' are incapable of rendering an otherwise high expectation of privacy unreasonable); para 57 ("Mr Spencer was not personally a party to these agreements, as he accessed the Internet through his sister's subscription."). See also *R v Duarte*, [1990] 1 SCR 30 (lack of a contractual relationship with the recipient of a telephone call does not affect the reasonableness of privacy expectations). *R v Jones*, 2016 ONCA 543, para 16: "There was also nothing to suggest that Telus was contractually bound to the appellant..."

[49] *R v Pelucco*, 2015 BCCA 370, per Goepel, JA, dissenting, para 118: "A person who – without any guarantee of confidentiality or indication from the recipient that the message will be kept confidential – communicates information has made an autonomous choice ... who, how and to what extent to communicate information to the fullest extent possible. Any further claim against a recipient is a claim that the sender can then determine who, how and to what extent the recipient will communicate information to further third parties, which interferes with the recipient's notional sphere of personal autonomy."

[50] *Jones v Tsige*, 2012 ONCA 32, para 72: "intrusions into matters such as one's financial or health records, sexual practises and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive."

[51] *Caltagirone v Scozzari-Cloutier*, [2007] OJ No 4003 (Small Claims Court)(aunt entrusted with HIV status of nephew cannot disclose to parents of nephew); *Doe 464533 v ND*, 2016 ONSC 541, para 47 ("the defendant posted on the Internet a privately-shared and highly personal intimate video recording of the plaintiff. I find that in doing so he made public an aspect of the plaintiff's private life. I further find that a reasonable person would find such activity ... to be highly offensive."); *Griffin v Sullivan*, 2008 BCSC 827, (individual publicly identifies pseudonymous member of online suicide crisis support discussion board)("... the plaintiff had a reasonable expectation that any member of the ASH group who obtained his personal information or photograph would not publish it on the internet. The defendant did so."); *Condon v Canada*, 2014 FC 250, paras 55-61 (reckless disclosure of legitimately acquired financial records can constitute tortuous invasion of privacy).

[52] *R v Sandhu*, 2014 BCSC 303; Respondent, Her Majesty the Queen in Right of Canada, paras 60-62; Respondent in *R v Marakah*, Her Majesty the Queen in Right of Ontario, paras 49-50. *R v Gomboc*, 2010 SCC 55, para 41; *R v Spencer*, 2014 SCC 43, para 67.

content to a third party, the sender may still retain a reasonable expectation that the state will not collect all such communications.[53] Nonetheless, the legal ability to prevent individual recipients of private communications from disclosing them further strengthens the already high privacy interests implicated.

20. However, *Jones* and *Marakah* raise a wholly different factual matrix, where the collection occurs at the initiative of the state, not that of the recipient.[54] In neither case did the intended recipient of the communications in question participate in the state's search and, moreover, in *Jones* the communications were obtained directly from a service provider and hence subject to *Personal Information Protection and Electronic* Documents *Act* [PIPEDA].[55] PIPEDA strictly limits the ability of service providers to disclose customer information to law enforcement voluntarily.[56] This is particularly so where, as here, police conduct "engage[s] a more significant privacy interest."[57] PIPEDA imposes these restrictions regardless of whether the target of a state search is the subscriber associated with the sending account, the subscriber associated with the recipient account, or one of these subscriber's partners.[58] As such, CIPPIC respectfully submits that the legislative context strengthens the already robust privacy expectations an individual can expect in sent text messages, whether acquired from the recipient or from a service provider.

C. Part VI regulates access to historical text messages from an intermediary

21. Part VI of the *Criminal Code* imposes strong protections against the unauthorized interception of private communications, seeking to ensure such invasive activity does not become a "humdrum and routine administrative matter".[59] CIPPIC readily acknowledges that Part VI does not create a complete framework for state access to private communications, with less protective production orders offering an appropriate vehicle in some contexts. However, where a communications intermediary stores communications ephemerally for the purpose of facilitating message delivery, Part VI remains engaged.

22. Part VI is to be interpreted broadly, in a manner informed by privacy expectations, so as to ensure its

---

[53] *R v Duarte*, [1990] 1 SCR 30; *R v Cole*, 2012 SCC 53, paras 60-65.

[54] *R v Buhay*, 2003 SCC 30, paras 33-34; *R v Spencer*, 2014 SCC 43, para 64: "... entirely different considerations may apply where an ISP itself detects illegal activity and of its own motion wishes to report this activity to the police."; *R v Cole*, 2012 SCC 53, paras 60-65. But see *contra*: *R v Edwards*, [1996] 1 SCR 128, para 51.

[55] SC 2000, c 5. *R v MacInnis*, [2007] OJ No 2930, 163 CRR (2d) 111 (ON SC), paras 36 and 49: "[PIPEDA] has now recognized a privacy interest in such information and therefore it is not necessary to consider the issue with respect to the subscriber." *R v Spencer*, 2014 SCC 43.

[56] *R v Spencer*, 2014 SCC 43, paras 61-64, 70: ("*PIPEDA* prohibits disclosure of the information unless the requirements of the law enforcement provision are met..."); *R v Craig*, 2016 BCCA 154, para 122.

[57] *R v Spencer*, 2014 SCC 43, paras 66-67; *R v MacInnis*, [2007] OJ No 2930, 163 CRR (2d) 111 (ON SC), paras 50, 56(c).

[58] Ontario Respondent, Queen in Right of Ontario, para 9; *R v MacInnis*, [2007] OJ No 2930, 163 CRR (2d) 111 (ON SC), para 48; *R v Spencer*, 2014 SCC 43, paras 7, 12 and 57.

[59] *R v Duarte*, [1990] 1 SCR 30, para 47.

protections are applied in a neutral manner in light of technological developments.[60] A plurality of this Court rejected narrow interpretations of the term 'interception' in light of the multi-faceted manner in which data is stored by modern communications delivery networks.[61] Where, as here, a communications intermediary temporarily stores communications to facilitate their accurate and efficient delivery, the acquired messages are not 'residing at their destination' but rather acquisition occurs 'between the place of origin and the destination'.[62] Purposively, such storage remains 'ancillary' or 'incidental' to the message delivery process, even where not temporally contemporaneous.[63] Individuals view text messaging as a 'running communication', attracting similar expectations to those that arise from voice communications which are not stored by most communications intermediaries.[64] Indeed, text messages are not typically stored by intermediaries either. CIPPIC notes that different considerations arise where an individual permanently stores private communications with a service provider, as is common with email.

D. Unintended consequences of the current standing rule must be accounted for

23. Finally, while CIPPIC does not question the general requirement for individuals to establish a personal expectation of privacy in order to assert section 8, CIPPIC notes that the issue is more appropriately framed as a question of the subsistence of substantive rights than one of standing.[65] However, as noted above, one consequence of retaining the current standing rule is that it undermines the right to silence and against self-incrimination. In other instances, as secondary use, retention and disclosure of personal information increasingly raises *Charter* implications that are divorced from its initial collection, the current standing rule might require revisiting to ensure individuals are not robbed of meaningful remedies.[66]

PART IV – COSTS

24. The intervener will not seek costs and asks that no costs be awarded against it.

---

[60] *Lyons v The Queen*, [1984] 2 SCR 633; *R v TELUS Communications Co*, 2013 SCC 16, paras 24, 26, 31, 40.

[61] *R v TELUS Communications Co*, 2013 SCC 16, para 35.

[62] *R v TELUS Communications Co*, 2013 SCC 16, para 37*; R v Giles*, 2007 BCSC 1147, para 34; *R v McQueen*, [1975] 25 CCC (2d) 262 (ABCA).

[63] *R v Hoelscher*, 2016 ABQB 44, para 104. See also: *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers,* [2004] 2 SCR 427, paras 4, 6, 92-96, 114-116; *Entertainment Software Association v Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 34, paras 5, 10, 28, 36 and 40-42.

[64] *R v TELUS Communications Co*, 2013 SCC 16.

[65] *US v Salvucci*, (1980) 448 US 83 (SCOTUS), footnote 4: "In *Rakas*, this Court discarded reliance on concepts of "standing" in determining whether a defendant is entitled to claim the protections of the exclusionary rule. The inquiry, after *Rakas*, is simply whether the defendant's rights were violated by the allegedly illegal search or seizure. Because *Jones* was decided at a time when "standing" was designated as a separate inquiry, we use that term for the purposes of re-examining that opinion."

[66] See for example: *R v Rogers Communications*, 2016 ONSC 70; *X (Re)*, 2016 FC 1105*; Wakeling v United States of America*, 2014 SCC 72.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 15th day of March, 2017

for Jill R Presser

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

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

Tamir Israel

Samuelson Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
FTX 102, 57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

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

Counsel for the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

PART VI – TABLE OF AUTHORITIES

Authority		Reference in Factum
Cases		
1	*AT v Globe24h.com*, 2017 FC 114, http://www.canlii.org/en/ca/fct/doc/2017/2017fc114/2017fc114.html	14
2	*Bennett v Lenovo*, 2017 ONSC 1082, http://www.canlii.org/en/on/onsc/doc/2017/2017onsc1082/2017onsc1082.html	10
3	*Caltagirone v Scozzari-Cloutier*, [2007] OJ No 4003 (Small Claims Court), Book of Authorities, Tab 1	19
4	*Condon v Canada*, 2014 FC 250, http://www.canlii.org/en/ca/fct/doc/2014/2014fc250/2014fc250.html	19
5	*Doe 464533 v ND*, 2016 ONSC 541, http://www.canlii.org/en/on/onsc/doc/2016/2016onsc541/2016onsc541.html	14, 19
6	*Entertainment Software Association v Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/749/index.do	22
7	*Gardner v US*, (2012) 680 F.3d 1006 (US, 7th Circuit, Court of Appeals), http://cases.justia.com/federal/appellate-courts/ca7/10-1576/10-1576-2012-05-25.pdf	17
8	*Griffin v Sullivan*, 2008 BCSC 827, http://www.canlii.org/en/bc/bcsc/doc/2008/2008bcsc827/2008bcsc827.html	19
9	*Hunter v Southam Inc*, [1984] 2 SCR 145, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/5274/index.do	
10	*Jones v Tsige*, 2012 ONCA 32, http://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.html	19
11	*JS v MM*, 2016 ONSC 3072, http://www.canlii.org/en/on/onsc/doc/2016/2016onsc3072/2016onsc3072.html	9
12	*Lyons v The Queen*, [1984] 2 SCR 633, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2501/index.do	22
13	*R v Boudreau-Fontaine*, 2010 QCCA 1108, http://www.canlii.org/en/qc/qcca/doc/2010/2010qcca1108/2010qcca1108.html	17
14	*R v Buhay*, [2003] 1 SCR 631, 2003 SCC 30, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2062/index.do	20
15	*R v Cole*, [2012] 3 SCR 34, 2012 SCC 53, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/12615/index.do	16, 18-20

	http://www.canlii.org/en/bc/bcca/doc/2016/2016bcca154/2016bcca154.html	
17	*R v Duarte*, [1990] 1 SCR 30, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/559/index.do	4, 10, 18-19, 21
18	*R v Dyment*, [1988] 2 SCR 417, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do	12-14
19	*R v Edwards*, [1996] 1 SCR 128, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1340/index.do	14, 20
20	*R v Farrah*, 2011 MBCA 49, http://www.canlii.org/en/mb/mbca/doc/2011/2011mbca49/2011mbca49.html	17
21	*R v Fearon*, [2014] 3 SCR 621, 2014 SCC 77, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14502/index.do	15
22	*R v Giles*, 2007 BCSC 1147, http://www.canlii.org/en/bc/bcsc/doc/2007/2007bcsc1147/2007bcsc1147.html	22
23	*R v Gomboc*, [2010] 3 SCR 211, 2010 SCC 55, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7898/index.do	18-19
24	*R v Jones*, [2012] OJ No 6508 (ONCJ) (Trial Judgement)	5, 14, 16
25	*R v Jones*, 2016 ONCA 543, http://www.canlii.org/en/on/onca/doc/2016/2016onca543/2016onca543.html	5, 16, 18
26	*R v Hoelscher*, 2016 ABQB 44, http://www.canlii.org/en/ab/abqb/doc/2016/2016abqb44/2016abqb44.html	15, 22
27	*R v Ley*, 2014 BCSC 2108, http://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc2108/2014bcsc2108.html	16
28	*R v MacInnis*, [2007] OJ No 2930, 163 CRR (2d) 111 (ONSC), http://www.canlii.org/en/on/onsc/doc/2007/2007canlii29342/2007canlii29342.html	12, 20
29	*R v Mann*, 2014 BCCA 231, http://www.canlii.org/en/bc/bcca/doc/2014/2014bcca231/2014bcca231.html	9
30	*R v Marakah*, 2016 ONCA 542, http://www.canlii.org/en/on/onca/doc/2016/2016onca542/2016onca542.html	5, 8
31	*R v McQueen*, [1975] 25 CCC (2d) 262 (Alta SC (App Div)), Respondent, Queen in Right of Ontario, *Jones v Her Majesty the Queen*, SCC File No 37194, Book of Authorities, Tab 6	22
32	*R v Patrick*, [2009] 1 SCR 579, 2009 SCC 17, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7611/index.do	4
33	*R v Pelucco*, 2015 BCCA 370, http://www.canlii.org/en/bc/bcca/doc/2015/2015bcca370/2015bcca370.html	16, 19

	2015, (Office of the Privacy Commissioner of Canada), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-001/	
50	Telecom Regulatory Policy CRTC 2009-657, *Review of the Internet traffic management practices of Internet service providers*, CRTC File No 8646-C12-200815400, October 21, 2009, (Canadian Radio-television and Telecommunications Commission), http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm	14
Academic		
51	Sofian Berrouiguet, *et al*, "Post-acute crisis text messaging outreach for suicide prevention: A pilot study", (2014) 217(3) *Psychiatry Research* 154, http://www.sciencedirect.com/science/article/pii/S0165178114001723	9
52	Canadian Radio-television and Telecommunications Commission, Communications Monitoring Report – 2016, (Ottawa, CRTC, 2016), http://www.crtc.gc.ca/eng/publications/reports/policymonitoring/2016/cmr5.htm#a55iii	15
53	Canadian Wireless Telecommunications Association, Canadian Common Short Code – Application Guidelines, Ver 3.0, March 11, 2015, pp 27-31, http://www.txt.ca/wp-content/uploads/2015/06/Canadian-Common-Short-Code-Application-Guidelines.pdf	9
54	Cindy Cohn, "Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt", (2016) *126 Yale LJ 107*, http://www.yalelawjournal.org/pdf/11.CohnFinalPDF_d5acfu8u.pdf	10
55	Human Rights Watch & American Civil Liberties Union, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law & American Democracy", July 2014, *Human Rights Watch*, https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf	10
56	Sarah Mitroff, "No Download Needed: The Rise of Chatbots", May 3, 2016, CNET.com, https://www.cnet.com/news/sms-based-apps/	9
57	Helen Nissenbaum, "Privacy in Context: Technology, Policy and the Integrity of Social Life" (Stanford University Press, 2010), Book of Authorities, Tab 2	12
58	PEN America, "Global Chilling: The Impact of Mass Surveillance on International Writers", January 5, 2015, http://pen.org/global-chill	10
59	Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31(1) *Berkeley T L J* 117, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645	10
60	Brian Rinker, "Meeting Teens Where They Are: Suicide Prevention by Text Message", September 16, 2014, *Oakland North*, https://oaklandnorth.net/2014/09/16/meeting-teens-where-they-are-suicide-	9

61	Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", (2016) 93(2) *Journalism & Mass Communication Q* 296, http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255	10
62	United Nations General Assembly, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/29/32, May 22, 2015, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32	10
63	United States Department of Commerce, National Institute of Standards and Technology, "Digital Identification Guidelines: Authentication and Lifecycle Management", DRAFT NIST Special Publication 800-63B, https://pages.nist.gov/800-63-3/sp800-63b.html	9
64	World Health Organization, "mHealth: New Horizons for Health Through Mobile Technologies", *Global Observatory for eHealth Series*, Vol 3, (World Health Organization, 2011), http://www.who.int/goe/publications/goe_mhealth_web.pdf	9