The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference

Volume 71 (2015) Article 19

Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence

Susan Magotiaux

Citation Information

Magotiaux, Susan. "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence." *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 71. (2015).
http://digitalcommons.osgoode.yorku.ca/sclr/vol71/iss1/19

Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence

Susan Magotiaux[*]

I. INTRODUCTION

Canadian legislation on police powers in the criminal sphere have recently been "updated" and the Supreme Court of Canada has considered and pronounced on conflicts of privacy and investigation in a digital context. But are we doing enough to adapt to the changing context or are we out of sync?

This article offers a review of recent Supreme Court of Canada search and seizure cases to demonstrate the awkward ongoing waltz of old law and new technology. In 2013-2014, the Supreme Court decided *R. v. Vu*,[1] *R. v. TELUS Communications Co.*,[2] *R. v. Spencer*[3] and *R. v. Fearon*;[4] four cases addressing the parameters of section 8 of the Charter[5] in the context of computers, digital communications, Internet subscriber information and mobile phones, respectively. In each case the Court was forced to confront the ill-matched partnership between technology and legal principle. Is a computer a thing? Are texts like conversations? When is a phone like a computer? When is a computer like a filing cabinet? Can we claim anonymity online? The carefully crafted answers are meaningful, but the time lag between actual technological developments and consideration of the limits of police powers in using those advancements hampers law enforcement and leaves rights-holders suspicious and uncertain. It's an ill-fated marriage; law and technology.

---

* Counsel, Crown Law Office Criminal, Ministry of the Attorney General for Ontario. The views expressed in this article are those of the author alone.

1 [2013] S.C.J. No. 60, [2013] 3 S.C.R. 657, 2013 SCC 60 (S.C.C.) [hereinafter "*Vu*"].

2 [2013] S.C.J. No. 16, [2013] 2 S.C.R. 3, 2013 SCC 16 (S.C.C.) [hereinafter "*TELUS*"].

3 [2014] S.C.J. No. 43, [2014] S.C.R. 212, 2014 SCC 43 (S.C.C.) [hereinafter "*Spencer*"].

4 [2014] S.C.J. No. 77, [2014] 3 S.C.R. 621, 2014 SCC 77 (S.C.C.) [hereinafter "*Fearon*"].

5 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter "Charter"].

One is the result of researched, reasoned, incremental progress, the other a dash of innovation and experiment. No wonder we can't keep up.

Police seeking guidance are met with confusion. Section 8 of the Charter protects citizens from unreasonable search and seizure. Since *Hunter v. Southam*[6] in 1984, the starting place for a constitutional search is pre-authorization. Technology challenges our ability to plan ahead. For computer searches, officers increasingly don't know where evidence will be, in what form, or how it may be accessed. Data cannot always be seized, brought back and examined later. Leaving aside the technical question of *how* things can be seized, the "*what*" and "*why*" of privacy determinations are also moving targets. Figuring out what will be reasonable, on a normative appreciation of privacy, is a daunting task not well suited to frontline investigatory work.

The potential for the commission and facilitation of crime online, and the amplified impact and permanence of harm done to some victims of crime cannot be forgotten in the dialogue. Safety, security and the suppression of crime are legitimate countervailing concerns. As succinctly put by Binnie J. in *R. v. Tessling*, the community wants privacy but it also insists on protection.[7] The Supreme Court of Canada has repeatedly rooted privacy decisions in the values and reasonable expectations of Canadians, not in the technical fine-points of a given intrusion.[8] The focus is and should remain on what we are willing to give up in the ground between privacy and law enforcement objectives, not on what tools will we use to carve the dividing line in any given case. Section 8 jurisprudence has developed with a lens wide enough to encompass the changing tides of technology.[9]

II. SECTION 8 AND "NEW" TECHNOLOGY IN THE SUPREME COURT

Police powers get tested against the section 8 standard in the courtroom. As social behaviour changes and lives are lived increasingly online or leaving traceable digital breadcrumbs, it is of course logical that investigation of crime will engage more and more technological tools and digital landscapes. Police will capture digital evidence,

---

6 *Hunter v. Southam Inc*., [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145 (S.C.C.).

7 *R. v. Tessling*, [2004] S.C.J. No. 63, [2004] 3 S.C.R. 432, 2004 SCC 67, at para. 17 (S.C.C.) [hereinafter "*Tessling*"].

8 *Id.*, at paras. 29-30; *R. v. Wong*, [1990] S.C.J. No. 118, [1990] 3 S.C.R. 36, at 43-44 (S.C.C.) [hereinafter "*Wong*"].

9 *Wong*, *id.*, at 44.

prosecutors will bring cases of cybercrime and judges will be called upon to draw reasonable boundaries in an uncertain field.

The struggle to understand new technology and apply legal principles is not new. The fundamental and normative principles of privacy that guide Canadian courts can and do adapt to brave new worlds. *Vu*, *Fearon* and *Spencer* offer some salient examples of practical application of traditional search principles in the technological age. They offer warnings too. Both must be heeded if we are to successfully navigate these uncharted waters.

1. Is it a Bird? Is it a Plane?

There is nothing new about approaching new information by trying to fit it into existing paradigms. Start with what you know. But in many cases, technology shifts too far for analogy to past experience to be instructive. For computers and other digital devices, attempts to analogize to more traditional tangibles have recently been curtailed.

In *Vu*, Cromwell J., writing for the Supreme Court of Canada, conclusively settled the debate; computers are not like filing cabinets. They are not like briefcases, and cannot be approached in the same fashion in applying section 8 analysis and determining where the individual's right to be left alone is drawn. A warrant can authorize a search through whatever cupboards and closets may contain the items to be seized, but it cannot authorize dumping the digital drawers of a computer without explicit reference. Justice Cromwell noted that computers differ in important ways from the receptacles we have considered under the traditional section 8 framework and computer searches give rise to unique privacy concerns that are not adequately addressed by the "old" approach.[10] Post-*Vu*, police must obtain specific pre-authorization to search a computer.[11]

The discarding of analogies to non-digital receptacles was an important and necessary step in bringing search law up to date. Not just because of the sheer amount of information potentially accessible to authorities on a personal computer, but, as explored in *Vu*, because the nature of digital information and evidence is of different quality in ways

---

[10] *Vu*, *supra*, note 1, at para. 2.

[11] *Vu* does leave room for the unanticipated find; a device found when executing a warrant can be seized for preservation and a fresh authorization sought to particularly address the authorization for computer search, *Vu*, *supra*, note 1, at para. 49.

that matter in the privacy debate. Unlike in cupboards and desks, digital data is created without conscious action or even knowledge of the user and may remain, in recoverable form, when the user tries to destroy it. The individual control over personal information is reduced in digital data, and control over information is a key component to informational privacy.[12]

In *Fearon*, Cromwell J., again writing for the Court, maintained the consistent message that digital devices require a fresh approach. Cell phones and other mobile communications devices, like the computers considered in *Vu*, cannot be understood for section 8 purposes as the equivalent of briefcases and purses.[13] Again, the Court emphasized the nature and scope of the information potentially (though not inevitably) accessible to law enforcement through the digital device and found that the new technologies required a new and specific restraint of police power.

The *Fearon* majority made the important point that courts should avoid crafting different tests for the different capabilities of individual technological devices.[14] Examination or search of computers and smartphones does not inherently or inevitably result in a vast invasion of personal privacy. The device itself may not contain intimate details, and, significantly, police can be constrained in examination. As demonstrated in *Fearon*, it is possible to add safeguards to the exercise of police power to ensure section 8 compliance. The majority imposed measures to limit the potential privacy intrusion by modifying the common law search incident to arrest power and rejected the "all or nothing" approach.

2. *R. v. Spencer* — A New Normative

Section 8 cases struggle with the balance between individual intrusions and law enforcement objectives. Finding the line is an exercise in value interpretation. The broader context complicates our sense of normal. The world has changed rapidly. That is hardly a new sentiment.[15] But in the specific realm of public accessibility of personal information, the daily lives of young Canadians display a seismic shift from former

---

[12] *Vu*, *supra*, note 1, at para. 24. See also paras. 40-44.

[13] *Fearon*, *supra*, note 4, at para. 51.

[14] *Fearon*, *supra*, note 4, at para. 52.

[15] See discussion of public fear at the introduction of the threatening new technology of Kodak in 1902 in Omer Tene & Jules Polonetsky, "A Theory of Creepy: Technology, Privacy and Shifting Social Norms" (2013) 16 Yale J.L. & Tech 59, at 72.

generations. Classrooms have twitter feeds, pre-teens have YouTube channels, and images of our families, our pets, our food, our fashion, our failures and our friends are posted or transmitted in ever-growing circles, out of our control. Emotions are expressed with emoticons. Relationships bloom, grow and wither with no in-person contact; love at first site, first byte. Businesses gather and collate our mass digital dalliances to predict our preferences and provide us with better more individualized products and services.[16] That's "normal".

There is and absolutely should be a high standard for state access to the personal pieces we wish to guard, but courts, or rather judges, who may not be personally entrenched in the digital norm of today's youth, cannot be expected to measure with precision the social temperature on privacy. We want privacy but we want publicity too. We overshare but might later wish for over-protection, though it is well-accepted that the Charter does not protect want we want to be kept confidential, only what we can reasonably expect to keep private.[17]

In *Tessling*, Binnie J., for the Court, remarked that "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place".[18] In the "public" spaces of online activity, the line is no longer as clear.

In *Spencer*, the Court addressed file-sharing over public paths and the scope of police power to put a subscriber's name and address to a publicly broadcast Internet Protocol ("IP") address.

Spencer's actual finding was of limited scope; police must now obtain prior judicial authorization to access basic subscriber information from an Internet Service Provider ("ISP"). The discussion around how courts approach and should approach privacy dialogue in a digital age was far-reaching. Privacy is a normative concept. It must be considered anew in each context. Courts assessing privacy interests must consider not only what we actually believe is confidential or protected, but also what we want to be private.[19] The social values of Canadian society weigh heavily in the mix. Social values, of course, change and conflict.

---

[16] Tene & Polonetsky provide a review of various corporate attempts at data analysis and tailored marketing and service-delivery and the mixed consumer response to use of data.

[17] *Tessling*, *supra*, note 7, at para. 26.

[18] *Id.*, at para. 40.

[19] *Spencer*, *supra*, note 3, at para. 18; *Tessling*, *supra*, note 7, at para. 42; *R. v. Patrick*, [2009] S.C.J. No. 17, [2009] 1 S.C.R. 579, 2009 SCC 17, at para. 14 (S.C.C.).

In *Spencer*, the Supreme Court of Canada explored an emerging concept in the privacy debate; a right to anonymity.[20] *Spencer* broke new ground in search law by defining informational privacy as comprised of three elements: secrecy, control and anonymity.[21] The concept of anonymity was "not novel" but the application to the Internet context and the suggestion of a right to anonymity in the online world is an extension of uncertain ambit. The Court acknowledged the concern that over-extension of online anonymity protection could impede the investigation of Internet crime, but responded that "recognizing that there *may* be a privacy interest in anonymity depending on the circumstances falls short of recognizing any 'right' to anonymity and does not threaten the effectiveness of law enforcement in relation to offences committed on the Internet".[22] While a totality of circumstances test can never offer precise predictability, it is questionable how police will translate such nuanced analysis into frontline decisions about the scope of their powers.

3. The Third Party Problem

In traditional search analysis, when evidence was found in shoe boxes and file cabinets, courts could analyze assertions of privacy by reference to such (non-exhaustive) factors as ownership and the ability to exercise control over a space or to exclude people.[23] Now we cannot exclude the third parties from our information, though many could, practically speaking, exclude us. A web-based e-mail service may choose to preserve what the user would prefer to erase.[24] A company, within the bounds of privacy legislation and court orders, sets policy on when and how it will provide data to police, and the contracts imposed on users ultimately come to factor into the decision on what we expected and could reasonably expect to remain private. *Spencer* demonstrated the

---

[20] The concept of a right to Internet anonymity was earlier developed in a very similar context by Doherty J.A. writing for the Ontario Court of Appeal in *R. v. Ward*, [2012] O.J. No. 4587, 2012 ONCA 660, 112 O.R. (3d) 321, at paras. 70-75 (Ont. C.A.). Justice Doherty's analysis was cited with approval in *Spencer*, *supra*, note 3, at para. 48.

[21] *Spencer*, *supra*, note 3, at para. 4.

[22] *Id.*, at para. 49.

[23] *R. v. Edwards*, [1996] S.C.J. No. 11, [1996] 1 S.C.R. 128, at para. 45 (S.C.C.). Of course, the Supreme Court has adapted the framework for questions of informational privacy and applied analysis to developing technologies and computer contexts: *R. v. Plant*, [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281, at 45 (S.C.C.); *Tessling*, *supra*, note 7, at para. 32; *R. v. Cole*, [2012] S.C.J. No. 53, [2012] 3 S.C.R. 34, 2012 SCC 53, at paras. 39-58 (S.C.C.).

[24] See discussion of *TELUS*, below.

difficult decision as to how to weigh contractual terms in the privacy balance.[25] While the Court in *Spencer* found that there is "no doubt" that contractual and statutory schemes play an important role in the reasonable expectation of privacy analysis, their weight in the balance is uncertain.[26]

Our lack of control over digital information in the hands of third parties is a social problem beyond the criminal arena. Permanence of past slips is a pressing global concern. The Court of Justice of the European Union issued a ground-breaking judgment in May 2014, finding that a person had a "right to be forgotten" and that an Internet search engine had a legal obligation to act on personal requests to remove links to historical information that was accurate when posted but is irrelevant, inadequate or excessive in light of passage of time.[27] The decision has sparked international conversation and debate about the ability to regulate the Internet and exercise control over information in the public domain.[28] Freedom of expression clashes with freedom from the permanent links of history, but it is Google that must balance the interests of the individual requester and the public interest in access to information. No one is quite sure where privacy interests lay, or how they change with age.

4. Passwords and Protocols

The Supreme Court has effectively (and wisely) avoided pushing judges too far into the forensic technology world at the stage of judicial pre-authorization for anticipated search and seizure. In *Vu*, the Court

---

[25] *Spencer*, *supra*, note 3, at paras. 52-60. See also *R. v. Gomboc*, [2010] S.C.J. No. 55, [2010] 3 S.C.R. 211, 2010 SCC 55 (S.C.C.).

[26] *Spencer*, *supra*, note 3, at para. 54.

[27] *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, OJ C 165, 9.6.2012, Case C-131/12, Court of Justice, May 13, 2014. See also Google's Report on implementation of the judgment "The Advisory Council to Google on the Right to be Forgotten", February 6, 2015, accessed April 3, 2015 online: <https://www.google.com/advisorycouncil/>.

[28] See for example: Katie Engelhart, "The right to be forgotten online: Will it ruin the Internet?", *MacLean's*, November 10, 2014, accessed April 2, 2015 online: <http://www.macleans.ca/news/world/the-right-to-be-forgotten-online-will-it-ruin-the-internet/>; François LeBel & Mandy Woodland, "The Right to be Forgotten", Privacy Pages, October 2014 – CBA National Privacy and Access Law Section Newsletter, accessed April 1, 2015 online: <http://www.cba.org/CBA/sections_privacy/newsletters2014/forgotten.aspx.>; and Andre Mayer, "'Right to be forgotten': How Canada could adopt similar law for online privacy", June 16, 2014, accessed April 3, 2015 online: <http://www.cbc.ca/news/technology/right-to-be-forgotten-how-canada-could-adopt-similar-law-for-online-privacy-1.2676880>.

considered and rejected a proposal that all computer searches be pre-authorized with a specific examination protocol.[29] Although judicial officers retain the discretion to impose conditions in any warrant to search, extending the obligation to require advance approval of the detailed manner of search would be impractical, if not impossible, and is not required to ensure constitutionality of a computer search. The Court recognized that technological advancement leads to uncertainty in predicting the investigative tools that may be required to meet law enforcement objectives in a given case. Evidence cannot be found in discrete "places" on a device, and all manner of methods may be used to "hide" evidence. Without knowing in advance how devices or technology has been used, police cannot rationally set plans for forensic examination, and judicial officers cannot be expected to meaningfully evaluate any such technical strategy.

Search protocols may be possible in the right case, and may be imposed under the discretionary powers of an issuing justice. Although finding that protocols were not constitutionally required, the Supreme Court acknowledged that Parliament could take action in delineating standard conditions, and that police could, where appropriate in the circumstances, return to a justice post execution to seek a second authorization with clarified terms or limits reflective of the preliminary discovery and informed assessment of necessary tools and examination.[30] The Court allowed for room to grow into our technological understanding. For now, in most cases of computer seizure, it is highly unlikely that police could set out with any kind of useful precision the exact pathways and plans for a digital examination. Any current forensic strategies may well be obsolete between drafting and application given the speed and permutations of technological advancement.

Protocols were approached with caution in *Vu* and passwords were similarly sidelined as the arbiters of privacy in *Fearon*, where the Supreme Court dialled back the technical distinction that had gained traction in lower courts.[31] The *Fearon* Court dismissed an argument that the presence or absence of a password should be definitive in the privacy analysis. Again, it was a practical approach. It is dangerous to ascribe legal meaning to an ill-understood feature of some devices, some of the time. In the cases before *Fearon*, the password problem had been a

---

29 *Vu*, *supra*, note 1, at paras. 53-62.

30 *Vu*, *supra*, note 1, at paras. 56 and 62.

31 *Fearon*, *supra*, note 4, at para. 53.

dividing line. The Court of Appeal in *Fearon* prompted headlines with a finding that the cursory mobile phone search conducted incident to arrest would not have been permitted had the phone been password-protected.[32] In Nova Scotia, the Court of Appeal took a different view, finding that that "because a password is not on at the very moment the police seize a cell phone cannot mean that the state is welcome and free to roam through its contents".[33] *Fearon* avoided ascribing prominence to the presence or activation of a particular feature — it was but one fairly insignificant factor in the totality of circumstances establishing an expectation of privacy. Though, as a matter of practice, technological features such as passwords or encryption can frustrate the exercise of police powers regardless of where the legal debate lands.

III. TECHNOLOGY AND THE *CRIMINAL CODE* SEARCH POWERS

Search law in Canada has a rich history of back and forth between courts and Parliament. Cases are pursued through provincial courts, the Supreme Court decides an issue, and Parliament responds with amendments to the search provisions to address a constitutional shortcoming or gap.[34] It has happened with consent wiretaps,[35] video surveillance warrants,[36] tracking warrants[37] and emergency wiretaps.[38]

---

[32] *R. v. Fearon*, [2013] O.J. No. 704, 2013 ONCA 106, 114 O.R. (3d) 81, at paras. 73-75 (Ont. C.A.); "OK for police to search cellphone if no password, says court", February 21, 2013, CBC News, online: <http://www.cbc.ca/news/canada/toronto/ok-for-police-to-search-cellphone-if-no-password-says-court-1.1310260>.

[33] *R. v. Hiscoe*, [2013] N.S.J. No. 188, 2013 NSCA 48, 328 N.S.R. (2d) 381, at para. 81 (N.S.C.A.).

[34] For a historical look at Parliament's *Criminal Code*, R.S.C. 1985, c. C-46 [hereinafter "*Criminal Code*"] responses to Supreme Court of Canada cases on s. 8, see Michal Fairburn, "Twenty-Five Years in Search of a Reasonable Approach" (2008) 40 S.C.L.R. (2d) 55 [hereinafter "Fairburn"].

[35] The 1990 decision in *R. v. Duarte*, [1990] S.C.J. No. 2, [1990] 1 S.C.R. 30 (S.C.C.) [hereinafter "*Duarte*"] was followed by s. 184.2 [as am. S.C. 1993, c. 40, s. 4] of the *Criminal Code*, *supra*, note 34, governing interception of communications where one party has consented.

[36] *Wong*, *supra*, note 8, decided the same year as *Duarte*, *id.*, led to the enactment of video surveillance provisions located in a general search warrant section (487.01) but importing the protections of Part VI wiretap authorizations, *An Act to Amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunications Act*, S.C. 1993, c. 40, s. 15.

[37] After the Supreme Court of Canada's decision in *R. v. Wise*, [1992] S.C.J. No. 16, [1992] 1 S.C.R. 527 (S.C.C.), regarding the privacy intrusion on a beeper used to track a vehicle, Parliament added s. 492.1 [as am. S.C. 1993, c. 40, s. 18] of the *Criminal Code*, *supra*, note 34, to specifically authorize the use of tracking devices.

[38] After *R. v. Tse*, [2012] S.C.J. No. 16, [2012] 1 S.C.R. 531, 2012 SCC 16 (S.C.C.), Parliament enacted amendments to Part VI to require both notice and reporting on emergency

But the glacial pace of a case's progression on the plodding wheels of justice to the pinnacle, followed by a run through the law-making mill, is an obviously poor pathway for response to rapid advancement of technology. The resulting *Criminal Code* is a patchwork of isolated responses to specific search problems, rather than a contemplated and cohesive whole.[39] At its very foundation, the Code embodies concepts that are losing their relevance in a digital age.

1. Traditional Warrants and Authorization

The bedrock of police search powers in the *Criminal Code* is the search warrant. Found in section 487, it is the original and generalized vehicle for judicial pre-authorization of state intrusion into the sphere of personal privacy. When the necessary grounds are made out, a justice may authorize the seizure of things that may afford evidence of an offence from a specific named place. Things in places. That bedrock may have faults.

Is a computer a thing? Is the data on it a thing? Is the string of binary code sent through satellites in pieces and reassembled at some other machine a thing? Is it the same "thing" when it lands as it is when it travels in pieces? And what of the places? Police can't knock and announce their presence at the door of satellites and clouds and mobile servers. Yet without particularity of place, current tools may be unavailable.

The search provisions in the *Criminal Code* have been updated to address the lack of tangibility and physical presence of digital data. In 1997, section 487 was amended to include provisions aimed directly at the problem of gathering digital "things". Section 487(2.1) and (2.2) provide that, in a regular search warrant under section 487, a police officer or a person at the search location may "use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system". The scope of the subsection has not been widely considered. It is potentially boundless. If taking and examining the desktop box was deemed in *R. v. Morelli* to be the most intrusive, extensive, and invasive search imaginable,[40] what

wiretaps to address constitutional infirmities identified in the Supreme Court decision: *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, S.C. 2013, c. 8.

[39] Fairburn, *supra*, note 34, at 79 and 82-83.

[40] *R. v. Morelli*, [2010] S.C.J. No. 8, [2010] 1 S.C.R. 253, 2010 SCC 8, at paras. 2-3 and 105 (S.C.C.).

about a search of all that is "accessible to" that box while its stands connected in a home or office? Depending on the configurations and active connections of a given device, there could be data accessible to the device from other people, other networks, other countries, or other businesses. The section 487 warrant looks for things in a place, yet the Court in *Vu* recognized that "a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized".[41]

Wiretap provisions have also fallen out of step. Part VI of the *Criminal Code* governs interception of private communications. Modern communications are not fixed in time and place in the same fashion as communications over original telephone wires used to be, making our traditional understanding of "wiretapping" an uneasy fit with the reality of police investigations involving private communication. The wire room is now wireless. Telephone conversation used to disappear when they were over, so police required the extraordinary power to grab them from the airspace and record them for eternity. Modern communications do not fit that mold.[42] Communications are far more often recorded in transit, independent of police involvement and may be stored routinely by external companies, and sometimes sent in indecipherable code, encryption, to maintain privacy in transit. Applications and devices are peddled on the Internet marketplace that boast features designed to maintain secrecy and destroy all digital trace of our doings.

In 1990, when *R. v. Duarte* was decided on the issue of recording communications, La Forest J., writing for the majority, was concerned with the state taking the transient spoken word and immortalizing it in exact replica. He wrote that privacy would be destroyed if the state were free, unfettered, to make surreptitious permanent electronic recordings of our private communications.[43] Pre-authorization was required to guard against the "insidious danger" that the state would "record and transmit our words".[44] We have come a

---

[41] *Vu*, *supra*, note 1, at para. 44. Justice Cromwell, for the Court, later expressly noted that police executing a traditional warrant to search that *did* specifically address computer search would have the benefit of s. 487(2.1) and (2.2) to gather data, though there was no particular discussion of the ambit or implications of that avenue of search.

[42] For discussion of the application of electronic surveillance requirements to telephone and then digital communications in the United States, see Susan Freiwald, "First Principles of Communication Privacy", 2007 Stan. Tech. L. Rev. 3, at paras. 13-18.

[43] *Duarte*, *supra*, note 35, at para. 22.

[44] *Id.*, at para. 21.

significant distance since *Duarte*. In text-based communications, standard fare for younger generations, the originator of a communication is the one creating the permanent record and releasing it to the uncontrolled cyberspace. The state no longer holds the secret microphone, but merely accesses that which the sender has packaged in permanency.[45] The Supreme Court has been clear to cut chords with the past where limits do not make sense in modern technological reality. Computers are not filing cabinets and phones are not briefcases. Communications too have changed in character as well as in form. Privacy will need to be reconsidered in this new context.

The 2013 decision in *TELUS* is a good example of the difficulty understanding technology and applying traditional concepts to an untraditional world. In *TELUS*, police sought stored text-messages as well as future, as yet unsent, messages to be delivered on a prospective, ongoing basis. Although the subject matter of the search was clear, the future communications of named targets, the Supreme Court was significantly divided on the proper approach for law enforcement.[46] Justice Abella, for three justices, found that Part VI authorization (a "wiretap") was required because an intercept occurs whenever the police acquire the content of a text message from a service provider who has stored it during the transmission process.[47] Justice Moldaver, for two justices, agreed that Part VI was the right tool but for a different reason. He declined to define "intercept" but found that courts should approach the question from a standpoint of substantial equivalence, that is, if what the police are seeking in substance looks like an intercept, then that is the appropriate form and standard of pre-authorization.[48] The Chief Justice and Cromwell J. dissented, and commented that the definition of intercept proposed by Abella J. would undermine well-established law that said stored communications, already delivered, were accessible by

---

[45] For recent discussion in lower courts on the application of *Duarte* to text-based undercover communications, see *R. v. Ghorta*, "Ruling #1: The Admissibility of Text Messages" (unreported decision of Durno J., Brampton, Ont. S.C.J., March 16, 2015) and *R. v. Graff*, [2015] A.J. No. 717, 2014 ABQB 415, at paras. 51-66 (Alta. Q.B.).

[46] The availability of already sent and stored text-messages was not contentious; the parties agreed that stored text messages were available by production order: *TELUS*, *supra*, note 2, at para. 11.

[47] *TELUS*, *supra*, note 2, at paras. 1-46.

[48] *Id.*, at paras. 47-108. Justice Moldaver was influenced by the statutory exclusion of the use of general warrants where another authorization was available in the *Code* (s. 487.01(2)(c)) and by the fact that the statutory preconditions for an intercept were significantly more onerous than the general warrant.

search warrant.[49] Text communications may have been intercepted by Telus, but police did not "intercept" when they obtained the already stored messages. The dissenters would have found that the general warrant, not an authorization for interception, could properly support the police request.

TELUS tells us how much we don't understand about technology. Law enforcement in the midst of an investigation must determine what pre-authorization tool is available and should be sought to permit particular evidence-gathering techniques. Yet even at the highest court in the country, with years of research and contemplation to assist, the answer remains uncertain.

TELUS is also an instructive lesson in the power of third party information holders. The intercept crystallized for three justices, at the point that the police acquired the messages. But police could only access that content because Telus, as a business practice, had formed a system where all messages were copied and temporarily stored. The average consumer will not likely know the storage practices of her service provider. If a telecommunications provider's decisions as to how to store communications, unbeknownst to clients, could define law enforcement powers of access, the result would be inconsistent and unprincipled. Yet modern information storage and communication is heavily dependent on the facilities and services of private entities. How much power do our court decisions put in the hands of profit-driven private entities?

2. New Provisions: Bill C-13

In March 2015, new provisions came into effect to update the *Criminal Code* search scheme. The new powers include separate authorizations for transmission data, data preservation schemes, tracking warrants for things and for people, and several new species of production order depending on the type of data sought. "Data", "transmission data" and "tracking data" are also newly defined.[50] It is too soon to say whether law enforcement will find the new tools meaningful, and whether courts will find them a sensible matrix for the consideration of criminal search powers. There are likely to be some growing pains.

---

[49] *TELUS*, *supra*, note 2, at paras. 109-196; reference to the inconsistency between the reasons of Abella J. and prior law on computer search of stored communications at para. 155.

[50] *Criminal Code*, *supra*, note 34, s. 487.011 [as am. S.C. 2014, c. 31, s. 20].

IV. CONCLUSION

There is yet no legislative response to recent computer and cellphone cases in the Supreme Court. While the judgments in *Vu* and *Fearon* leave room for legislated options to address seizure of computers and search of mobile devices, they do not specifically call out for reform or identify a pressing need for amendment. In *Fearon*, the majority indicated that legislation "may well be desirable" and that there are many ways in which the law enforcement and privacy concerns may be balanced in the digital context.[51] Parliament has not demonstrated an appetite to enact particular conditions for computer search. *Spencer* may yet invoke a Parliamentary response, though it would be in the realm of a new power[52] not conditions of search.

The Charter leaves room to address the problem of after-the-fact resolution of legal lines of privacy. Although the Supreme Court has stated that police should err on the side of caution, usually pre-authorization, when faced with grey areas of law, the analysis under section 24(2) of the Charter permits admissibility of evidence in the broader interests of justice even where breaches have occurred. Where the law changes post-search, as opposed to just being unclear, exclusion of evidence is less likely to result.[53]

Statutory provisions and legal distinctions should not be technology-based. They will be too fleeting. *Tessling*'s wisdom should be heeded; focus on the information obtained by the technique in the case at hand and deal with advances step by step, as they actually arise.[54] *Vu* and *Fearon* offer incremental common law developments that allow for application of traditional principles but avoid technological distinctions that would hamper practical application.

---

[51] *Fearon*, *supra*, note 4, at para. 84.

[52] A production order is available for Internet subscriber information. A possible change would be creation of a form of pre-authorization that reflects a lower threshold for police to meet to access basic subscriber information. At present the general production order can be obtained on a reasonable belief standard (s. 487.014). Given the low privacy interest in the subscriber data, a reasonable suspicion standard, which is the standard for transmission data production (s. 487.016), would likely suffice to pass constitutional muster.

[53] See for example *Fearon*, *supra*, note 4, at para. 95: "The police simply did something that they believed on reasonable grounds to be lawful and were proven wrong, after the fact, by developments in the jurisprudence." The evidence produced by the search incident to arrest of a cell phone in *Fearon* was not excluded, nor was the Internet subscriber data produced without a warrant in *Spencer*, *supra*, note 3, at para. 81.

[54] *Tessling*, *supra*, note 7, at para. 55.

What's next? Well, for courts, what is next is what has already happened. Years ago. The Supreme Court will continue to make small but important steps to manage our expectations in new technological fields, while individuals experiment with the newer, faster and farther reaching capabilities that are years away from courtroom contemplation. Interception of applications on mobile devices, interjurisdictional debate over how to erect borders in a landscape of air, authorization for new techniques such as deliverable programs that install themselves on a target computer and report back with video, images, microphone and content recording;[55] the next issues are crowding the horizon. Lawyers and courts will be plodding slowly through the fields, trampling a safe path, creating case law as road signs to guide us towards that ever-elusive frontier.

[55] See the United States District Court discussion of this technique in the Texas case *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp. 2d 753 (2013).