SCC Court File No.: 34252

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

BETWEEN:

TELUS COMMUNICATIONS COMPANY

APPELLANT
(APPELLANT)

- and -

HER MAJESTY THE QUEEN

RESPONDENT
(RESPONDENT)

MEMORANDUM OF ARGUMENT
OF SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC
(Motion for leave to intervene)

Pursuant to Rules 47 and 55 of the Rules of the Supreme Court of Canada

---

PART I – FACTS

A. Overview

1. The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic ("CIPPIC") seeks an Order granting it leave to intervene in this appeal.

2. This appeal will address issues of great importance relating to the need to ensure privacy protections are not outstripped by technical evolutions in communications. Specifically, the term 'interception' must be interpreted in a manner that is in line with its natural meaning, but also does not operate to undermine the purpose for those protections. An overly narrow interpretation will have serious implications for the privacy of communications – not just with respect to text messages, but

also with respect to online information exchanges

3. If successful in its motion for leave to intervene, CIPPIC will assist the Court in its consideration of the important issues before it by offering useful submissions different from those of the other parties.

4. In providing its useful and different submissions, CIPPIC will draw on the unique knowledge and expertise it has developed through its specialized activities in this area of law and policy. CIPPIC's experience in Internet privacy policy in general has included participation in legislative, academic, judicial, quasi-judicial, and client-centered processes. It has also been an active participant in international policy-making processes relating to privacy and technology, as well as a number of processes where the question of privacy's evolving role within judicial procedures has been directly at issue.

B. CIPPIC

5. CIPPIC is a legal clinic based at the University of Ottawa's Centre for Law, Technology and Society. Its core mandate is to advocate in the public interest where the law intersects with new technologies in ways that may detrimentally impact on the public. CIPPIC is Canada's sole legal clinic dedicated entirely to internet policy and public interest law. Internet policy issues impact on most aspects of CIPPIC's advocacy and public outreach activities. CIPPIC has intervened in the courts, testified before Committees of the House of Commons and Senate, participated in numerous quasi-judicial fora, helped shape Internet policy at the International level through participation in various Internet governance processes and produced numerous publications and public outreach documents on law and technology issues.

Affidavit of Kent Mewhort, sworn on March 28, 2012, Motion Record, Tab 2

6. This Hounourable Court has previously recognized CIPPIC's capacity to assist the Court on questions relating to the balance of competing values in an online environment by granting CIPPIC leave to intervene in a number of internet policy-related cases. In 2006, this Honourable Court granted CIPPIC leave to intervene in a case concerning computer sales over the internet, *Dell Computer*

Corporation. v. *Union des consommateurs*, 2007 SCC 34. In 2010, this Honourable Court granted CIPPIC leave to intervene in a defamation case with the potential to expand Canadians' liability for posting content on the internet, *Crooks* v. *Newton*, 33412 (SCC). In 2011, this Honourable Court granted CIPPIC leave to intervene in five copyright cases: (*Re:Sound v. Motion Picture Theatre Associations of Canada, et al.*, 34210 (SCC); P*rovince of Alberta as represented by the Minister of Education et al. v. Canadian Copyright Licensing Agency Operating as "Access Copyright"*, 33888 (SCC); E*ntertainment Software Association et al.* v. *Society of Composers, Authors and Music Publishers of Canada, 33921 (SCC); Rogers Communications Inc., et al.* v. *Society of Composers, Authors and Music Publishers of Canada, 33922 (SCC);* and *Society of Composers, Authors and Music Publishers of Canada* v. *Bell Canada et al.*, 33800 (SCC)).

Mewhort Affidavit, sworn on March 28, 2012, Motion Record, Tab 2

7. In addition to this generalized privacy experience, CIPPIC has participated in numerous processes where the proper scope of privacy protections and reasonable expectations of privacy were at issue. These include, for example, its interventions in *BMG Canada Inc.* v. *Doe*, 2004 FC 488 and 2005 FCA 193, and *Warman* v. *Wilkins-Fournier*, 2010 ONSC 2126 (Ont. Div. Ct.). In addition, CIPPIC's participation in international policy-making bodies such as the OECD (via its membership in the Civil Society Information Society Advisory Council to the OECD) on issues relating to the role of Internet intermediaries will be of direct relevance. CIPPIC is additionally in the process of completing a research project funded by the Privacy Commissioner of Canada and aimed at examining the evolving role of telecommunications in the broader context of electronic state surveillance capacities.

PART II – STATEMENT OF QUESTIONS AT ISSUE

8. The only issue before the Court in this motion is whether CIPPIC should be granted leave to intervene in this matter of important public interest.

PART III – ARGUMENT

9. An applicant seeking leave to intervene before this Court under section 55 of the *Rules of the Supreme Court of Canada* must address two issues, as established in case law and codified in section

57(2):

(a) whether the applicant has an interest in the issues raised by the parties to the appeal; and

(b) whether the applicant's submissions will be useful to the Court and different from those of the other parties.

***Reference re Workers' Compensation Act,* 1983 (Nfld.), [1989] 2 S.C.R. 335 (SCC) at para. 8**
***R.* v. *Finta*, [1993] 1 S.C.R. 1138 (SCC) at para. 5**
***Rules of the Supreme Court of Canada*, SOR/2002-156, ss. 55, 57(2)**

A. CIPPIC's Interest in this Appeal

10. CIPPIC's interest in this appeal flows directly from its mandate to participate in internet policy debates and to advocate for the public interest where new technologies intersect with legal/policy development. Privacy has long been a core pillar of that mandate, particularly with respect to the privacy in communications infrastructure and the role of telecommunications service providers in defining shifting privacy expectations. The issues raised in this Appeal implicate these aspects of CIPPIC's work and mandate directly.

B. Useful and Different Submissions

11. The "useful and different submission" criteria is satisfied by an applicant who has a history of involvement in the issue, giving the applicant expertise that can shed fresh light or provide new information on the matter.

***Reference re Workers' Compensation Act,* 1983 (Nfld.), [1989] 2 S.C.R. 335 (SCC), at para. 12**

12. CIPPIC's submissions will be useful because CIPPIC brings to these proceedings the experience of a legal clinic that has worked with various stakeholders on all sides of competing interests in privacy and freedom of expression online. CIPPIC can offer the Court a useful and balanced perspective on the wider issues raised in this Appeal.

Mewhort Affidavit, Motion Record, Tab 2

13. CIPPIC's submissions will be different from those of the current parties, as they will be informed by its rich experience across the broad spectrum of law and policy related to online privacy as well as

by its specific expertise on the role of Internet intermediaries.

14. Additionally, CIPPIC's proposed submissions do not raise any concerns that have traditionally led this Honourable Court to refuse intervention. CIPPIC does not intend to expand the issues under appeal beyond those raised by the existing parties.

***Reference re Workers' Compensation Act*, 1983 (Nfld.), [1989] 2 S.C.R. 335 (SCC), at para. 12**

C. CIPPIC's Proposed Submissions

15. If granted intervener's status, CIPPIC proposes to argue that the Court below erred in law by applying incorrect principles of statutory interpretation in defining the term 'interception' within the context of Part VI of the *Criminal Code*. The Court below narrowly construed 'interception' as applying solely to simultaneous capture of communications in transit. This interpretation is not required by the wording of Part VI, and is in conflict with its legislative purpose, common law principles relating to the role of communications intermediaries, and principles embodied in section 8 of the *Charter* protecting the reasonable expectations of privacy of Canadians. Endorsement of the principle adopted by the Court below will have a serious and detrimental impact on the privacy of Internet communications.

16. The term 'intercept' is defined in section 183 of the *Criminal Code* to be inclusive of an act to: "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof." As the term 'intercept' is defined within the *Code*, there is no need to import dictionary definitions of the term. Section 184 of the *Code* designates the act of wilfully intercepting a private communication by means of an electronic device to be an indictable offence. Nothing in the *Code* definition of 'intercept' mandates that an 'interception' amount to a "real time capture of otherwise transient communications". If retained, this narrow definition will have serious implications for the privacy of communications and, particularly, for the privacy of Internet communications, which often rely on less transient content caching and temporary preservation of content as a necessary part of the communications delivery process.

***R. v. Telus Communications Co.*, 2011 ONSC 1143, paras. 43, 47**

17. Parliament enacted Part VI of the *Criminal Code* in order to curtail the privacy invasive natures of electronic surveillance. Electronic surveillance was deemed particularly harmful for its surreptitious nature, and for the ease by which mass amounts of personal communications could be gathered, as noted by Justice Dickson in *R. v. Commissio* (dissenting, but not on this point):

> The unique legislative treatment of electronic surveillance is a reflection of its nature. The modern technology is both powerful and unobtrusive. The technology permits massive invasion of the privacy with ease. It is also indiscriminate about the content of any communication intercepted. Parliament has determined that this potential constitutes a threat to individual freedom and the right to privacy. The evidentiary rule of exclusion fortifies the stipulation that interceptions of private communications are illegal unless specified conditions are met.

Justice Martin of the Ontario Court of Appeal elaborated on the privacy risks inherent in interception orders as opposed to traditional search and seizure warrants:

> It is also apparent that, although an analogy may be drawn between judicial authorizations to intercept private communications and judicial authorizations for conventional search warrants, there are substantial differences between the two types of authorizations. A search warrant authorizes the search of specified premises for specific things already in existence. The person executing a search warrant will normally know whether a particular item found on the searched premises comes within the scope of the warrant. A search warrant authorizes a single entry of the premises to be searched, and if the items sought are not found, an application for a second search warrant must be made in order to make a further entry. In contrast, an authorization to intercept private conversations authorizes the interception of conversations which have not yet taken place. The interception may occur at any time during the period specified in the authorization. It will often be the case that the listener will not be able to determine whether the intercepted conversation constitutes the evidence sought until after he has heard it in its entirety in the context of other conversations similarly overheard

***R. v. Commissio*, [1983] 2 S.C.R. 121, p. 134**
***R. v. Finlay and Grellette*, (1986) 54 O.R. (2d) 509 (Ont. C.A.)**

18. While communications technologies have since evolved, the concerns related to communications interception have not. Text messages are retained by telecommunications service providers (TSPs) to ensure better service delivery. Where police make use of such communications stores through means such as production orders or, as in this case, general warrants, they gain the capacity to surreptitiously access mass amounts of personal communications with great ease, by means of electronic equipment. This effectively bypasses the legislative purpose of Part VI and, to the extent that is reasonable, section

184 should be interpreted to encompass such conduct.

19. To the extent that the term 'interception' is limited in scope to 'interference with a communication that is passing from its source to its destination', the *speed* by which this message is moving is not relevant. Nor should the question of whether a message has yet arrived at its intended destination or not at the time of interception be determinative whether an interception has occurred. Interception is, at its core, aimed at ameliorating the extraction of personal communications from the infrastructure that facilitates that communication. The term 'interception should be flexible enough to account for technological evolutions in the nature, efficiency and accuracy of message delivery.

***R. v. Telus Communications Co.*, 2011 ONSC 1143, para. 48**

20. In its text message delivering capacity, TELUS is operating as a common carrier or TSP to the extent that it is operating an infrastructure for message delivery. The acts of common carriers, when necessary to the message delivery process, have always had special salience when assessing the legalities of a particular communication. Features inherent in common carriers have, historically, included liability limitations and added privacy obligations. The concept of common carriage can be traced back to well before the age of the Internet and finds its precursors in mail delivery systems. Susan Landau finds the precursors of the U.S. Wiretapping Law in the 1792 U.S. Act that established the postal system, which made it a criminal offence to open letters prior to delivery (similar provisions are found in the *Canada Post Corporation Act*).

***Canada Post Corporation Act*, R.S.C., 1985, c. C-10, section 48**
S. Landau, "Surveillance or Security? The Risks Posed by New Wiretapping Technologies", (Boston: Massachusetts Institute of Technology, 2010)

21. Common carrier activities are defined in a number of areas of law. Under the *Copyright Act*, for example, 'mere conduit' activity necessary to the delivery of telecommunications messages by a TSP is deemed not to amount to a 'communication to the public by telecommunication'. As this Honourable Court held in *SOCAN v. CAIP*, the use of 'caching' (making local copies of musical works at various parts of the TSPs' network so that users in that locale can access it more readily) is a 'mere conduit' activity that falls within the scope of the 'message delivery' process. Caching, while different in kind

from the historical means of message delivery inherent in telephone communications, is made necessary by the 'exigencies of the Internet':

> The creation of a "cache" copy, after all, is a serendipitous consequence of improvements in Internet technology, is content neutral, and in light of s. 2.4(1)(*b*) of the Act ought not to have any *legal* bearing on the communication between the content provider and the end user…"Caching" is dictated by the need to deliver faster and more economic service, and should not, when undertaken only for such technical reasons, attract copyright liability.

The intermediary nature of TSPs resonates in other areas of the law, where 'mere conduit' activity, defined loosely as 'activity necessary to deliver the message', has special legal significance.

> ***Copyright Act*, R.S.C., 1985, c. C-42, section 2.4(1)(b)**
> ***Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, at paras. 114-116**

22. As noted above, if granted leave to intervene, CIPPIC will argue that neither speed of message delivery nor simultaneity are determinative of 'interception'. Interception is, rather, interference with the infrastructure of delivery, which, in a rapidly evolving technological age, should be informed by well entrenched legal definitions of what is and is not part of that message delivery infrastructure.

23. TELUS employs a 30 day retention period for text messages transmitted on its network. It is not the length of the retention period that is relevant, but rather its purpose. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) restricts telecommunications companies to collecting personal information solely for clearly identified purposes. Outside a few well-defined exceptions enumerated in sub-section 7(3), PIPEDA requires telecommunications companies to gain user consent for those clearly identified purposes. PIPEDA further prevents telecommunications companies from retaining personal information once that initial purpose has expired. TELUS has no legitimate purpose to retain text message data other than to ensure message delivery and internal functions. For the retention period (absent unusual circumstances, maintenance or a warrant) TELUS should have no legitimate reason to remove text messages from their network storage in order to view the contents of these messages. This bolsters reasonable users' expectations – they do not expect text messages to be kept for longer than necessary to ensure message *delivery*.

***Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5, s. 7(3), and Principles 4.2.2, 4.3.2 and 4.5.3 of Schedule 1**

24. Part VI of the *Criminal Code* was enacted to protect what has become a constitutionally protected human right to privacy now enshrined in sections 7 and 8 of our *Charter of Rights and Freedoms*. Section 8 in particular acts to prevent the State's legitimate interests in investigating its citizens from overbearing individuals' reasonable expectations of privacy in a disproportionate manner. Given the interplay between constitutionally protected rights and Part VI, interpretation of the term 'interception' should be informed by principles of privacy protection as developed by this Honourable Court through its section 8 jurisprudence.

25. The expectation of privacy in a communication that is in the process of delivery has, historically, been high. The nature of the interception, as noted by Justice Martin in *Finlay*, above, is such that there is no manner of knowing how much irrelevant information will be captured alongside the desired elements of the communication. There is no telling ahead of time how sensitive the communications will be. Moreover, as noted by Justice Estey in *R. v. Lyons*:

> The necessary result of such legislation is the express and implied recognition of invasion of citizens' rights... It is the invasion of the mind through the covert discovery and recording of the voice, that is, that makes the powers granted in these provisions so significant in our community. It is the entry into the mind by the power to intercept private communications

Such 'intrusions into the mind' implicate a biographical core of personal information and should be treated as highly invasive.

***R. v. Lyons*, [1984] 2 S.C.R. 633**

26. Reasonable privacy expectations of privacy are contextual. While it may be true that 'simply searching stored messages' on a mobile communications device may or may not be an 'interception', the same cannot be said for the retrieval via search of the same communication from network equipment and infrastructure. Users are not overly concerned with the mechanics of message delivery and, instead, expect their text messages to be treated to the same level of protections at their voice communications while in the infrastructure of their service provider. As noted in *R. v. Finley*, the

constitutionality of Part VI interceptions is in some ways dependent on the specific limitation regime adopted for surreptitious interception of communications. This is what reasonable expectations of privacy require.

***R. v. Finlay and Grellette*, (1986) 54 O.R. (2d) 509 (Ont. C.A.)**

PART IV – COSTS

27. CIPPIC will not seek costs in this matter and asks that costs not be awarded against it in this motion or in the appeal if leave to intervene is granted.

PART V PART V – ORDER SOUGHT

28. CIPPIC respectfully requests an Order from this Honourable Court:

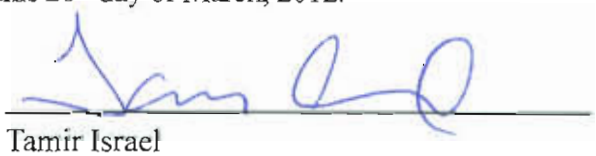
(i) granting CIPPIC leave to intervene in this appeal;

(ii) permitting CIPPIC to file a factum of no greater length than 20 pages;

(iii) permitting CIPPIC to present oral argument at the hearing of this appeal; and

(iv) such further or other Order as deemed appropriate.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 28th day of March, 2012.



Tamir Israel

Samuelson Glushko Canadian Internet
Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law,
Common Law Section
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 Proposed Intervener,
Samuelson-Glushko Canadian Internet
Policy and Public Interest Clinic**

PART VI – TABLE OF AUTHORITIES

	Authority	Reference in Argument
	Cases	
1.	*Reference re Workers' Compensation Act, 1983 (Nfld.)*, [1989] 2 S.C.R. 335 (SCC)	9, 11, 14
2.	*R. v. Commissio*, [1983] 2 S.C.R. 121, p. 134	17
3.	*R. v. Finlay and Grellette*, (1986) 54 O.R. (2d) 509 (Ont. C.A.)	17, 26
4.	*R. v. Finta*, [1993] 1 S.C.R. 1138 (S.C.C.)	9
5.	*R. v. Lyons*, [1984] 2 S.C.R. 633	20
6.	*Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427,	21
7.	*R. v. Telus Communications Co.*, 2011 ONSC 1143	16, 19
	Academic	
8.	S. Landau, "Surveillance or Security? The Risks Posed by New Wiretapping Technologies", (Boston: Massachusetts Institute of Technology, 2010)	20
	Legislation	
9.	*Canada Post Corporation Act*, R.S.C., 1985, c. C-10, section 48	20
10.	*Copyright Act*, R.S.C., 1985, c. C-42, section 2.4(1)(b)	21
11.	*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5, section 7(3), and Principles 4.2.2, 4.3.2 and 4.5.3 of Schedule 1	23
12.	*Rules of the Supreme Court of Canada*, SOR/2002-156	9