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

- and -

HER MAJESTY THE QUEEN

RESPONDENT

- and -

ATTORNEY GENERAL OF ONTARIO, CANADIAN CIVIL LIBERTIES ASSOCIATION, AND SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

INTERVENERS

MEMORANDUM OF ARGUMENT OF THE INTERVENER SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Pursuant to Rules 37 and 42 of the Rules of the Supreme Court of Canada

---

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

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

Counsel for the Proposed Intervener

TO: THE REGISTRAR

COPY TO:

Stockwoods LLP Barristers
Royal Trust Tower
Suite 130, P.O. Box 140
77 King Street West
Toronto, ON, M5K 1H1

Brian Grover
Scott Hutchison
Brennagh Smith

Tel: (416) 593-7200
Fax: (416) 593-9345
Email: briang@stockwoods.ca

Counsel for the Appellant, TELUS Communications Company

Michael J. Sobkin
Barrister & Solicitor
Unit #2
90 Boulevard de Lucerne
Gatineau, QC, J9H 7K8

Michael J. Sobkin

Tel: (819) 778-7794
Fax: (819) 778-1740
Email: msobkin@sympatico.ca

Agent for the Appellant, TELUS Communications Company

AND TO:

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

Lisa Matthews
Tom Andreopolous

Tel: (902) 446-1455
Fax: (902 406-3140

Counsel for the Respondent, Her Majesty the Queen

Directeur des poursuites pénales du Canada
2ième étage, 284 rue Wellington
Ottawa, ON, K1A 0H8

François Lacasse

Tel: (6133) 957-4770
Fax: (613) 941-7865
Email: flacasse@ppsc-sppc.gc.ca

Agent for the Respondent, Her Majesty the Queen

AND TO:

Attorney General of Ontario
720 Bay Street, 10th Floor
Toronto, ON, M5G 2K1

Michal Fairburn

Tel: (416) 326-4658
Fax: (416) 326-4656
Email: michal.fairburn@ontario.ca

Counsel for the Intervener, the Attorney General of Ontario

Burke-Robertson LLP
70 Gloucester Street
Ottawa, ON, K2P 0A2

Robert E. Houston, Q.C.

Tel: (613) 566-2058
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Agent for the Intervener, the Attorney General of Ontario

AND TO:

Torys LLP
Suite 3000, 79 Wellington Street West
Toronto, ON, M5K 1N2

Osler, Hoskin & Harcourt LLP
Suite 1900, 340 Albert Street
Ottawa, ON, K1R 7Y6

Wendy Matheson
Rebecca L. Wise

Tel: (416) 865-8133
Fax: (416) 865-7380
Email: wmatheson@torys.com

Counsel for the Intervener, the Canadian Civil Liberties Association

Patricia J. Wilson

Tel: (613) 787-1009
Fax: (613) 235-2867
Email: pwilson@osler.com

Agent for the Intervener, the Canadian Civil Liberties Association

TABLE OF CONTENTS

Page

PART I – OVERVIEW AND FACTS

1. This appeal raises the novel and critical question of how to assess temporary storage activities ancillary to communications delivery mechanisms when determining if an 'interception' has occurred under Part VI of the *Criminal Code*.

PART II – QUESTIONS AT ISSUE

2. There are two closely intertwined issues in this appeal. CIPPIC's intervention focuses on the first and addresses the second briefly:

A) What is the meaning of the term 'interception' in light of evolving technological changes?

B) Should mechanisms such as general warrants be permitted to undermine encoded privacy protections?

PART III – MAIN ARGUMENT

3. The past several decades have brought about dramatic technological innovations that have revolutionized our capacity to interact and communicate. This evolution in communications has brought about a concomitant increase in the state's capacity to surveille the activities of its citizens. Electronic surveillance, while playing an undeniably vital role in facilitating legitimate criminal investigations, has the additional potential to erode any meaningful semblance of privacy. It was the highly invasive capacity of electronic surveillance techniques (and, particularly, of communications interception) that prompted Parliament to enact Part VI of the *Criminal Code*. In light of the invasive potential posed by some forms of electronic surveillance and the highly private nature of communications, Part VI of the *Code* should be interpreted flexibly and in a manner that accounts, where possible, for technological evolutions in message delivery mechanisms.

R. v. Duarte, [1990] 1 S.C.R. 30, paras. 21-22

A. Part VI, Section 8 & Electronic Surveillance

4. The relationship between Part VI of the Code and section 8 of the Charter is a complex one. Part VI's inspiration, Title III of the U.S. Omnibus Crime Control and Safe Streets Act, was an attempt to legislate a list of safeguards that the U.S. Supreme Court declared a pre-requisite to constitutional wiretapping. In Canada, Part VI predated the adoption of the Charter, and courts have made it clear that some, but not all of the strong safeguards imposed by Part VI are necessary to constitutionally valid interception of communications. Regardless of whether elements of the Part VI framework are a constitutional pre-requisite to communications interception or not, its interpretation has evolved in a manner that is highly informed by section 8 principles and, particularly, those section 8 principles relating to other forms of electronic surveillance. This affinity and its potential impact merit some elaboration.

Lyons v. The Queen, [1984] 2 S.C.R. 633, p. 679-680; ***R. v. Tse***, 2012 SCC 16, paras. 10-11

Section 8 and Electronic Surveillance

5. Section 8 strives to balance legitimate state interests in information necessary to protect its citizens with the right to prevent unreasonable intrusion on individual privacy. (*Tessling*) This balance is struck largely around the concept of 'reasonable expectations of privacy' – the line that demarcates a 'zone of privacy' which individuals can reasonably expect to stay free of unfettered state intrusion. Electronic communications have, historically, attracted high expectations of privacy under section 8

jurisprudence (*Duarte;* Oliver; *S.M.*): "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance and to which, in consequence, the protection accorded by s. 8 should be more directly aimed..."

> **W.M. Oliver**, "Western Union, the American Federation of Labor, Google, and the Changing Face of Privacy Advocacy", (2012) 81(5) *Miss. L.J.* 971; ***Duarte***, *supra*, paras. 18-19; ***R. v. S.M.***, 2012 ONSC 2949, paras. 24-25; ***R. v. Tessling***, [2004] 3 S.C.R. 432, paras. 17-18, 22

6. Particularly in the context of electronic surveillance, Courts have sought to adopt a flexible, comprehensive approach that seeks to assess reasonable expectations of privacy based on a "totality of the circumstances". The 'totality of the circumstances' approach posits a principled framework that, while providing flexibility for a rapidly evolving array of investigative techniques, ensures the spirit of section 8 is not "constrained by narrow legalistic classifications." (*Duarte;* Stewart; *Tessling*) By keeping these objectives firmly in mind, the flexibility inherent in the 'totality of the circumstances' test may ensure that section 8 remains viable as a means of checking "the impact...of observation on the values protected by the right to privacy."

> **Canadian Bar Association**, "Submission on *Lawful Access* – Consultation Document", December 2002, pp. 3-4; H. **Stewart**, "Normative Foundations for Reasonable Expectations of Privacy", (2011), 54(2) *S.C.L.R.* 335, p. 355; ***Duarte***, *supra*, para. 19; ***Tessling***, *supra*, para. 19

7. Section 8 protections are also intended to "keep pace with technological development" so as to ensure a continuing framework for assessing legitimate exercise of state powers against the need to protect against unauthorized privacy intrusions "whatever technical form the means of invasion may take." (*Wong*) In the past, this Honourable Court has avoided an analysis of invasiveness that is 'fixed in time', stressing the importance of ensuring a potentially invasive technology is "evaluated according to its *present* capacity" to reveal intimate details about the lifestyle of an individual. (*Tessling*)

> ***Tessling***, *supra*, paras. 42, 54-55; ***R. v. Wong***, [1990] 3 S.C.R. 36, paras. 9, 15

Part VI and Electronic Surveillance

8. The objective of Part VI, in its broadest sense, reflects that of section 8 in its attempt to strike a "balance between the privacy interest of the individual and the competing interest of the public in law enforcement" (*Wiretap Reference*). More specifically, the rationale for Part VI is to "regulat[e] the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it." (*Duarte*) Part VI has been said to recognize a "right to private communication" and establish the narrow conditions under which this right can be undermined. Implicit in its passing is a recognition of the high privacy interest inherent in telecommunications, and the need to limit the means by which the state may undertake an "invasion of the mind" in order to further its legitimate investigative objectives:

> This is the important crux of [Part VI]. 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...
>
> ***Duarte***, *supra*, para. 21; ***Lyons***, *supra*, p. 694, per Estey, J.; ***Wiretap Reference***, [1984] 2 S.C.R. 697, pp. 702-703, per Dickson, J., dissenting on another point; ***R. v. Welsh and Uannuzzi (No. 6)***, (1977), 32 C.C.C. (2d) 363, (Ont. C.A.) as cited with approval by Dickson, J., in ***Wiretap Reference***, *supra*, pp. 702-703

9. In light of the heightened privacy interest attaching to electronic communications, Part VI enacts a number of safeguards that are tailored to the specific issues raised by the state's technical capacity to intercept electronic telecommunications. In addition to guarding against some particular problems posed by intercept technologies to civil liberties, these safeguards, taken *in toto*, aim to "prevent the possibility that the police view recourse to electronic surveillance as a humdrum and routine administrative matter..."

(*Duarte*). This latter element of the Part VI framework is evident in the exhaustion requirement (paragraph 186(1)(b)) and has the effect of rendering the "administrative cost and inconvenience of complying with the warrant" a salient consideration.

> ***Criminal Code***, S.C., 1985, c. C-46, s. 186; ***Duarte***, *supra*, para. 47; **Respondents Factum**, April 23rd, 2012, para. 19

10. The structure of Part VI evinces Parliament's intent to apply its provisions in a technologically neutral manner:

> This is broad legislation embracing in these extensive provisions the use of a wide range of…devices for listening to and recording private communications as broadly defined. It is not "wiretapping" legislation, nor eavesdropping legislation, nor radio regulation. It is the regulation of all these things and "any other device" that may be used to intercept intelligence reasonably expected by the originator not to be intercepted by anyone other than the intended recipient.

It must, therefore, be "read and applied with an awareness of the community it seeks to regulate. It was not an age of smoke signals or even simple telephony into which these extensive regulations were launched."

> ***Lyons***, *supra*, per Estey, J., p. 665; ***Entertainment Software Association v. SOCAN***, 2012 SCC 34, para. 5

11. Part VI is also a response to technological evolutions in electronic surveillance capabilities that enable surreptitious surveillance on a massive scale (*Commissio*, cited in *Lyons*):

> 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.

The technological underpinnings of Part VI are such that it can be taken to have "[t]he reasonable needs of the community for adequate crime detection services utilizing modern technology, as well as the reasonable need of the community for protection from these new techniques" in mind (*Lyons*, per Estey, J.).

> ***Lyons***, *supra*, per Estey, J., p. 665 ; ***R. v. Commissio***, [1983] 2 S.C.R. 121, p. 134, Dickson, J., dissenting on another point, as cited in ***Lyons***, p. 641

Statutory Interpretation and the Structure of Surveillance Powers

12. In sum, both the objectives of Part VI and the Court's section 8 jurisprudence are informed by reasonable expectations. Additionally, both recognize the heightened privacy interest inherent in telecommunications, the threat posed to privacy by technological advancements in electronic surveillance, and, importantly, the need for flexible, purposive, technologically neutral interpretive frameworks capable of keeping pace, to the extent possible, with shifting technological developments.

13. The modern principle of statutory interpretation reads legislative words "in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament." Further, while the safeguards in Part VI are not necessarily a constitutional imperative, this principle favours interpretations that further *Charter* values even where strict compliance is not required:

> Underlying this approach is the presumption that legislation is enacted to comply with constitutional norms…"For centuries courts have interpreted legislation to comply with common law values, not because compliance was necessary for validity, but because the values themselves were considered important. This reasoning applies with even greater force to entrenched constitutional values". Accordingly,

where legislation is permitting of two equal interpretations, the Court should adopt the interpretation which accords with *Charter* values.

The constitutional affinity between Part VI and section 8 of the *Charter* reinforces a need to ensure the former is not applied in a narrow manner that allows its objectives to be defeated through narrow or fixed interpretations.

Tse, *supra*, paras. 20-21 (citations omitted)

14. The Part VI framework is carefully designed to address specific problems arising from the state's ability to intercept private communications (*Tse*). This means that not all of its imperatives are suitable to all types of electronic surveillance. Where elements of the Part VI framework prove unworkable, or are otherwise clearly not applicable, courts have and should use restraint in applying the framework to evolved communications mechanisms. Some technological contexts may require the more nuanced protections that a Parliamentary process can offer (*TELUS; Lyons*). However, where there is ambiguity as to its potential scope of application, it should be resolved in favour of ensuring technological developments are not permitted to undermine the protections offered by Part VI. In addition, given the centrality of reasonable expectations in assessing the scope of section 8 protections, the concept of reasonable expectations can be a useful mechanism for informing such interpretations (*S.M.*).

Oliver, *supra*, p. 980; ***R. v. Telus Communications Company***, 2011 ONSC 1143, para. 61; ***S.M.***, *supra*., paras. 24-27; ***Tse***, *supra*; ***Lyons***, *supra*, p. 665

B. Evolving Communications Delivery & Temporary Storage

15. The general and technologically responsive nature of Part VI calls for interpretations catered to the technological context to which it is being applied. In this sense, many have recognized the challenges posed by technological evolutions in communications delivery to traditional privacy protections against interception. Voice-based communications are being supplanted in prominence by text-based (Short Messaging Service, Email) conversations that convey at least the same level of information. The largely instantaneous and linear communications process that was once common has been largely replaced by mechanisms that blur the line between 'storage' and 'in transit'. This means that "nearly all transient communication can now end up permanently and accessibly stored in the hands of third parties", which in turn become easily locatable, centralized targets for information gathering techniques. The speed and efficiency of these new communications techniques drives their broad adoption but the underlying delivery mechanisms themselves do little to "reduce the reasonable expectation of privacy users associate with [such] communication" (CBA). While not all of these challenges can be addressed through Part VI, they should inform the scope and limits of its application in a given technical context.

Appellant's Factum, para. 1 note 2; **CBA**, *supra*, p. 4; D. **Gilbert,** I. **Kerr** & J. McGill, "The Medium is the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers", (2007) 51(4) *Criminal Law Quarterly* 469; J. **Gruenspecht**, '"Reasonable' Grand Jury Subpoenas: Asking for Information in the Age of Big Data", (2011) 24(2) *Harv. J. L. & Tech.* 543, pp. 545, 548-55`; T. **Scassa**, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", (2010) 7 *Can. J. L. & Tech.* 193, pp. 204-207; ***U.S. v. Councilman***, 418 F.3d 67 (1st Circ., *En Banc*, 2005), p. 79; J. **Zittrain**, "Search and Seizures in a Networked World", (2006) 119 *Harv. L. Rev. Forum* 83

16. On the record of this proceeding, TELUS provides detailed descriptions of the delivery mechanism for its Short Messaging Service (SMS). TELUS employs a store and forward mechanism, which utilizes various databases and routing mechanisms. The first relevant mechanism a SMS message encounters when entering TELUS' delivery network is the Short Message Service Center (SMSC). At the SMSC, SMS messages are automatically stored for 5 days, during which time the SMSC employs various routing mechanisms in attempts to deliver any particular SMS message to its ultimate destination on an end device. In addition,

SMS messages are automatically copied to one of a set of three temporary storage databases (PSMS 1-3, collectively the 'database message engine'). Finally, SMS messages are subjected to automated processing and copied to another temporary storage database (PECSMS). Messages are retained in the PSMS and PECSMS databases for at least 30 days, but can be retained for as long as 45 days depending on manual purging processes.

> Affidavit (sworn June 25, 2010) and Supplementary Affidavit (sworn November 12, 2010) of **Don Calpito**, Appellant's Application for Leave to Appeal, *Telus Communications Company v. Her Majesty the Queen*, SCC File No. 34252

17. The SMSC is the delivery mechanism by which messages are sent to their final destinations. As SMS messages cannot be delivered to end devices that are not active, the 5 day retention period is necessary to ensure a high rate of delivery. The *sole* purpose of the temporary storage databases (PSMS and PECSMS) is to facilitate troubleshooting of SMS message delivery. The SMS message itself, as well as data about it are stored so that if there is, for example, a delivery failure, TELUS technicians will be able to easily locate the SMS message in question and to investigate technical delivery issues. It is these databases that are the object of the general warrant in the case at bar. All of these storage mechanisms are incidental to the message delivery process as their sole objective is to facilitate efficient message delivery. All of these storage mechanisms are temporary, as they are regularly and systematically deleted as a matter of course.

> **Calpito** Affidavit and Supplementary Affidavit

18. The 'store and forward' technology employed by TELUS for SMS message delivery (which is similar to that employed by Email protocols) is designed to permit a message to exist in more than one place at more than one time, distorting the once instantaneous and direct communications delivery process. A Department of Justice consultation document explains these challenges cogently. It notes, in the context of emails, how new methods of delivery:

> …create some confusion as to whether an e-mail should be seized or intercepted. The problem stems from how this "store and forward" technology works. It is in fact possible to access an e-mail at various places or at various stages of the communication or delivery process using various techniques.

In consequence, where communications under control of third party delivery mechanisms are at issue, it becomes increasingly difficult to demarcate 'in storage' from 'in transit'.

> **Department of Justice**, "Lawful Access – Consultation Document", August 25, 2002, ["**DOJ Consult**"], p. 15; ***Councilman***, *supra*, p. 79

19. The interpretive "morass" that can result from the move to new communications delivery technologies has been addressed in various legal contexts. While each solution is tailored to its own purposive and legislative context, notions of knowledge, control and passivity have played a central role in determining what conduct should or should not be legally salient. Particularly where dealing with communications intermediaries – entities that merely 'facilitate' communications between others – courts have also stressed the importance of adopting a purposive approach in order to determine whether a particular intermediary act is *intended* to be ancillary to a facilitating a communication or not.

> ***Councilman***, *supra*, pp. 80, 87, 89; **OECD**, "The Role of Internet Intermediaries in Advancing Public Policy Objectives", June 2011, DSTI/ICCP(2010)11/FINAL

20. **'No Transmission' Contract.** In *Electric Despatch v. Bell*, the defendant Bell had assigned its messenger service to the plaintiff. The assignment agreement included a non-competition clause by which Bell agreed to "in no manner and at no time...transmit or give,

directly or indirectly...any messenger...orders to any person...except the Electric Company". Bell's general purpose telephone service allegedly breached this agreement by allowing Bell customers to transmit, among other things, orders to any competitor of the plaintiff through Bell's telephone wires. However, as Bell remained "utterly ignorant of the nature of the message intended to be sent", its facilitative act was not a 'transmission' within the context of the contract. The Court additionally held that Bell's contractual obligations did not extend so far as to require it to *develop* the capacity to "intercept...all orders passing along the wires from one lessee to another which asks for a messenger or a cab..." Such capacity could only be achieved by "employing persons for the special purpose of spying and prying into every communication which passes along the wires" – a practice the Court found to be "by no means commendable".

> ***Electric Despatch Co. of Toronto v. Bell Telephone Co. of Canada*** (1891), 20 S.C.R. 83; ***Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)***, (2011) Case C-70/10 (European Court of Justice), paras. 1, 50-52

21. **Constructive Possession of Illegal Images.** Courts have rejected the notion that 'constructive possession' can occur where an illegal image from a remote website is merely viewed on a local computer. This is in spite of the fat that the viewing computer will create an automatic local copy of the file that can survive for several days:

> ...while it does not matter for the purposes of criminal possession how briefly one is in possession of the object, the thing said to be culpably possessed cannot...be essentially evanescent...When accessing Web pages, most Internet browsers will store on the computer's own hard drive a temporary copy of all or most of the files that comprise the Web page...While the configuration of the caching function varies and can be modified by the user, cached files typically include images and are generally discarded automatically after a certain number of days, or after the cache grows to a certain size. On my view of possession, the automatic caching of a file to the hard drive does not, without more, constitute possession. While the cached file might be in a "place" over which the computer user has control, in order to establish possession, it is necessary to satisfy *mens rea* or fault requirements as well. Thus, it must be shown that the file was *knowingly* stored and retained through the cache.
>
> ***R. v. Morelli***, 2010 SCC 8, paras. 28-38

22. **Communicating a copyrighted work.** The *Copyright Act* defines 'communicating to the public' as excluding any intermediary that merely provides the means for others to communicate. Whether a particular act of an intermediary qualifies as purely facilitative or not, is dependent on the extent to which the intermediary has control over a work being transmitted (para. 101) and knowledge of its infringing nature (paras. 89, 95, 99). The *purpose* of a given intermediary activity is also integral to its assessment. Specifically, periodic temporary storage of content by intermediaries remains 'mere conduit' activity if undertaken *for the purpose of facilitating downstream user communications in a more efficient manner*:

> 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.

Similarly, a download of a purchased work from an online vendor is not a communication, but "simply a technological taxi that delivers a durable copy...to the end user." 'Communication' must be interpreted with a mind to the purpose of the act in question, focused on whether a given transmission is "impermanent in nature, and does not leave the viewer...with a durable copy of the work" or, alternatively, is intended to furnish the end user with a durable copy "the user is meant to keep as [her] own".

> ***Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers***, [2004] 2 S.C.R. 427, at paras. 4, 6, 92-96; 114-116; ***ESA***, *supra*, paras. 5, 10, 28 and 36, 40-42

23. **Defamatory Communication.** While "facilitat[ing] the transfer of [defamatory] information" remains "a traditional hallmark of publication", merely linking to defamatory content "does not involve exerting *control* over the content". Hence, hyperlinking to defamatory content is not sufficiently robust an act to amount to communication of the linked content. Particularly with respect to the activities of intermediaries, some purely instrumental acts may be "so passive they should not be held to be publication" as such acts lack "knowing involvement" in the *specific* content in question. In undertaking definitional challenges of this nature, courts should avoid "formalistic application" of traditional rules that ignore the "importance of the communicative and expressive function" engaged. Statutory interpretations should seek to "accord with a more sophisticated appreciation of *Charter* values" as well as "with the dramatic transformation in the technology of communications."

Crookes v. Newton, 2011 SCC 47, paras. 21, 26-36, 51

24. A few principles can be extracted from these cases. First, Courts appear to recognize that care must be taken when assessing the legal salience of intermediary activity. Strict application of legal standards to activities merely facilitative of the communications of *others* can lead to adverse effects for important values such as innovation and economic efficiency (*SOCAN; ESA*), free expression (*Crookes*) and privacy (*Bell*). Second, and as a result, some acts of communications intermediaries are deemed not to have legal salience as they do no more than provide a 'conduit' for the activity of others. Third, in determining which intermediary activities should or should not 'count', the degree of knowledge, control and passivity of the intermediary with respect to the content being delivered are assessed. Where the intermediary has no *current* knowledge of the *specific* nature of the message (*Bell; SOCAN*), has exerted no editorial or creative control over the creation of the content (*Bell*; *Crookes*), and where its *purpose* for interacting with the content in question remains ancillary to facilitating communications (*ESA*; *SOCAN*; *Councilman*), its interactions are likely to be treated as mere conduit or background activities that are not legally salient. Finally, courts have specifically recognized that modern communications techniques require some degree of storage on the part of the intermediary in order to facilitate more efficient and accurate communications exchanges. Even where such storage is for several days, it is often treated as transient and temporary (*Morelli*; *SOCAN*).

Bell, *supra*.; ***Crookes***, *supra*, paras. 21, 26-36, 51; ***Councilman***, *supra*, p. 79; ***ESA***, *supra*, paras. 5, 10, 28 and 36, 40-42; ***Szymuszkiewicz***, *supra*, pp. 705-706; ***Morelli***, *supra*, paras. 28-38; ***SOCAN***, *supra*, paras. 4, 6, 92-96, 114-116

25. Applying these principles to TELUS' SMS message delivery mechanism can be instructive. TELUS automatically and indiscriminately caches *all* SMS messages that pass through its network. It does not choose to save some messages over others based on knowledge of their content. Unless there is a specific need to do so, TELUS does not interact with the contents of a particular message and purges all messages within 30-45 days of receipt. Messages are stored and accessed for the *sole* purpose of facilitating and troubleshooting message delivery. Arguably, where TELUS has (for the purpose of service quality control checks, for example) accessed a *specific* message and gained knowledge of its content, it might no longer be acting as a mere conduit with respect to that *particular* message (*Weir*). However, this appears to be the exception rather than the rule as the majority of TELUS' messages appear to enter and exit its various databases unread. Similarly, it could well be that Part VI will offer little assistance to remote storage scenarios where the end user retains control over what is stored with the intermediary and for how long (Zittrain). However, this is not the case with TELUS' message delivery service.

R. v. Weir, 2001 ABCA 181, paras. 3, 9; **Zittrain,** *supra*

C. 'Interception' of Stored Communications

26. It remains to apply these various principles to the specific interpretive task at hand. While the definition of 'interception' adopted in Part VI of the *Code* is facially broad enough to encompass the acquisition of private communications in storage, many courts have narrowed that definition to mean "interference between the place of origination and the place of destination of the communication". Some Courts have recognized the additional obligation that acquisition must occur 'contemporaneously' with the communication in order to qualify as an 'interception'. There is also wide-spread agreement that acquisition from the means of communications itself can be at the same time a Part VI interception *and* a 'seizure' of stored data.

DOJ Consult, *supra*, pp. 15-16; ***R. v. McQueen***, [1975] 25 C.C.C. (2d) 262 (Alta. C.A.); ***U.S. v. Szymuszkiewicz***, 622 F..3d 701 (7th Circ., 2010)

27. While Canadian courts have debated whether acquisition of stored data can amount to an 'interception', most decisions to date (see Respondent's Factum, para. 66, notes 103-104) involve scenarios where data is acquired from a different stage of the communications delivery process than the case at bar. Specifically, most relate to acquisition from an end device such as a cellular phone or computer. While this *can* amount to interception (*Bengert*), acquisition directly from the means of communications is different in character. When deposited in an end device, a communication is within the individual end-user's control, meaning that messages are retained selectively: "[m]any are deleted by the recipient upon reading – precisely because it is considered inappropriate or unnecessary to keep a record of such communication." (CBA) When acquisition is from an end device, it will typically be incidental to arrest (*Giles; Manley*) or to the acquisition of a computer or cellular phone during a warranted search of a location (*S.M.; Jones*). Such acquisition may raise the potential of self-incrimination (*Boudreau-Fontaine*; DOJ Consultation Document).

CBA, *supra*, p. 5; **DOJ Consult**, *supra*, p. 10; **Respondent's Factum**, para. 65 and notes 103-104 to para. 66; ***R. v. Bengert, Robertson et al. (No. 2)***, [1978] 47 C.C.C. (2d) 457 (B.C.S.C.); ***R. v. Boudreau-Fontaine***, 2010 QCCA 1108, para. 39; ***R. v. Giles***, 2007 BCSC 1147, paras. 11-14; ***R. v. Jones***, 2011 ONCA 632; ***R. v. Manley***, 2011 ONCA 128, paras. 35, 37-39; ***R. v. S.M.***, *supra* paras. 24-27

28. In the case at bar, the data being acquired remains in the third party intermediary's control. Parties to the communication have minimal control over retention of such communications, and will rarely be aware acquisition has occurred. There is a "fundamental difference" between surreptitious acquisition from a third party and acquisition of messages "sent, received and resid[ing] at their destination" (*Giles*). In such contexts, it is important to prevent privacy protections associated with communications are not "in any way diminished as a result of the channeling of the data which constitutes the communication." (CBA) Such technical neutrality in application is particularly important in light of technological innovations in message delivery that challenge traditional notions of 'storage' and 'in transit' such as those employed by TELUS here.

CBA, *supra*, p. 4; ***R. v. Giles***, *supra*, para. 34

29. It may well be that the instant a message arrives at its end point, it is 'in storage' and no longer capable of being 'intercepted' (*McQueen; Bengert; S.M; Councilman*). If the same rule applied to storage on servers of communications intermediaries, it would place *most* Internet-based communications "outside the scope of the provisions of Part VI" (*Szymuszkiewicz; Giles*). While the need for flexible storage/in transit dichotomies has been recognized, the interpretive "morass" of how to assess such dichotomies in the context of Part VI protections remains open. Many seek to draw the line at the point where the message is read by the recipient, but this does not seem to address the realities of modern message delivery mechanisms. Attempting to graft this concept directly onto store and forward delivery mechanisms yields results that are "illogical and impractical" (*TELUS*). This is because the

correlation between 'in transit on the delivery network' and 'read by recipient' is now tenuous at best (DOJ Consult).

> ***Bengert***, *supra*, paras. 7-12; ***Councilman***, *supra*, pp. 72-73, 79, 80, 87 and 89; **DOJ Consult**, p. 16; ***Giles***, *supra*, para. 43; ***McQueen***; ***S.M.***, *supra*, para. 19; ***TELUS***, *supra*, paras. 59-61

30. U.S. Courts have rejected rigid 'storage/in transit' distinctions and deemed to include temporary storage that is incidental to the delivery process as part and parcel of a communications delivery transaction (*Councilman; Szymuszkiewicz*):

> In saying that the rerouting of the information was contemporaneous with the transit of each email, we do not imply agreement with any statement that the interception must be "contemporaneous." Decisions articulating such a requirement are thinking football rather than the terms of the statute. There is no timing requirement in the Wiretap Act, and judges ought not add to statutory definitions…

There is as yet no clear authority on what might constitute 'temporary/transient' storage or what acts might be deemed 'incidental to the delivery process' as of yet, a principled basis for such distinctions exists. Where, as here, intermediary storage is inherently *temporary* (*Councilman*; *Morelli*; *SOCAN*), where it is processed automatically, without *knowing discrimination* based on the *content* of specific messages (*Bell*; *SOCAN*; *SABAM*), and where it is for the *purpose* of merely facilitating the efficiency or accuracy of the communications delivery process (*SOCAN*; *ESA*), such storage should be treated as mere conduit activity that is "necessary", "intrinsic" or "incidental" to the communications facilitation process (*SOCAN*; *Councilman*).

> ***Bell***, *supra.*; ***Crookes***, *supra*, paras. 21, 26-36, 51; ***Councilman***, *supra*, pp. 79-80 and 87, 89; ***ESA***, *supra*, paras. 5, 10, 28 and 36, 40-42; ***Szymuszkiewicz***, *supra*, pp. 705-706; ***Morelli***, *supra*, paras. 28-38; ***SABAM***, *supra*, paras. 50-52; ***SOCAN***, *supra*, paras. 4, 6, 92-96, 114-116

31. In addition, where Courts are particularly likely to disregard mere conduit activity where doing so advances important *Charter* values such as privacy (*Crookes*; *Bell*; *SABAM*). In this particular case, allowing TELUS' temporary storage activities to bring its message delivery services outside the scope of what constitutes an 'interception' will deprive Canadians of the special protections offered by Part VI to their private text communications. General warrants do not present comparable protection, as they lack notice requirements and do not limit interception to serious offences or scenarios where serious harm can arise (*Tse*). Individuals will not know, in many cases, whether their communications have been intercepted, leading to potential chilling effects on the (*Duarte*). They employ no reporting mechanism, meaning that interceptions diverted away from the traditional Part VI interception regime will be excluded from annual calculations of the changing scope of electronic surveillance of communications (Forbes). There are no direct imperatives protecting privileged information (s. 186(2)-(3)). There is no exhaustion requirement (paragraph 186(1)(b)), raising the risk such interceptions will become "a humdrum and routine administrative manner" (*Duarte*).

> ***Bell***, *supra.*; ***Criminal Code***, s. 186; ***Crookes***, *supra*, paras. 21, 26-36, 51; ***Duarte***, *supra*, paras. 35-36, 47; ***SABAM***, *supra*, paras. 50-53; ***Tse***, *supra*.

32. Use of general warrants in such contexts directly bypasses these important protections, which Parliament has carefully tailored to protect private communications of Canadians against unauthorized acquisition 'between the place of origination and the place of destination of the communication.' Indeed, given the high costs involved with the types of daily production processes contemplated by this general warrant, TELUS may well opt to voluntarily employ their operative real-time text message forwarding mechanism instead, particularly if such orders become common practice. Under the rule proposed by the respondent, it is not clear what existing legal impediments might prevent TELUS from doing so voluntarily in response to anticipatory general warrant requests and the economic incentives, even if these are deemed 'reasonable' (*TELUS*) greatly favour doing so.

> ***TELUS***, supra, para. 81

D. Overlap: General Warrants, Production Orders & Part VI

33. CIPPIC submits that the particular case at bar constitutes an 'interception' within the context of Part VI of the *Code*. However, two additional scenarios are raised by the facts of this case that warrant comment. First, the Court should not permit the use of general warrants to undermine express privacy protections placed in the *Code*. In cases where, for example, private data already in existence is under the control of a third party such as an email service provider, but is *not* in temporary storage for purposes ancillary to message delivery, general warrants such as that employed in the case at bar should be avoided. Such warrants bypass express protections put in place to limit the scope of production orders to data "already in existence" and "in possession or control" of the object of the order (s. 487.012(1)(b) and (3)(c)). The general warrant at issue in this case transforms the backward looking production orders Parliament enacted into "anticipatory orders" that "permit…monitor[ing] transactions for a specified period of time" on an ongoing basis (DOJ Consult). Anticipatory warrants also blur the line between 'production', 'preservation' and 'retention/recording'. While the warrant at issue here only required TELUS to produce messages in its control at the end of a set 24 hour period, it is questionable whether TELUS retained its discretion to delete messages covered by the general warrant.

> ***Criminal Code***, *supra*, s. 487.012 **DOJ Consult**, *supra*, pp. 10-11, 14

34. Second, there may be some scenarios where Part VI authorized acquisition may overlap with access by means of production orders. That is, where private communications held in temporary storage by a communications intermediary for purposes ancillary to message delivery are at the same time data "already in existence" and "in possession or control" of a third party (s. 487.012). In such scenarios, the prohibition on interception found in Part VI should be pre-eminent. There is U.S. precedent for such an approach, as two Circuits have rejected claims that the existence of overlapping 'stored communications' access provisions might in some way vitiated more rigorous obligations attaching to 'interceptions' or private communications (*Councilman*; *Szymuszkiewicz*; Respondent's Factum). Precedent aside, it is unclear how the mere availability of overlapping alternative acquisition powers in the *Criminal Code* could diminish the need to meet the authorization requirements in Part VI. Whereas these other powers are permissive, Part VI imposes a direct prohibition on interception, to which narrow and specific exceptions exist. If Part VI was capable of being undermined by the mere presence of alternative acquisition powers, Part VI protections could quickly become irrelevant. For example, s. 487(2.1) could be used to cause telecommunications companies to search 'computer systems' in their facilities and reproduce or output details of real-time telecommunications. In *Councilman*, the emails were intercepted from the "random access memory (RAM) or..the hard disks, or both, within [the defendant's] computer system."

> ***Councilman***, *supra*, pp. 81-82; ***Criminal Code***, *supra*, s. 487.012; **DOJ Consult**, *supra,* pp. 10-11; **Respondent's Factum**, paras. 65, 41; ***Szymuszkiewicz***, *supra*, p. 706

PART IV – COSTS

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

PART V – ORDERS SOUGHT

36. CIPPIC respectfully requests that the appeal be granted and that the Court take its submissions into account when deciding the matter under appeal.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 16th day of September, 2012

[original signed]

Tamir Israel

Samuelson Glushko Canadian Internet Policy
and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
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.	***Crookes v. Newton***, 2011 SCC 47	23, 30-31
2.	***Electric Despatch Co. of Toronto v. Bell Telephone Co. of Canada*** (1891), 20 S.C.R. 83, [Bell]	20, 24, 30-31
3.	***Entertainment Software Association v. Society of Composers, Authors and Music Publishers of Canada***, 2012 SCC 34, [ESA]	10, 22, 24
4.	***Lyons v. The Queen***, [1984] 2 S.C.R. 633	4, 8, 10-11, 14
5.	***R. v. Bengert, Robertson et al. (No. 2)***, [1978] 47 C.C.C. (2d) 457 (B.C.S.C.)	27, 29
6.	***R. v. Boudreau-Fontaine***, 2010 QCCA 1108	27
7.	***R. v. Duarte***, [1990] 1 S.C.R. 30	3, 5-6, 8-9, 31
8.	***R. v. Giles***, 2007 BCSC 1147	27-28
9.	***R. v. Jones***, 2011 ONCA 632	27
10.	***R. v. Manley***, 2011 ONCA 128	27
11.	***R. v. McQueen***, [1975] 25 C.C.C. (2d) 262 (Alta. C.A.)	26, 29
12.	***R. v. Morelli***, 2010 SCC 8	21, 24, 30
13.	***R. v. S.M.***, 2012 ONSC 2949	5, 14, 27, 29
14.	***R. v. Telus Communications Company***, 2011 ONSC 1143, [TELUS]	14, 29, 32
15.	***R. v. Tessling***, 2004 SCC 67	5-7
16.	***R. v. Tse***, 2012 SCC 16	4, 13-14, 31
17.	***R. v. Weir***, 2001 ABCA 181	25
18.	***R. v. Wong***, [1990] 3 S.C.R. 36	7
19.	***Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)***, (2011) Case C-70/10 (European Court of Justice), [SABAM]	20, 30-31
20.	***Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers***, [2004] 2 S.C.R. 427, [SOCAN]	22, 24, 30

PART VII – LEGISLATION

Criminal Code, S.C., 1985, c. C-46, Part VI, excerpts

Definitions

183. In this Part,

"authorization" means an authorization to intercept a private communication given under section 186 or subsection 184.2(3), 184.3(6) or 188(2);

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;

[…]

Interception

184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

Saving provision

(2) Subsection (1) does not apply to

(*a*) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;

(*b*) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;

(*c*) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service;

(*d*) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or

(*e*) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication

originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for

(i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or

(ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).

Use or retention

(3) A private communication intercepted by a person referred to in paragraph (2)(*e*) can be used or retained only if

(*a*) it is essential to identify, isolate or prevent harm to the computer system; or

(*b*) it is to be disclosed in circumstances referred to in subsection 193(2).

R.S., 1985, c. C-46, s. 184; 1993, c. 40, s. 3; 2004, c. 12, s. 4.

Application for authorization

185. (1) An application for an authorization to be given under section 186 shall be made ex parte and in writing to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 and shall be signed by the Attorney General of the province in which the application is made or the Minister of Public Safety and Emergency Preparedness or an agent specially designated in writing for the purposes of this section by

(*a*) the Minister personally or the Deputy Minister of Public Safety and Emergency Preparedness personally, if the offence under investigation is one in respect of which proceedings, if any, may be instituted at the instance of the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or

(*b*) the Attorney General of a province personally or the Deputy Attorney General of a province personally, in any other case,

and shall be accompanied by an affidavit, which may be sworn on the information and belief of a peace officer or public officer deposing to the following matters:

(*c*) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence,

(*d*) the type of private communication proposed to be intercepted,

(*e*) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used,

(*f*) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (*e*) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made,

(*g*) the period for which the authorization is requested, and

(*h*) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

Exception for criminal organizations and terrorist groups

(1.1) Notwithstanding paragraph (1)(*h*), that paragraph does not apply where the application for an authorization is in relation to

(*a*) an offence under section 467.11, 467.12 or 467.13;

(*b*) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or

(*c*) a terrorism offence.

Extension of period for notification

(2) An application for an authorization may be accompanied by an application, personally signed by the Attorney General of the province in which the application for the authorization is made or the Minister of Public Safety and Emergency Preparedness if the application for the authorization is made by him or on his behalf, to substitute for the period mentioned in subsection 196(1) such longer period not exceeding three years as is set out in the application.

Where extension to be granted

(3) Where an application for an authorization is accompanied by an application referred to in subsection (2), the judge to whom the applications are made shall first consider the application referred to in subsection (2) and where, on the basis of the affidavit in support of the application for the authorization and any other affidavit evidence submitted in support of the application referred to in subsection (2), the judge is of the opinion that the interests of justice warrant the granting of the application, he shall fix a period, not exceeding three years, in substitution for the period mentioned in subsection 196(1).

Where extension not granted

(4) Where the judge to whom an application for an authorization and an application referred to in subsection (2) are made refuses to fix a period in substitution for the period mentioned in subsection 196(1) or where the judge fixes a period in substitution therefor that is less than the period set out in the application referred to in subsection (2), the person appearing before the judge on the application for the authorization may withdraw the application for the authorization and thereupon the judge shall not proceed to consider the application for the authorization or to give the authorization and shall return to the person appearing before him on the application for the authorization both applications and all other material pertaining thereto.

R.S., 1985, c. C-46, s. 185; 1993, c. 40, s. 5; 1997, c. 18, s. 8, c. 23, s. 4; 2001, c. 32, s. 5, c. 41, ss. 6, 133; 2005, c. 10, ss. 22, 34.

Judge to be satisfied

186. (1) An authorization under this section may be given if the judge to whom the application is made is satisfied

(*a*) that it would be in the best interests of the administration of justice to do so; and

(*b*) that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

Exception for criminal organizations and terrorism offences

(1.1) Notwithstanding paragraph (1)(*b*), that paragraph does not apply where the judge is satisfied that the application for an authorization is in relation to

(*a*) an offence under section 467.11, 467.12 or 467.13;

(*b*) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or

(*c*) a terrorism offence.

Where authorization not to be given

(2) No authorization may be given to intercept a private communication at the office or residence of a solicitor, or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients, unless the judge to whom the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any other such solicitor or a member of the solicitor's household has been or is about to become a party to an offence.

Terms and conditions

(3) Where an authorization is given in relation to the interception of private communications at a place described in subsection (2), the judge by whom the authorization is given shall include therein such terms and conditions as he considers advisable to protect privileged communications between solicitors and clients.

Content and limitation of authorization

(4) An authorization shall

(*a*) state the offence in respect of which private communications may be intercepted;

(*b*) state the type of private communication that may be intercepted;

(*c*) state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given, and generally describe the manner of interception that may be used;

(*d*) contain such terms and conditions as the judge considers advisable in the public interest; and

(*e*) be valid for the period, not exceeding sixty days, set out therein.

Persons designated

(5) The Minister of Public Safety and Emergency Preparedness or the Attorney General, as the case may be, may designate a person or persons who may intercept private communications under authorizations.

Installation and removal of device

(5.1) For greater certainty, an authorization that permits interception by means of an electro-magnetic, acoustic, mechanical or other device includes the authority to install, maintain or remove the device covertly.

Removal after expiry of authorization

(5.2) On an ex parte application, in writing, supported by affidavit, the judge who gave an authorization referred to in subsection (5.1) or any other judge having jurisdiction to give such an authorization may give a further authorization for the covert removal of the electro-magnetic, acoustic, mechanical or other device after the expiry of the original authorization

(*a*) under any terms or conditions that the judge considers advisable in the public interest; and

(*b*) during any specified period of not more than sixty days.

Renewal of authorization

(6) Renewals of an authorization may be given by a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 on receipt by him or her of an ex parte application in writing signed by the Attorney General of the province in which the application is made or the Minister of Public Safety and Emergency Preparedness — or an agent specially designated in writing for the purposes of section 185 by the Minister or the Attorney General, as the case may be — accompanied by an affidavit of a peace officer or public officer deposing to the following matters:

(*a*) the reason and period for which the renewal is required,

(*b*) full particulars, together with times and dates, when interceptions, if any, were made or attempted under the authorization, and any information that has been obtained by any interception, and

(*c*) the number of instances, if any, on which, to the knowledge and belief of the deponent, an application has been made under this subsection in relation to the same authorization and on which the application was withdrawn or no renewal was given, the date on which each application was made and the name of the judge to whom each application was made,

and supported by such other information as the judge may require.

Renewal

(7) A renewal of an authorization may be given if the judge to whom the application is made is satisfied that any of the circumstances described in subsection (1) still obtain, but no renewal shall be for a period exceeding sixty days.

R.S., 1985, c. C-46, s. 186; 1993, c. 40, s. 6; 1997, c. 23, s. 5; 1999, c. 5, s. 5; 2001, c. 32, s. 6, c. 41, ss. 6.1, 133; 2005, c. 10, ss. 23, 34.

Criminal Code, S.C., 1985, c. C-46, s. 487.012

Production order

487.012 (1) A justice or judge may order a person, other than a person under investigation for an offence referred to in paragraph (3)(*a*),

(*a*) to produce documents, or copies of them certified by affidavit to be true copies, or to produce data; or

(*b*) to prepare a document based on documents or data already in existence and produce it.

Production to peace officer

(2) The order shall require the documents or data to be produced within the time, at the place and in the form specified and given

(*a*) to a peace officer named in the order; or

(*b*) to a public officer named in the order, who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

Conditions for issuance of order

(3) Before making an order, the justice or judge must be satisfied, on the basis of an ex parte application containing information on oath in writing, that there are reasonable grounds to believe that

(*a*) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;

(*b*) the documents or data will afford evidence respecting the commission of the offence; and

(*c*) the person who is subject to the order has possession or control of the documents or data.

Terms and conditions

(4) The order may contain any terms and conditions that the justice or judge considers advisable in the circumstances, including terms and conditions to protect a privileged communication between a lawyer and their client or, in the province of Quebec, between a lawyer or a notary and their client.

Power to revoke, renew or vary order

(5) The justice or judge who made the order, or a judge of the same territorial division, may revoke, renew or vary the order on an *ex parte* application made by the peace officer or public officer named in the order.

Application

(6) Sections 489.1 and 490 apply, with any modifications that the circumstances require, in respect of documents or data produced under this section.

Probative force of copies

(7) Every copy of a document produced under this section, on proof by affidavit that it is a true copy, is admissible in evidence in proceedings under this or any other Act of Parliament and has the same probative force as the original document would have if it had been proved in the ordinary way.

Return of copies

(8) Copies of documents produced under this section need not be returned.

2004, c. 3, s. 7.