FBI v. Apple and Beyond: Encryption in the Canadian Law of Digital Search and Seizure

by Gerald Chan and Stephen Aylward[1]

I. Introduction

The stakes have never been higher in the arms race among tech companies, hackers, and law enforcement. Tech companies are continually developing measures to enhance the digital security of their users. Hackers and law enforcement agencies, while working toward very different objectives, are themselves developing new techniques to circumvent this encryption in order to access the treasure trove of information contained in digital devices and communications services.

The fight between the FBI and Apple in the United States over the encryption of iPhones has become a flashpoint for this controversy. Tim Cook, the CEO of Apple Inc., has attracted headlines with his highly publicized challenge to court orders obtained by the FBI compelling Apple to assist in unlocking iPhones.[2] This paper examines the implications of the FBI v. Apple dispute in the Canadian context. The Canadian perspective on encryption issues will be of interest to a broader audience, both because the Canadian debate is free of some of the technical *minutiae* of the American cases, and because of the similarity of the *Canadian Charter of Rights and Freedoms* to other international human rights covenants, such as the *European Convention on Human Rights*. Moreover, as an important foreign market for American technology companies, Canada will be an important test case to gauge the appetite of American companies to take on foreign governments in the defence of user privacy.

Part II of this article begins by setting out the legal and policy context of the FBI v. Apple debate. Part III sets out the Supreme Court of Canada's approach to digital privacy issues in the context of elaborating the constitutional right to be "secure against unreasonable search and seizure". Part IV examines the broader legal context in Canada and identifies a number of uncertainties over how Canadian law treats state attempts to compel third parties to decrypt devices or data. The authors conclude that the state of Canadian law is unsatisfactory. Clearer safeguards are needed to protect third parties from unduly burdensome law enforcement requests and to protect the privacy of the end users of digital devices and services.

II. FBI v. Apple: Legal and Policy Context

a. The San Bernardino Dispute

In February, 2016, Apple announced that it would challenge an order obtained by the FBI compelling it to provide "reasonable technical assistance" to unlock the iPhone of one of the attackers in the San Bernardino shooting.[3] Apple had previously challenged similar orders, but the San Bernardino case drew intense publicity, owing in part to the high profile nature of the

---

1 Gerald Chan is Counsel at Stockwoods LLP and practises criminal, constitutional and regulatory litigation. He has been involved in a number of leading digital search and seizure cases with his colleague Nader R. Hasan (also Counsel at Stockwoods LLP), including *R. v. Fearon,* [2014] S.C.R. 621 [*Fearon*]; *R. v. Vu,* [2013] 3 S.C.R. 657 [*Vu*]; and *R. v. Cole,* [2012] 3 S.C.R. 34 (co-counsel with Frank Addario). Stephen Aylward is an associate at Stockwoods LLP with a practice in civil and commercial litigation, as well as administrative and criminal law. This paper has been accepted for publication by the *Journal of Data Protection & Privacy* and is republished with permission.

2 Eric Lichtblau and Katie Benner, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", *New York Times*, 17 February 2016, available: http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html

3 Ibid.

case and in part to a new feature of this request. Previous court challenges had dealt with less sophisticated models of the iPhone or iOS, Apple's proprietary operating system for the iPhone. The novel feature in the San Bernardino iPhone case was that Apple itself lacked the technical ability to hack its own phone: it would have needed to develop new software to allow it to comply with the court order.[4] Apple objected to this order on the grounds that it would unduly infringe its users' privacy by weakening the iPhone's security measures and increasing the possibility of the "backdoor" being leaked, or by setting a precedent for further weakening encryption either in the United States or abroad.[5] The debate at its heart raises the fundamental question of whether our society should allow the development of encryption technologies so powerful that no one, including the developer, can circumvent it. In that sense, the dispute between Apple and the FBI can be seen as the latest episode of the encryption wars that date back to debates in the 1990s over controls on the development of encryption and the repeal of Cold War-era export restrictions on cryptography software and hardware.[6]

The issue has polarized public opinion in the United States. One poll by the Pew Research Center found that 51% of Americans supported unlocking the iPhone, while 38% were against.[7] Another poll, released the same week, found that 46% of respondents supported Apple's position, while 35% of respondents said they disagreed with it.[8] The difference in the polls is likely attributable to the wording of the question posed to respondents.[9]

The San Bernardino case was rendered moot when the FBI announced that it had hired a private contractor to unlock the phone, and so no longer needed Apple's assistance.[10] However, given Apple and Google's commitment to enhancing encryption features on their devices, this is a temporary cease-fire, not a truce.

b. Encryption debates beyond the San Bernardino iPhone

While the San Bernardino incident captured the public imagination, other cases between Apple and law enforcement have also worked their way through the court system. Apple successfully challenged a court order in another high profile case in the US District Court in the Eastern District of New York.[11] Much of Magistrate Judge Orenstein's analysis focuses on the jurisdiction of the court to make an order compelling a third party to provide assistance to law enforcement under the *All Writs Act,* an arcane federal statute dating back to 1789. This analysis is a legal quirk with little relevance outside the United States. For instance, in Canada the

---

4 Ibid.

5 Ibid.

6 Herb Brody, "Of Bytes and Rights", Nov/Dec 1992 *Technology Review*; U.S. Department of Commerce, Bureau of Export Administration, "Revised u.S. Encryption Export Control Regulations", January 2000, 15 CFR Parts 734, 740, 742, 770, 772, and 774.

7 Pew Research Centre, "More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone", 22 February 2016, available: http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/?utm_source=viz&utm_medium=viz.referral&utm_campaign=viz.ref&utm_viz_id=jjvOqTxYGDX&utm_pubreferrer=www.forbes.com%2Fsites%2Fnelsongranados%2F2016%2F02%2F20%2Fapple-can-should-and-will-help-fbi-unlock-shooters-iphone%2F

8 Jim Finkle, "Solid Support for Apple in iPhone Encryption Fight: Poll", *Reuters*, 24 February 2016, available: http://www.reuters.com/article/us-apple-encryption-poll-idUSKCN0VX159

9 Krishnadev Calamur, "Public Opinion Supports Apple Over the FBI—or Does It?", *The Atlantic*, 24 February 2016, available: http://www.theatlantic.com/national/archive/2016/02/apple-fbi-polls/470736/

10 Katie Benner and Eric Lichtblau, "U.S. Says It Has Unlocked iPhone Without Apple" *New York Times*, 28 March 2016, available: http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0

11 *In Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant* (29 February 2016).

jurisdiction of a court to issue an "assistance order" to a third party under s. 487.02 of the *Criminal Code* is uncontroversial. However, Magistrate Judge Orenstein also goes on to decide that even if there were jurisdiction to make such an order, he would not exercise his discretion to do so. In reaching this conclusion, he considered three factors in determining whether to compel a company to provide assistance to law enforcement:

> [1] the closeness of Apple's relationship to the underlying criminal conduct and government Investigation; [2] the burden the requested order would impose on Apple; and [3] the necessity of imposing such a burden on Apple.[12]

Encryption issues have arisen for other technology companies. WhatsApp, a private messaging service owned by Facebook, allows millions of users to connect in an end-to-end encrypted environment.[13] WhatsApp's encryption has stymied the ability of law enforcement to execute wiretap authorizations and has led to a dispute with the company, although it is has not yet resulted in litigation in the US.[14] In Brazil, a court recently went so far as to temporarily suspend access to WhatsApp nationwide following a refusal by the company to comply with a court order requiring it to decrypt communications thought relevant to a drug investigation.[15]

Court documents filed in a mafia murder case in Montreal, *R. v. Mirarchi*, reveal that the Royal Canadian Mounted Police ("RCMP") obtained the "global encryption key" to Blackberry messages. With the facilitation of Blackberry, they were able to decrypt over one million messages in the course of their investigation.[16] In late 2015, Dutch police claimed that they had cracked the encryption in Blackberry communications, although Blackberry has denied this claim.[17]

In a related context, Microsoft has recently sued the Justice Department for the alleged overuse of "gag orders" in the context of production orders requiring Microsoft to provide user data to law enforcement.[18] Microsoft contends that these "gag orders" violate the Fourth Amendment rights of their users by preventing them from being informed of the fact that the government has searched their data. Microsoft also argues that the "gag orders" violate the company's First Amendment right of free speech by restricting its communications with its customers.

c. Policy Implications of the Encryption Debate

There is no doubt that encryption poses a new challenge for law enforcement. Francois Molins, the chief prosecutor of the Paris terrorist attacks of November, 2015, has been quoted as saying

---

c.12 Ibid. at 1.

13 Matt Puzzo, "WhatsApp Encryption Said to Stymie Wiretap Order", *New York Times*, 12 March 2016, available: http://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html

14 Ibid.

15 Stephanie Mlot, "Brazil Bans WhatsApp(Again) Over Encryption", *PC Magazine*, 3 May 2016, available: http://www.pcmag.com/news/344200/brazil-bans-whatsapp-again-over-encryption

16 Jordan Pearson & Justin Ling, "Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages", *Motherboard*, 14 April 2016, available: https://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada

17 Blackberry, "BlackBerry Devices: Secure As They Have Always Been", 16 January 2016, available: http://blogs.blackberry.com/2016/01/blackberry-devices-secure-as-they-have-always-been/

18 Steve Lohr, "Microsoft Sues Justice Department to Protest Gag Order Statute", *New York Times*, 14 April 2016, available: http://www.nytimes.com/2016/04/15/technology/microsoft-sues-us-over-orders-barring-it-from-revealing-surveillance.html?_r=0

that: "With all these encryption software programs we can't penetrate into certain conversations and we're dealing with this gigantic black hole".[19]

Encryption has posed an obstacle to law enforcement investigating simpler crimes. A Baton Rouge, Louisiana woman, was shot by an unknown person at the front door of her apartment. Police have been unable to gather any further information about who the possible shooter is, although it is believed that she kept a diary on her iPhone which may reveal clues about the killer. The diary cannot be accessed because the phone is locked.[20]

Encryption has also stymied police investigating the recent phenomenon of "swatting", a malicious hoax in which the prankster calls in a false report of violence to 911, leading a special weapons and tactics ("SWAT") team to respond to an unsuspecting person's house.[21] The prank callers use encrypted voice over internet protocol ("VOIP") services, proxy servers, and virtual private networks to disguise their identity and hinder police efforts to identify them.

James Comey, the Director of the FBI, testified before the Congressional House Judiciary Committee about the "going dark problem" that encryption poses by allowing terrorists and other bad actors to coordinate their activity with communications that cannot be intercepted or deciphered by law enforcement.[22]

On the other hand, high profile data breaches have reminded the public of the importance of digital security. The dating website Ashley Madison was the victim of a data breach that exposed the data of millions of users.[23] Consumers increasingly use digital devices and services to store banking information, health records, communications with friends, and other intimate aspects of their lives. Cybersecurity is essential to protecting consumers from malicious hackers and identity theft, and to ensuring a sphere of personal privacy in the digital age.

Tensions in the encryption debate are rising around the world. In France, in the wake of the Paris shooting, a bill has been introduced that would make it illegal for a tech company to refuse to decrypt data.[24] On the other hand, the French government has stated that it does not approve of "encryptographic backdoors", or "vulnerability by design", as the French Digital Affairs Minister puts it.[25]

In the United Kingdom, a bill has been tabled that would grant intelligence authorities greater ability to access personal data of tech companies as well as telecommunications and internet

---

19 Quoted in Nelson Granados, "The Apple-FBI Battle is Dangerously Polarizing Public Opinion", 21 March 2016, available: http://www.forbes.com/sites/nelsongranados/2016/03/21/how-the-apple-vs-fbi-battle-is-dangerously-polarizing-public-opinion/#188c0aee4bd8

20 Jon Schuppe, "Mother's Murder Among Cases Hampered By Locked iPhones", *NBC News*, 27 February 2016, available: http://www.nbcnews.com/news/us-news/mother-s-murder-among-cases-hampered-locked-iphones-n526916

21 Dan Tyman, "The Terror of Swatting: How the Law is Tracking Down High-Tech Pranksters", *The Guardian*, 15 April 2016, available: https://www.theguardian.com/technology/2016/apr/15/swatting-law-teens-anonymous-prank-call-police

22 James B. Comey, "Statement Before the House Judiciary Committee", 1 March 2016, available: https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy

23 Nicole Perlroth, "Ashley Madison Chief Steps Down After Data Breach", *New York Times*, 28 August 2015, available: http://www.nytimes.com/2015/08/29/technology/ashley-madison-ceo-steps-down-after-data-hack.html

24 Sam Schechner & Daisuke Wakabayashi, "Fight to Unlock Phones in Terror Cases Persists in Europe", *The Wall Street Journal*, 31 March 2016, available: http://www.wsj.com/articles/fight-to-unlock-phones-in-terror-cases-persists-in-europe-1459447009

25 Paul Ducklin, "Cryptographic backdoors? France says, "Non!", *Naked Security*, 18 Jan 2016, available: https://nakedsecurity.sophos.com/2016/01/18/cryptographic-backdoors-france-says-non/

service providers. Under the bill, companies would be obliged to decrypt data where "reasonably practicable".[26]

The emerging patchwork of different regulatory approaches around the world creates a risky environment for tech companies. The obligations to protect user privacy in one country may conflict with obligations to assist law enforcement in another. For instance, Microsoft says that Brazilian laws requiring it to disclose Skype data stored remotely in the United States to law enforcement would violate US wiretapping laws.[27]

III. The Supreme Court of Canada's Approach to Digital Privacy in the Constitutional Context

The Supreme Court of Canada has taken a robust approach to digital privacy issues in a line of cases starting in 2010.[28] While a thorough examination of this case law is beyond the scope of this paper, the general principles from these cases are essential to understanding the encryption debate in Canada.

Section 8 of the *Canadian Charter of Rights and Freedoms* states that:

> 8. Everyone has the right to be secure against unreasonable search and seizure.

From the outset, the Supreme Court of Canada has emphasized that s. 8 should be interpreted purposively so as to protect the reasonable expectation of privacy of Canadians.[29] Where an individual has a reasonable expectation of privacy, a warrantless search by the state is presumed to be unreasonable. This presumption can only be rebutted where the search is authorized by law, the law is reasonable, and the search is conducted in a reasonable manner.[30]

a. *Vu*: Adapting Traditional Doctrine to the Digital Age

In *Vu*,[31] the Supreme Court of Canada recognized the need to adapt the law of search and seizure to better reflect digital privacy interests by requiring that a warrant specifically authorize the search of digital devices, such as computers and smartphones. Police obtained a warrant to search the accused's residence based on an information to obtain ("ITO") indicating that there

---

26 Mark Scott, "American Tech Giants Face Fight in Europe Over Encrypted Data", *The New York Times*, 27 March, 2016, available: http://www.nytimes.com/2016/03/28/technology/american-tech-giants-face-fight-in-europe-over-encrypted-data.html

27 Joshua Brustein, "Apple's Privacy Fight Could Be Even Worse in Europe", *Bloomberg*, 9 March 2016, available: http://www.bloomberg.com/news/articles/2016-03-09/apple-s-privacy-fight-could-be-even-worse-in-europe

28 See generally, Gerald Chan, "Life After *Vu: Manner of Computer Searches and Search Protocols*" (2014) 67 S.C.L.R. (2d) 433; Nader Hasan, "A Step Forward or Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age" (2015) 71 S.C.L.R. (2d) 439.

29 *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 at p. 155.

30 *R. v. Collins*, [1987] 1 S.C.R. 265; The determination of what an individual has a reasonable expectation of privacy in a place, thing, or information is a normative, not a descriptive question: *R. v. Tessling*, [2004] 3 S.C.R. 432 at para. 42. The question is "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement": *Hunter v. Southam*, cit. 23 aove at pp. 159 – 160. The Supreme Court has taken an expansive approach to the reasonable expectation of privacy inquiry, holding that the "totality of the circumstances" must be examined, including matters such as the place of the search, whether the information was in the possession of a third party (and if so, if it was subject to confidentiality requirements), and the intrusiveness of the search technique.30 This normative inquiry aims to strike a balance between privacy and the legitimate countervailing concerns of safety, security, and the suppression of crime: *Tessling* at para. 17. The purpose of the inquiry is not to maintain the balance that existed at any historical point of time, but rather to achieve a balance that reflects evolving societal values: *Tessling* at para. 61. In this respect, the Canadian approach differs from that adopted by the majority opinion of the Supreme Court of the United States, written by Scalia J., in *Kyllo v. United States*, which placed an emphasis on preserving the balance between privacy and other interests that existed at the time the framers adopted the Fourth Amendment: Ibid.; *Kyllo v. United States*, 533 US 27 (2001) at pp. 34 – 35.

31 *Vu*, cit. 1 above.

were reasonable and probable grounds to suspect there would be evidence relating to the theft of electricity at the premises.[32] The ITO referred to "computer-generated documents" but did not specifically refer to computers or other digital devices.[33] The accused challenged the search of two computers and a smartphone seized by the police under this warrant.

Under the traditional framework of the law of search and seizure, a search warrant authorizes police to search a place specified in the warrant but also any "receptacle" or "place" within that place, provided that the search is consistent with the objective of the initial search.[34] The Crown argued that a computer should be treated as any other receptacle, such as a filing cabinet, a view that had been accepted by lower courts.[35] Justice Cromwell, writing for a unanimous Court, rejected this argument and held that digital devices were qualitatively different from traditional "receptacles."

The distinct nature of digital devices flowed from four considerations. First, the scale and intimate quality of information, including information belonging to the "biographical core of personal information," makes digital devices quite different from filing cabinets.[36] Second, digital devices tend to generate and retain data automatically, often unbeknownst to the user.[37] Third, even when users believe they have deleted data, it may remain on their system.[38] Fourth, unlike traditional "receptacles," whose contents are found within the place of the original search, searches of digital devices may lead investigators to data that is not in any meaningful sense stored at the location of the search, but is rather hosted in a remoted location.[39]

As a result of these considerations, digital devices must be treated more like a separate "place" than a receptacle, thus requiring specific prior judicial authorization for police to validly conduct a search on such devices.[40]

At its core, *Vu* stands for the proposition that simplistic analogies (as between a computer and a "receptacle") do not suffice to afford sufficient privacy protections for digital devices. This is an instructive lesson in the context of the FBI v. Apple debate, where it is difficult to identify an analogy for the encryption technology that is in issue. No safe or real world lock can shield the sheer volume or nature of data contained on an iPhone. Similarly, there is no key in the real world that can undermine the security of all locks in the future. Special rules are needed when it comes to digital privacy.

New technologies can both enhance and diminish privacy. They can propel us into the future and, in some respects, take us back in time. For instance, in the WhatsApp example, the protection of text communications through to end-to-end encryption may be seen as taking a category of evidence to which law enforcement has long had access (through wiretapping) completely off the grid. Alternatively, it may be seen as turning back the clock to an age in

32 Ibid. at para. 4.

33 Ibid.

34 Ibid. at para 39.

35 *R. v. Giles*, [2007] BCJ No 2918 at para 56 (BCSC); *R. v. Polius*, [2009] OJ No 3074 at par. 47 (ONSC) ("[a] cell phone is the functional equivalent of a locked briefcase…").

36 *Vu,* cit. 1, above at para. 41.

37 Ibid. at para. 42.

38 Ibid. at para. 43.

39 Ibid. at para. 44.

40 Ibid. at para. 51.

which private communications were invulnerable to interception — an age in which private communications would always remain private.

b. *Spencer*: Privacy as Anonymity Online

In *Spencer*,[41] the Supreme Court turned to the issue of privacy and anonymity in the broader virtual space of the internet. The police identified an individual who was downloading and uploading child pornography through Limewire, a peer to peer file sharing program. The program allowed to see the accused's internet protocol ("IP") address. An IP address can readily be traced to a general geographic location and an Internet Service Provider ("ISP"), which assigns IP addresses to individual subscribers. The police determined that the IP address in question was located in or around Saskatoon and was assigned by Shaw Communications. The investigating officer contacted Shaw with a "law enforcement request", a letter that purported to authorize the disclosure of subscriber information, including a subscriber's name and address, under applicable privacy legislation. No warrant was obtained for this request. Shaw revealed that the IP address belonged to the accused's sister. A search of her residence, where the accused also lived, led to the seizure of the accused's computer, on which child pornography was found. The accused appealed his conviction on the grounds that the law enforcement request to Shaw violated his privacy rights under s. 8 of the *Canadian Charter of Rights and Freedoms* and that the results of the subsequent search were thus inadmissible.

The IP address of a user's internet connection is broadcast publicly in the course of certain activities, including peer to peer file sharing. IP addresses are also frequently logged by websites and other web services. An internet user will, often unwittingly, leave a trail of breadcrumbs in their online peregrinations in the form of their IP address. While a user's IP address is often on public display on the internet, however, individuals benefit from anonymity on the internet insofar as the IP address is just a collection of numbers. So long as the name and address of the internet user behind the IP address remains hidden, the individual's anonymity remains. In *Spencer,* the Supreme Court held that this anonymity is an essential part of the privacy interests enshrined in s. 8 of the *Charter.*

In explaining the relationship between privacy as anonymity, the Court cited *R v Wise*, one of its earlier decisions dealing with tracking devices. In *Wise,* the Court held that the ongoing monitoring of a vehicle's whereabouts on public highways using a tracking device amounted to a violation of the suspect's reasonable expectation of privacy.[42] Even though the suspect was driving his car in public areas for all the world to see, there was a qualitative difference between the casual observation of the public and ongoing electronic monitoring that tracked the vehicle's every movement.[43] We do not give up our anonymity simply by leaving our homes and moving about in the public space. Neither should we give up our anonymity online simply by moving from website to website in the cyber-world.

41 *R. v. Spencer*, [2014] 2 S.C.R. 212 [*Spencer*].

42 *R. v. Wise*, [1992] 1 S.C.R. 527 at 538.

43 Ibid. It should be noted that *Wise* was decided at a time when the police were limited to fixing (now seemingly ancient "beepers" onto cars — technology that is now obsolete owing to GPS tracking devices. In *United States v. Jones*, 132 S. Ct. 945 (2012), the U.S. Supreme Court reached a similar result as in *Wise* in the context of modern GPS tracking devices, and in *Torrey Dale Grady v. North Carolina*, 135 S. Ct. 1368 at 1370 (2015), it clarified that its holding in *Jones* applies equally to tracking people as it does to vehicles.

Spencer illustrates that there is nothing nefarious about online anonymity. Users have a legitimate right to protect their digital data from unwarranted police snooping. The use of encryption technology is a means of buttressing the user's online privacy interests by supplementing the anonymity aspect of online privacy with secrecy. Compelling technology companies to decrypt their devices and services would risk undermining this form of privacy protection.

c. *Fearon:* Cell Phone Searches

In *Fearon*,[44] the Supreme Court addressed the limits of police searches of cell phones, a topic closer to the FBI v. Apple debate. The issue was whether the police can conduct a warrantless search of the contents of a cell phone incident to arrest. This required the Court to once again grapple with the question of how rules developed to govern search and seizure in pre-digital age should be applied to digital devices. And the Court again held that the traditional framework for search and seizure was insufficient to protect privacy rights and introduced new safeguards specific to the search of digital devices.

The police had arrested the accused on suspicion of involvement in an armed robbery at a flea market in which jewelry was stolen at gunpoint. On his arrest, the police conducted a pat-down search and discovered a cell phone. The police then searched the phone and discovered incriminating text messages and photos relating to the robbery. One text referred to the jewelry and began, "We did it…".[45] The main question on appeal was whether the search of the cell phone incident to arrest was lawful or if specific authorization was required.

Justice Cromwell, writing for a majority of the Court, held that cell phones can be searched incident to arrest without a warrant. In doing so, he rejected the accused's argument that a warrant is required because of the heightened privacy interests in the contents of digital devices such as cell phones.[46] In this respect, the Supreme Court of Canada differed from the Supreme Court of the United States' approach in *Riley v. California* and *United States v. Wurie.*[47] Justice Cromwell did, however, hold that the traditional framework for warrantless searches incident to arrest had to be modified in three respects to account for these heightened privacy concerns.

First, in most cases only recently sent or created text messages, emails, photos, or call logs will be the proper subject of the search.[48] This additional requirement is intended to address the privacy concerns raised by the "virtually infinite storage capacity of cell phones".[49]

Second, digital searches incident to arrest will generally only be available for more serious crimes.[50]

---

44 *Fearon*, cit. 1 above.

45 Ibid. at para. 8.

46 This would appear to create an odd inconsistency where the police execute a search warrant at a residence and simultaneously arrest the occupants of the residence (*i.e.,* a "takedown warrant"). Under *Vu,* the police would need a warrant specifically authorizing the search of computers and cell phones in order search the contents of the same. Under *Fearon,* however, the police would be able to conduct a limited search of the computers and cell phones in the residence so long as the nature and extent of the search were truly incidental to the arrest.

47 *Riley v. California*; *United States v. Wurie*, 573 U.S. ___ (2014).,

48 *Fearon*, cit. 1, above at para. 76.

49 Ibid. at para. 77.

Third, cell phones can only be searched for the purpose of discovering evidence where "the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest", such as where other perpetrators, firearms, or stolen property are at large.[51]

Going forward, it will be interesting to see if *Fearon* remains relevant or is quickly overtaken by technological advances. In many ways, *Fearon* is the perfect illustration of how the law often lags far behind the technology. The actual facts of *Fearon* involved the now ancient "flip phone" rather than the smartphones that are now so ubiquitous. Fortunately, the Supreme Court did not feel compelled to limit its ruling to such primitive devices. But the Supreme Court also did not consider how its ruling might be practically affected by the fact that most people nowadays protect their smartphones with a passcode. If a smartphone is passcode protected, can the police compel the suspect to disclose the passcode? That would appear to be a violation of the right to silence, although there has been at least one arrest in Nova Scotia where an individual refused to disclose his passcode.[52] If the suspect cannot be so compelled, can the police compel the manufacturer of the smartphone to unlock the device, even if that would require the manufacturer to create new software to break through its own encryption? That is precisely the question that gave rise to the Apple v. FBI dispute.

IV. Encryption-Related Issues in the Broader Legal Context

The FBI v. Apple debate is part of an increasing trend toward law enforcement reliance on third parties to provide digital data in aid of investigations.[53]

a. Third Party Disclosure of Personal Information

Companies are motivated to secure the data of their customers as a matter of sound business practice.[54] In Canada, they are also required by law to take precautions with the data that they obtain from their customers. The *Personal Information and Protection of Electronic Documents*

---

50 Ibid. at para. 79.

51 Ibid. at para. 83; The Ontario Court of Appeal had held in the same case that the analysis of the level of s. 8 privacy protection should vary depending on whether the user had protected his or her device with a password: *R. v. Fearon*, 2013 ONCA 106 at paras. 73, 75. The Supreme Court rejected this approach, and held that little weight should be attributed to whether or not a device was password-protected.51 In other words, the reasonableness of a user's expectation of privacy is determined by the nature of the privacy interest in the information in the device itself.

52 Jack Julian, "Quebec Resident Alain Philippon to Fight Charge For Not Giving Up Phone Password at Airport", *CBC News*, 24 March 2015, available: http://www.cbc.ca/news/canada/nova-scotia/quebec-resident-alain-philippon-to-fight-charge-for-not-giving-up-phone-password-at-airport-1.2982236

53 In 2014, Parliament passed Bill C-13, the "*Cyber-Bullying Act*". This legislation introduced a lower standard of "reasonable grounds to suspect" (as opposed to the more common and onerous "reasonable grounds to believe" threshold) into the digital context. The "reasonable grounds to suspect" threshold has been upheld as constitutional in contexts where there is a reduced expectation of privacy in brief encounters with the police, such as dog sniff searches and pat down searches incident to an investigative detention: *R. v. MacKenzie*, [2013] 3 S.C.R. 250 at para. 2. Bill C-13 greatly expands the availability of this lower threshold for judicial authorization in the context of electronic data, despite the Supreme Court of Canada's holding in *R. v. Spencer* that certain types of digital information attracted a heightened expectation of privacy.53 A number of commentators, including the Privacy Commissioner, have expressed concern over the expanded use of this lower threshold for its impact on privacy rights.53 Increasing reliance on third parties for production of records will result in an increase in the number of battles between corporations and law enforcement as the courts struggle to articulate a new framework for the relationship between corporations, their users, and law enforcement.

54 Navneet Alang, "Best-Kept Secrets: the Battle to Safeguard Our Privacy", *The Globe and Mail*, 29 April 2016, available: http://www.theglobeandmail.com/report-on-business/rob-magazine/best-kept-secrets-the-battle-to-safeguard-our-privacy/article29759575/

Act[55] ("PIPEDA") prohibits the disclosure of customer data to third parties, including law enforcement officials, except in specifically enumerated circumstances.[56]

b. Lawful Intercept of Private Communications

In Canada, the interception of private communications is governed by Part VI of the *Criminal Code*. The verb "intercept" is defined to include "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof". It is a criminal offence to willfully intercept a private communication by means of any electro-magnetic, acoustic, mechanical or other device. [SA – cite to s. 184(1)] There are exceptions, however, for persons who are the intended recipients of the private communications; persons who intercept private communications in accordance with the proper prior judicial authorization, such as police officers; and persons who in good faith aid another person who they believe on reasonable grounds is acting with such prior judicial authorization, such as telecommunications companies. [SA – cite to s. 184(2)] While Part VI is often thought of as the regime that governs the "wiretapping" of phone conversations, it has been extended to include the interception of text messages. [SA – cite to SCC decision in *R.v . Telus Communications Inc.*]

While Part VI exempts telecommunications companies from criminal liability where they in good faith aid police officers who they believe on reasonable grounds are acting with the proper authorization, Canada does not have a broad legislative "lawful intercept" framework that *requires* telecommunications companies to facilitate the interception of communications by authorized law enforcement agencies.[57] Canada differs in this respect from other comparable jurisdictions, such as the United States, which has the *Communications Assistance for Law Enforcement Act* ("CALEA"),[58] and the United Kingdom, which has the *Regulation of Investigatory Powers Act, 2000* ("RIPA").[59] Bill C-74, introduced before Parliament in 2005, would have adopted similar legislative provisions in Canada, but the bill died on the order paper.[60] Similar provisions were again tabled as Bill C-30 by the Conservative government in 2012, but the bill was shelved after a public outcry over the scope of the proposed surveillance powers.[61] Clause 6 of Bill C-30 would have required a telecommunications service provider to decrypt any communication sent over its network that the service provider had encrypted, unless doing so would require it "to develop or acquire decryption techniques or decryption tools".[62]

---

55 S.C. 2000, c. 5.

56 In *Spencer*, the Supreme Court examined PIPEDA and concluded that a private company could only voluntarily disclose information in response to a warrantless police request where there are exigent circumstances, a reasonable law authorizing the disclosure, or in any case where the customer does not have a reasonable expectation of privacy in the information disclosed: *R. v. Spencer*, cit. 40, above at para. 71. This latter requirement is somewhat inelegant, since the highly contextual approach taken by the courts to determine if a reasonable expectation of privacy applies in a given case would be a costly and uncertain exercise for companies to determine in the absence of a court order. In *Spencer,* it was argued that the predecessor provision to s. 487.0195 of the *Criminal Code* authorized disclosure in the absence of a warrant. That provision provides immunity for anyone who voluntarily discloses information to law enforcement. This immunity, however, only applies where the disclosure is "not prohibited by law". In *Spencer*, the Court held that it would be circular to rely on this provision as providing authority to disclose. The upshot is that private companies will generally require police to produce a court order of some kind before they are allowed to disclose customer data**.**

57 Dominique Valiquet, "Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia", Library of Parliament, PRB 05-66E, 28 February 2006.

58 47 USC 1001 – 1010.

59 c. 23.

60 Dominique Valiquet, "Telecommunications and Lawful Access: I. The Legislative Situation in Canada", Library of Parliament, PRB 05-65E, 21 February 2006.

61 John Ibbitson, "Harper Government Kills Controversial Internet Surveillance Bill", *The Globe and Mail*, 11 February 2013, available: http://www.theglobeandmail.com/news/politics/harper-government-killing-internet-surveillance-bill/article8456096/

62 Kevin McArthur & Christopher Parsons, "Understanding the Lawful Access Decryption Requirement", 17 September 2012, available at SSRN: http://ssrn.com/abstract=2148060 orhttp://dx.doi.org/10.2139/ssrn.2148060

Clause 7 would have required telecommunications service providers to ensure that their transmission apparatus was configured so as to permit lawful interception of users' communications.

In 2014, many of the investigative powers first introduced in Bills C-74 and C-30 were ultimately enacted as part of the *Cyber-Bullying Act* (Bill C-13). Notably, this legislation did not include the "lawful intercept" provisions.

Despite not having legislation like CALEA or RIPA, however, Canadian regulators have to some extent secured industry compliance with lawful intercept requirements by making certain telecommunications licenses conditional on acceptance by telecommunications carriers of the "lawful intercept conditions" set out in the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications*.[63] This effectively requires telecommunications carriers to facilitate wiretapping by duly authorized law enforcement agencies. Standard 12 is particularly relevant. It provides that:

> lf network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

This licensing approach results in an awkward patchwork of regulation that applies differently depending on the type of communication and when the licence was issued. These regulations also lack the democratic legitimacy of a legislated approach. Indeed, there is not even clear empowering legislation that authorizes the imposition of these conditions.

c. Law enforcement access to encrypted data in storage

Much of the case law on digital privacy has pitted the police against individuals suspected of crime. A complex area for the law of digital privacy is where the State enlists a (willing or unwilling) third party to assist in the digital search of stored data. The innumerable constellations between suspect, police, and third party companies and citizens, remains an underanalyzed area.

While media attention in Canada has focused on the FBI v. Apple dispute south of the border, similar issues have arisen in Canada. After rumours surfaced in 2013 of a video showing former Mayor Rob Ford smoking crack cocaine, Toronto police began investigating Ford and his driver, Alexander Lisi, in relation to drugs-charges. Police obtained a search warrant for Lisi's iPhone but discovered it was locked with a passcode. They then obtained an assistance order under s. 487.02 of the *Criminal Code* requiring Apple to facilitate the unlocking. Justice Cole granted the order and Apple complied, releasing 10 gigabytes of video and other data to police.[64] The order required Apple to provide "reasonable technical assistance" to bypass the user's passcode.

The terms of the order issued by Justice Cole in the Lisi investigation are virtually identical to the terms the order issued by Magistrate Judge Orenstein in the New York case discussed in the previous section. Because Apple did not contest the order, however, Justice Cole gave no reasons explaining his decision. Accordingly, the precedential value of this order is minimal.

---

63 Industry Canada, "Licensing Framework for Mobile BroadbandServices(MBS) – 700 MHz Band, 7 March 2013 at paras. 291 – 298.

64 Kevin Donovan, "Apple Releases Sandro Lisi's iPhone Audio and Video", *The Toronto Star*, 22 February 2014, available: www.thestar.com.

Oddly, the RCMP recently released a statement stating that there is no specific authorization in the *Criminal Code* that compels technology companies to decrypt encrypted data:

> there is no specific power in the *Criminal Code* to compel a third party to decrypt or develop decryption tools, nor is there any requirement for telecommunications services to provide these services.[65]

As can be seen from the Lisi iPhone case, the Toronto Police Service takes a different view of the breadth of an assistance order. While it is true that the language of s. 487.02 does not specifically compel either decryption or the development of decryption tools, it does provide a broad general power. It remains an open question whether a court would interpret an assistance order as extending to require decryption. In any event, the statutory authority is certainly more clear-cut under s. 487.02 of the *Criminal Code* than under the *All Writs Act*, which is being relied on by the FBI in the United States. The operative provision of the *All Writs Act* states that federal courts may:

> issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

Section 487.02 of the *Criminal Code* is clearer and broader in scope:

> If an authorization is given under section 184.2, 184.3, 186 or 188 or a warrant is issued under this Act, the judge or justice who gives the authorization or issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant.

Canadian courts, however, have provided little interpretive guidance on the precise scope of assistance orders. The Supreme Court of Canada has held (in the context of an assistance order requiring a media organization to assist police in executing a search warrant) that a court making such an order must take account of the s. 2(b) and s. 8 *Charter* rights that are in play, but this provides little practical guidance to companies wishing to know the precise scope of their obligations.[66]

Two recent cases involving telecommunications companies expand on this guidance to some extent, although one of them *(Rogers)* relates to the production order power in s. 487.014 of the *Criminal Code* and not the assistance order power in s. 487.02. The two are different in that the former is a standalone search power that allows the police to compel a third party to produce documents or data within their possession or control, whereas an assistance order is meant only to be an adjunct to a search warrant. Because of this, the power to grant an assistance order (unlike a production order) is not contingent on any substantive evidentiary standard having been met (*e.g.,* reasonable grounds to believe) since law enforcement will have already met the evidentiary standard required for a search warrant.

i. Telus

65 Pearson & Ling, cit. 15, above.

66 *R. v. National Post*, [2010] 1 S.C.R. 477 at para. 78.

In *Telus*,[67] Telus received an assistance order in connection with an ongoing police investigation (the details of which were subject to a sealing order). The assistance order was in support of a transmission data recorder warrant ("TDRW") the police had obtained that allowed them to intercept the transmission data associated with certain phone numbers. The assistance order required Telus to provide subscriber information (customer name and address) that matched the phone numbers corresponding to the transmission data. Without the subscriber information, the police would only have known that one number had called another. The additional information gave the police evidence of who was calling whom and where they might be found.

Telus brought a challenge to this assistance order on the grounds that it infringed the privacy rights of its users and that it was an improper use of an assistance order. Telus argued that because assistance orders have no independent evidentiary threshold, they are not intended to transform one search power (a TDRW, which allows the police to access transmission data but not the subscriber information associated with that data) into a more invasive search power. Telus argued that the assistance order was unlawful because it went beyond providing the information specified in the warrant (transmission data) and extended it by connecting that information to specific individuals. Justice Nordheimer rejected this argument in terms that supported a sweeping breadth for assistance orders:

> TELUS contends that all an assistance order is intended to do is to ensure that the technical aspects, of making the TDRW operate as intended, are achieved. I do not agree. The wording of s. 487.02 is not that narrow. The section refers expressly to the fact that the granting of an assistance order is for the purpose of giving "effect to" an authorization. It does not say, for example, that its purpose is to "implement" or "execute" an authorization. In my view, to give effect to an authorization is not to be read as simply requiring the application of technical know-how, such as connecting wires, or flicking switches, or permitting the police to "plug into" a system. Rather, an assistance order is intended to do exactly what it says: to give effect to the authorization. I note that one of the definitions for the word "effect" is "the extent to which something succeeds or is operative".[68]

The *Telus* decision adopts an unduly broad approach to the scope of assistance orders. If Justice Nordheimer is correct, assistance orders may be used to compel companies to do what is necessary to give effect to a warrant. This approach does not taken into account any of the careful balancing of competing objectives that occurs under the analysis outlined by Magistrate Judge Orenstein in the New York iPhone unlocking decision.[69] The breadth of this approach may have been appropriate in an age when assistance orders were used to require landlords to open locked rooms, but does not represent a fair or well-reasoned division of responsibilities between companies and law enforcement in the context of digital investigations.

---

67 *R. v. Telus*, 2015 ONSC 3964.

68 Ibid. at para. 45; A somewhat different result was reached by the Alberta Provincial Court in *Reference Re Criminal Code, s. 487.016*, 2015 ABPC 178. In that case, police sought to obtain subscriber information through the use of a production order rather than an assistance order in support of a TDRW. The Court held that proper route to doing so was to resort to the general production order power in s. 487.014.68 This is significant because it requires the police to meet an independent evidentiary threshold with respect to the subscriber information specifically (*i.e.,* reasonable grounds to believe that the subscriber information will afford evidence of an offence).

69 *In Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant*, cit 11, above.

ii. Rogers

More recently, Telus and Rogers scored a victory in a battle against a "tower dump" production order.[70] They sought relief after being served with particularly broad and onerous production orders sought by police in the context of an investigation of a string jewelry store robberies.[71] The production orders were for "tower dumps", *i.e.* a blanket disclosure to police of cell phone records for all phones activated, receiving, or transmitting near the scenes of the crimes, including customer names and addresses.[72] The production orders as drafted required this information to be provided for over 40,000 customers of Rogers and Telus.[73] The actual production orders in issue had been revoked by police and replaced with narrower ones to permit the investigation to move forward, but Telus and Rogers proceeded with the challenge as a test case.

Justice Sproat held that there was a reasonable expectation of privacy both in the cell phone records and in the location information that police were seeking.[74] He referred to the submissions of counsel for Telus and Rogers, that "tower dumps" were unusual in that 99.9% of the individuals whose information was disclosed were not suspected of anything.[75] Justice Sproat endorsed the "minimal intrusion" principle as the animating principle behind the leading decisions of the Supreme Court, that "the state must always be alive to the privacy interests of the individual and must always infringe such interests as little as possible".[76] Justice Sproat forcefully concluded that the production orders were "overly broad" and "went far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation".[77]

Telus and Rogers asked the Court to provide guidelines for future use for parties to determine their obligations under production orders. The Court set out a number of guidelines for police requesting such orders. He declined to state any guidance on the use, retention, or disclosure of information obtained by production orders by police, or to require that production orders only be used as a last resort, on the basis that these issues would be more appropriately left to Parliament.[78] He set forth the following guidelines for police to follow in requesting production orders (and corresponding principles for justices in issuing them)[79]:

> a) One – a statement or explanation that demonstrates that the officer seeking the production order is aware of the principles of incrementalism and minimal intrusion and has tailored the requested order with that in mind. – An awareness of the *Charter*

70 *R. v Rogers Communications*, 2016 ONSC 70.

71 Ibid. at paras. 2, 5.

72 Ibid. at paras. 5 – 6.

73 Ibid. at para. 7.

74 Ibid. at para. 19.

75 Ibid. at para. 25.

76 Ibid. at para. 41.

77 Ibid. at para. 42.

78 Ibid.at paras. 60, 64.

79 Ibid. at para. 65.

requirements is obviously essential to ensure that production orders are focused and *Charter* compliant.

b) Two – an explanation as to why all of the named locations or cell towers, and all of the requested dates and time parameters, are relevant to the investigation. – This flows from what is now the s. 487.014(2)(b) *Criminal Code* requirement that there be reasonable grounds to believe that the documents or data requested will afford evidence respecting the commission of the offence.

c) Three – an explanation as to why all of the types of records sought are relevant. - For example, the Production Orders sought bank and credit card information, and information as to name and location of the party to the telephone call or text communication who was not proximate to the robbery location. This information was clearly irrelevant to the police investigation.

d) Four – any other details or parameters which might permit the target of the production order to conduct a narrower search and produce fewer records. – For example, if the evidence indicates that a robber made a series of calls lasting less than one minute this detail might permit the target of the order to narrow the search and reduce the number of records to be produced. If the evidence indicates that the robber only made telephone calls then there may be no grounds to request records of text messages. (Although the use of voice recognition software may make it difficult to distinguish between a person making a telephone call and a person dictating a text message.)

e) Five – a request for a report based on specified data instead of a request for the underlying data itself. – For example, in this case a report on which telephone numbers utilized towers proximate to multiple robbery locations would contain identifying information concerning only a small number of robbery suspects and not the personal information of more than 40,000 subscribers which the Production Orders sought. This would avoid the concern expressed by Telus that 99.9% of vast amounts of tower dump personal information relate to individuals who are not actually suspects.

f) Six – If there is a request for the underlying data there should be a justification for that request. – In other words, there should be an explanation why the underlying data is required and why a report based on that data will not suffice.

g) Seven – confirmation that the types and amounts of data that are requested can be meaningfully reviewed. – If the previous guidelines have been followed the production order should be focused which will minimize the possibility of an order to produce unmanageable amounts of data. This confirmation does, however, provide an additional assurance of *Charter* compliance.

It is also noteworthy that the subject of a production order may apply to a court under s. 487.0193(4)(a) to have the order set aside or varied where it would be "unreasonable in the circumstances to require the applicant to prepare or produce the document"; although the Supreme Court has rejected the application of an "undue burden" standard and has held with respect to financial burdens, the test is that "the financial consequences must be so burdensome

that it would be unreasonable in the circumstances to expect compliance".[80] Oddly, there is no equivalent provision permitting a third party to challenge an assistance order. It is difficult in principle to see why the subject of an assistance order should not be afforded the opportunity to make such an application.[81]

The *Rogers* case shows that the courts are alive to the potential impact of digital investigative techniques on a company's broader user base. Even where a statutory investigative power appears to permit sweeping culls of personal information, the courts may impose judicial constraints to protect the privacy rights of third parties. This analysis, and in particular the "minimization principle" will no doubt be litigated in future challenges to assistance orders. If Apple seeks to challenge an assistance order in Canada, the risk of undermining data security for all of its users may prove to be a compelling violation of the minimization principle that would warrant quashing the order.

A final question in this area is whether police may seek to use the "general warrant" power under s. 487.01 of the *Criminal Code*. Section 487.01 provides authority for the issue of a warrant to allow police to:

> use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if
>
> (a) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing;
>
> (b) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and
>
> (c) there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.

Section 487.01 was enacted in 1993 as part of a series of amendments to the *Criminal Code* in Bill C-109, S.C. 1993, c. 40. It was meant to make search warrants available for techniques or procedures not specified in the *Criminal Code*, but only as a residual source of authority.[82] It was enacted in response to the Supreme Court of Canada's decision in *R. v. Wong*,[83] which held that the *Criminal Code* did not authorize surreptitious video surveillance of private activities. In practice, s. 487.01 has most often been used to authorize covert entry (aka "sneak and peak") searches in drugs cases.[84]

---

80 *Tele-Mobile Company (aka Telus Mobility) v. Ontario*, [2008] 1 S.C.R. 305 at para. 67.

81 This lacuna may make the regime susceptible to a *Charter* challenge..

82 *R. v. TELUS Communications Co.*,]2013] 2 S.C.R. 3 at para. 16, *per* Abella J. (plurality opinion).

83 *R. v. Wong*, [1990] 3 S.C.R. 36.

84 See e.g. *R. v. Ha*, 2009 ONCA 340.

There are several aspects of s. 487.01 that would make it a better fit than the provisions discussed above for use in the encryption context. Section 487.01 was enacted specifically with a view to emerging technologies or techniques that the *Criminal Code* did not specifically authorize. The provision balances a broad authorization with substantive limits on its use. Unlike assistance orders, a general warrant has a stand-alone requirement for reasonable grounds to believe. Section 487.01 also includes additional requirements that the issue of the warrant is in the best interests of justice and that no other provision is available. These limits would be useful in the encryption context by requiring judges to give due consideration to the legitimate interests of third party companies and their users before making an order.

Despite these advantages, however, it is questionable whether the provision as currently framed could be used to compel a tech company to decrypt a digital device. Certainly, this use of the provision is removed from the original context for s. 487.01. More importantly, it is an awkward fit with the text of the statute, which creates a power to authorize police to "use any device or investigative technique or procedure or do any thing described in the warrant". This language appears to authorize police to use their own techniques or devices (and thus may permit police to use certain decryption techniques) but makes no reference to the devices or techniques of third parties. As such, s. 487.01 may be more useful as a guide to the public debate around what legislation in this area might look like rather than a direct answer to the problem.

V. Conclusion

The courts have been keen to ensure that privacy protections extend to the customers of telecommunications carriers. But the FBI v. Apple debate, and cases like it, mark a new direction for digital privacy law. At issue is not simply the production of specific user data, but rather the very question of whether Canadian technology companies should be permitted to develop forms of encryption that they themselves cannot decrypt.

A number of statutory provisions in Canadian law (especially the assistance order power in s. 487.02 of the *Criminal Code*) use broad language that law enforcement may seek to take avail itself of to compel third technology companies to crack their own encryption. But this would be an unfortunate result for Canadians. Bill C-30, which proposed broad surveillance measures that would have limited the ability of telecommunications carriers to use encryption technology, was abandoned by the government after a public outcry. To use the courts to achieve the same result by applying provisions that never contemplated the world of encryption would result in a drastic change in the privacy landscape without the benefit of dialogue. Encryption is a necessary tool to safeguard the wide range of private activity that has migrated to digital spaces. Weakening encryption by requiring tech companies to install backdoors for law enforcement would have serious negative impacts on millions of innocent users. The impacts of assistance orders on the private lives of all Canadians is a consideration that must weigh heavily in the balance in the next iteration of the encryption debate in Canadian courts.