TULANE JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW

VOLUME 25 SPRING 2017 NO. 2

The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users During the Course of Criminal Investigations in Canada and the United States

Sarit K. Mizrahi*

Cloud computing is generally favored for its provision of flexible on demand computing services. This is rendered possible by its multi-tenant and elastic properties based on which various virtual resources, all hosted on the same physical machine and allocated based on demand, are shared among numerous users unknown to one another. Within public clouds, this infrastructure exposes users to the risk of having their data stored alongside that of criminals using the cloud to store information relating to their illegal activities. As such, when law enforcement officers use digital forensics to search and seize data regarding criminal activity from servers that host public clouds, they may incidentally access the data of innocent cloud users in the process because there is no segregation between innocent users' information and that of the individual being investigated.

Using a comparative methodology, this Article argues that, while neither United States nor Canadian law serves to provide a sufficient degree of protection to the private data of innocent cloud users during cloud computing forensic investigations, safeguards offered in the United States to this effect are somewhat more accentuated than those extended by its Canadian counterpart. This is achieved by first outlining the privacy violations that innocent cloud users may be subject to throughout cloud criminal investigations, and then proceeding to examine the manner that the laws applicable to searches and seizures in each of these jurisdictions influence these incidental privacy breaches.

* © 2017 Sarit K. Mizrahi. LL.B., J.D., & LL.M. in Information Technology Law (University of Montreal); Ph.D. Candidate in Law and Technology (University of Ottawa); member of the Barreau du Québec; recipient of the Prix Henri Capitant 2014 for best Master's thesis; recipient of the Joseph-Armand Bombardier CGS Scholarship. I would like to thank Professor Elizabeth Judge for her insightful and helpful comments, as well as the members of the *Tulane Journal of International and Comparative Law* for their effort in editing my Article.

I. INTRODUCTION

Cybercrime is a rising societal problem that law enforcement has been grappling with for over a decade.[1] With new technologies such as cloud computing, enabling individuals to remotely store and access data seamlessly across borders, law enforcement has found it increasingly difficult to investigate threats of criminal activity, often resorting to any methods necessary to catch perpetrators. In their staunch desire to see

1. *See*, *e.g.*, Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 35 (2001) [hereinafter Bellia, *Chasing Bits*]; Philip Attfield, United States v Gorshkov*: Detail Forensics and Case Study; Expert Witness Perspective*, *in* PROCEEDINGS OF THE FIRST INTERNATIONAL WORKSHOP ON SYSTEMATIC APPROACHES TO DIGITAL FORENSIC ENGINEERING 3 (2005).

that these criminals face the reprimands of the law for their actions, however, law enforcement officers often neglect to consider the privacy violations that could be incurred to innocent users by criminal investigations performed in cyberspace.[2]

The privacy of the legitimate users in virtual environments is particularly accentuated when criminal investigations are performed in the public cloud. Cloud computing is often favored by individuals to store their data as a result of its ability to provide flexible on demand remote computing services.[3] This flexibility is accomplished using a multi-tenant platform where a pool of computing resources is allocated according to demand and shared among various users who are unknown to one another.[4] This infrastructure, however, necessarily exposes cloud users to the risk of having their data stored alongside that of criminals exploiting the cloud for illicit purposes. When law enforcement officers investigate the behavior of these lawless actors, they will inevitably access the data of legitimate users incidentally because they are unable to segregate this data from that of the individuals being investigated.[5]

Although law enforcement is endowed with rather sophisticated digital forensic technology, no resources exist that are adequate to sufficiently respond to this particular characteristic of the public cloud to

---

2. *See*, *e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005) [hereinafter Kerr, *Searches and Seizures*]; Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 40 (2001-2002); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 76 (1994); Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165, 1231 (1993); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006 (2010) [hereinafter Kerr, *Fourth Amendment and Internet*]; Matthew Johnson, *Privacy in the Balance—Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8,* 58 CRIM. L. Q. 442, 482 (2012); MICHAEL GEIST, LAW, PRIVACY AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 2 (Michael Geist ed., 2015) (ebook).

3. WAYNE JANSEN & TIMOTHY GRANCE, U.S. DEP'T COMMERCE, NAT'L INST. STANDARDS & TECH. [NIST], GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING 27 (NIST Special Pub. 800-144, 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

4. *Id.* at 11; PETER MELL & TIMOTHY GRANCE, U.S. DEP'T COMMERCE, NIST, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2 (NIST Special Pub. 800-145, 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

5. *See* NIST Cloud Computing Forensic Science Working Group, *NIST Cloud Computing: Forensic Science Challenges* (U.S. Dep't Commerce, NIST, NISTIR No. 8006, 2014), http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf [hereinafter NIST Cloud Forensic Challenges]; Keyun Ruan et al., *Cloud Forensics*, *in* ADVANCES IN DIGITAL FORENSICS VII 15, 22 (Gilbert Peterson & Sujeet Shenoi eds., 2011) [hereinafter Ruan et al., *Cloud Forensics*].

ensure the privacy protection of innocent cloud users.[6] It thus remains a matter of the law to maintain clear boundaries that ensure law enforcement does not overexert its powers in a manner that would infringe upon the privacy rights of legitimate users.

This Article will closely examine the legal frameworks surrounding the performance of criminal investigations and their extension to digital environments of both Canada and United States. The aim of this analysis is to determine whether each of the two jurisdictions sufficiently limits the powers of law enforcement in a manner that serves to adequately protect the privacy of public cloud users.

These comparators were chosen because Canada is generally viewed as a country that is largely protective of privacy, whereas the United States is often internationally criticized for implementing laws that erode user privacy.[7] The most recent in a long line of such accusations resulted in the European Court of Justice's invalidation of the Safe Harbor provisions,[8] which allowed the personal information of European citizens to be hosted in cloud servers located throughout the United States. The reason given by the Court for the dissolution of this Act was the allegedly indiscriminate surveillance practices adopted by the U.S. government, which the European Court of Justice determined had violated the privacy rights of European citizens.[9]

Canada was chosen, rather than another privacy-protective nation, because, in addition to being the United States' neighbor to the north, Canada is becoming an increasingly popular location for cloud data centers. Due to Canada's cold weather, affordable electricity costs, and business tax credits offered by some provincial governments,[10] eight major Cloud Service Providers (CSPs) have developed cloud server

---

6. *See* NIST Cloud Forensic Challenges, *supra* note 5, at 2; Ruan et al., *Cloud Forensics*, *supra* note 5, at 35-36.

7. *See* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 359-61, 394-95 (2005); Yves Faguy, *Privacy in the Age of Big Data*, CAN. B. ASS'N NAT'L MAG. (Nov. 11, 2014), http://www.nationalmagazine.ca/Articles/November-2014-Web/Privacy-in-the-age-of-Big-Data.aspx; *Privacy Laws in the United States, the European Union and Canada*, INNOVATIONS IDENTITY BLOG (Oct. 1, 2014), https://www.trulioo.com/blog/global-solution-privacy-laws-in-the-united-states-the-european-union-and-canada/.

8. *Safe Harbor*, EXPORT.GOV, http://2016.export.gov/safeharbor/ (last visited Apr. 4, 2017).

9. Natalia Drozdiak & Sam Schechner, *EU Court Says Data-Transfer Pact with U.S. Violates Privacy*, WALL STREET J. (Oct. 6, 2015, 1:42 PM), www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361.

10. Peter Nowak, *Why Google Built Its First Canadian Cloud Computing Facility in Montreal*, CANADIAN BUS. (Mar. 9, 2017), http://www.canadianbusiness.com/innovation/google-cloud-montreal/.

farms on Canadian territory within the past two years.[11] Even more recently, Google announced that it will develop a cloud region in the province of Quebec by the end of 2018.[12]

In adopting a comparative methodology,[13] the aim of this Article is to demonstrate that despite international criticisms of the United States, its laws governing the search and seizure of data as they extend to digital environments, such as the cloud, are not any more invasive of innocent users' privacy than those of its Canadian counterpart. To demonstrate the veracity of this statement, this Article will begin by examining the seemingly dichotomous role of CSPs in their obligation to assist law enforcement while simultaneously protecting user privacy. It will then proceed to briefly examine the cloud forensic techniques currently available and how their use for the search and seizure of the cloud data belonging to criminals risks incidentally violating innocent users' privacy. This Article will then compare the investigatory powers afforded to law enforcement by Canadian and U.S. law so as to demonstrate that the latter more effectively protects against incidental violations of the

---

11. Shane Dingman, *Microsoft To Build Two Data Centres in Canada as It Expands Cloud Services*, GLOBE & MAIL (June 2, 2015), http://www.theglobeandmail.com/technology/microsoft-to-build-two-data-centres-in-canada-as-it-expands-cloud-services/article24756853/; *Amazon Will Open Its First Canadian Data Centre in Montreal*, CBC NEWS (Jan. 15, 2016), http://www.cbc.ca/news/canada/montreal/amazon-aws-montral-data-center-1.3405616; Press Release, IBM, IBM Opens New Cloud Centre in Québec (Mar. 9, 2015), https://www.ibm.com/news/ca/en/2015/03/09/e715377m88048f63.html; Guillaume Gilbert, *OVH Finds a New Home in Montreal and Scales Up Its Ambitions for North America*, OVH NEWS (Oct. 28, 2015), https://www.ovh.com/ca/en/a1952.inauguration-new-headquarters-ovh-montreal; Press Release, Bell Business Markets, Bell Business Markets Announces Major Enhancements to Québec's Largest Data Centre (July 31, 2015), https://business.bell.ca/support/enterprise/montreal-data-centre-expansion; Kathryn Greenaway, *West Island Offers Ideal Conditions for Expansive Data Centres*, MONTREAL GAZETTE (Mar. 1, 2017), http://montrealgazette.com/news/local-news/west-island-gazette/west-island-offers-ideal-conditions-for-expansive-data-centres.

12. Josh McConnell, *Google Inc Announces First Canadian 'Cloud Region' in Montreal, Allows Sensitive Data To Stay Within Borders*, FIN. POST (Mar. 9, 2017), http://business.financialpost.com/fp-tech-desk/google-inc-announces-first-canadian-cloud-region-in-montreal-allows-sensitive-data-to-stay-within-borders?__lsa=a005-5c00.

13. To this effect, this Article will employ the functional approach of comparative law adopted by Konrad Zweigert & Hein Kötz, which maintains that laws aimed at fulfilling the same functions are sufficiently similar and may be compared. KONRAD ZWEIGERT & HEIN KÖTZ, AN INTRODUCTION TO COMPARATIVE LAW 2 (vol. I, 1977). Although the claim of this approach that the context of the law is irrelevant in comparative legal analyses has often been criticized, there is in fact room for the examination of the context of the law despite claims to the opposite. Jaakko Husa, *Methodology of Comparative Law Today: From Paradoxes to Flexibility*, 57 REVUE INT'L DE DROIT COMPARÉ 1095, 1104 (2006). That having been said, while this Article will examine the relevant context of the laws where it might affect the present comparison, it is not believed that this criticism will have much of an effect on the validity of this Article's contribution simply due to the fact that both the Canadian and U.S. laws relevant to this subject matter are substantially similar in their function, as well as comparable as to the contexts under which they were adopted.

privacy rights of innocent cloud users during the performance of criminal investigations. Finally, this Article will conclude by discussing the reasons that we believe Canadian law does *not*, contrary to popular belief, offer more acute protection to the privacy rights of innocent cloud users than U.S. law.

II. THE ROLE OF CLOUD SERVICE PROVIDERS IN THE SEARCH AND SEIZURE OF EVIDENCE IN THE CLOUD: GUARDING USER PRIVACY VS. ASSISTING LAW ENFORCEMENT

While the law is at the forefront with respect to the extent of privacy protection afforded to individuals during the course of cloud forensic investigations, CSPs play a significant role as well, depending on how they offer their services or if they choose to cooperate with law enforcement.[14] This Part will, in reference to five of the most widely used public cloud services, namely Dropbox, Amazon Cloud Drive, Google Drive, Microsoft's OneDrive, and Apple's iCloud,[15] outline both the method these services use to store data and how that method may affect user privacy, as well as the degree to which the language of terms of services agreements and privacy policies of each entity extends users privacy protection.

A. Cloud Service Provider Storage Practices and Their Impact on User Privacy

Two of the most attractive features of the cloud are its constant availability of stored data and the elasticity of cloud provisions.[16] The former is achieved by making multiple copies of the data in question and storing them across several servers so that if one of these servers should become inaccessible, the user will be able to access this information via another one.[17] Cloud provisions' elasticity, on the other hand, renders it possible to provide services to users based on demand and can be

---

14. *See* Nate Cardozo et al., *Electronic Frontier Foundation's Fifth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data*, ELECTRONIC FRONTIER FOUND. 4-5 (June 17, 2015), https://www.eff.org/files/2015/06/18/who_has_your_back_2015_protecting_your_data_from_government_requests_20150618.pdf.

15. Anthony Agius, *Five Popular Cloud Storage Services Compared*, PC & TECH AUTHORITY (Dec. 3, 2015), http://www.pcauthority.com.au/Feature/412614,five-popular-cloud-storage-services-compared.aspx; Edward Gately, *Survey Suggests SMB Market Embracing Cloud for Data Storage*, CHANNEL PARTNERS (Dec. 10, 2015), http://www.channelpartnersonline.com/news/2015/12/survey-suggests-smb-market-embracing-cloud-for-da.aspx.

16. MELL & GRANCE, *supra* note 4, at 2.

17. *Id.*

appropriated in unlimited quantities at any time.[18] In order to ensure these qualities, however, CSPs must use methods of storing user data that allow them to feasibly continue offering constantly available and scalable services.[19]

There are essentially two methods used for the storage of cloud data, namely block storage and object storage. Block storage splits files into evenly sized blocks of data, each with its own address, but with no additional data that provides context regarding what information that block contains.[20] In contrast, object storage can store large quantities of data in an object that is designated by additional data markers, known as metadata, permitting the stored data to be identified.[21] The main benefit of the object storage method is that it requires much less server space to store data. The move towards object storage is the result of the petabytes worth of data now being stored in the cloud and CSPs' inability to meet these demands with traditional forms of storage.[22] Furthermore, CSPs are able to avoid the duplication of data by using object storage, thus avoiding wasted server space by storing more than one copy of the same information.[23]

Out of the five most widely used public clouds, namely Dropbox, Amazon Cloud Drive, Google Drive, Microsoft's OneDrive, and Apple's iCloud,[24] only Dropbox is transparent with respect to the methods it uses.[25] To begin with, while Dropbox outsources the actual storage of

---

18. *Id.*

19. Yadin Porter de Léon & Tony Piscopo, *Object Storage Versus Block Storage: Understanding the Technology Differences*, DRUVA BLOG (Aug. 14, 2014), https://www.druva.com/blog/object-storage-versus-block-storage-understanding-technology-differences/.

20. *See* Alain Azagury et al., *Toward an Object Store*, *in* PROCEEDINGS OF THE 20TH IEEE/11TH NASA GODDARD CONFERENCE ON MASS STORAGE SYSTEMS AND TECHNOLOGIES 165 (2003).

21. *See* Michael Factor et al., *Object Storage: The Future Building Block for Storage Systems*, *in* LOCAL TO GLOBAL DATA INOPERABILITY—CHALLENGES AND TECHNOLOGIES 119-120 (2005).

22. Porter de Léon & Piscopo, *supra* note 19.

23. This should not be confused with the practice of replication used to ensure constant data availability, which is still done by CSPs.

24. Agius, *supra* note 15; Gately, *supra* note 15.

25. Although Amazon Cloud Drive appears to enable object file storage through reference to Amazon S3, it is not clear as to whether all files stored on Amazon Cloud Drive are done so in this manner. Peter Heinrich, *Amazon Cloud Drive Now Accessible via REST-based API*, AMAZON: DEVELOPER (Nov. 11, 2014), https://developer.amazon.com/public/community/post/TxRNQX3SWVLUYC/Amazon-Cloud-Drive-Now-Accessible-via-REST-based-API. Additionally, while Google and Microsoft are clear about their use of object storage for some of their paid services, they do not provide any information as to the manner in which they store data in their free services, OneDrive and Google Drive respectively. *See Objects*, GOOGLE CLOUD PLATFORM, https://cloud.google.com/storage/docs/json_api/v1/objects (last visited Apr. 4, 2017); *Introduction to Microsoft Azure Storage*, MICROSOFT AZURE (Feb. 24, 2017), https://azure.

users' files to Amazon S3,[26] which notes its use of object storage,[27] Dropbox itself manages the metadata of the files stored using its own services. To this effect, Dropbox modified its privacy policy in 2011 to inform users that, in order to make its services more efficient, it "may de-duplicate files, which means [it stores] only one copy of files or pieces of files that are the same."[28]

Dropbox has the ability to determine that a file is already present on its servers through use of specialized software that compares files being uploaded with those that already exist, removing any files that are not unique. A link to the existing file replaces the duplicate file so that it can ultimately be accessed by each user who sought to upload it.[29] Take, for example, a popular song that is uploaded by hundreds of users; rather than wasting server space to store each one of these copies, Dropbox will keep a single copy and provide all the users who uploaded the song with a link that will allow them to access it. It is not difficult to tell when an upload is a duplicate of a certain file already existing in Dropbox's system as, rather than taking the usual amount of time to upload large files to the service, it will be done in an instant.[30] Although Dropbox does encrypt all user data, it only does so once the entire file has been transmitted to its servers and, as such, renders the process of de-duplication possible.[31]

This feature could have severe privacy implications for Dropbox users, not the least of which is that law enforcement agencies have the ability to use this practice to their advantage by attempting to upload contentious files to Dropbox, and if the files load more quickly than would be expected of typical files that size, they may be able to obtain a

---

microsoft.com/en-us/documentation/articles/storage-introduction. Finally, Apple provides no information as to the manner in which they store cloud data.

26. *Working with Amazon S3 Buckets*, AMAZON: WEB SERVICES, http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html (last visited Apr. 4, 2017) (note that this is a different cloud than the Amazon Cloud Drive, which is a free service).

27. *Amazon S3*, AMAZON: WEB SERVICES, https://aws.amazon.com/s3/ (last visited Apr. 4, 2017).

28. Drew & Arash, *Changes to Our Policies (Updated)*, DROPBOX: BLOG (July 1, 2011), https://blogs.dropbox.com/dropbox/2011/07/changes-to-our-policies/.

29. Chris Poelker, *Data Reduplication in the Cloud Explained, Part One*, COMPUTERWORLD (Aug. 20, 2013), http://www.computerworld.com/article/2474479/data-center/data-deduplication-in-the-cloud-explained--part-one.html.

30. Stephen Foskett, *How Does Dropbox Store Data?*, BLOG.FOSKETTS.NET (July 11, 2011), http://blog.fosketts.net/2011/07/11/dropbox-data-format-deduplication/.

31. *Is Dropbox Safe To Use?*, DROPBOX: HELP CTR., https://www.dropbox.com/help/27 (last visited Apr. 4, 2017); Christopher Soghoian, *How Dropbox Sacrifices User Privacy for Cost Savings*, SLIGHT PARANOIA BLOG (Apr. 12, 2011), http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html.

court order for this information.[32] However, after the de-duplication feature was manipulated to trick Dropbox into providing individuals with access to files that they did not already possess,[33] Dropbox removed the de-duplication clause from its privacy policy.[34] While this clause's removal appears to denote that it has ceased employing this practice, no official statement was made to that effect by the company itself. Furthermore, although Dropbox encrypts all user data, both in transit using Secure Socket Layer (SSL)[35] and at rest, using 256-bit Advanced Encryption Standard (AES),[36] the fact that the encryption of these files is performed by Dropbox itself means that this entity possesses the keys to render this data readable again. Considering that its policies do not contain any indication to the contrary,[37] it would be entirely possible for Dropbox to hand over user data to law enforcement in its unencrypted form.

Although the other CSPs listed above do not provide information as to whether they use block storage or object storage methods for their user data, they do provide some information as to the level of encryption that their users' information enjoys through their services. To begin with, Amazon only uses SSL to protect its user data.[38] Although Google uses this same method of encryption for "many of [its] services," it neglects to specify exactly which of its services utilize this level of protection.[39] In addition to using SSL, OneDrive is protected by an encryption method known as "forward secrecy" that renders retrospective decryption impossible.[40] The iCloud, on the other hand, also uses SSL encryption for

---

32. Soghoian, *supra* note 31.

33. Kyle Orland, *Dropbox Knows When You're Playing Pirate*, WIRED UK (Mar. 31, 2014), http://www.wired.co.uk/article/dropbox-dmca-position; Mike Masnick, *Dropbox Tries To Kill Off Open Source Project with DMCA Takedown*, TECHDIRT.COM (Apr. 26, 2011, 8:00 AM), https://www.techdirt.com/articles/20110425/15541514030/dropbox-tries-to-kill-off-open-source-project-with-dmca-takedown.shtml.

34. *Dropbox Privacy Policy*, DROPBOX, https://www.dropbox.com/privacy (last visited Apr. 4, 2017).

35. Standard Socket Layer is a standard form of encryption meant to protect the information being transmitted between a server and a client.

36. Advanced Encryption Standards are used to protect the privacy and confidentiality of data at rest by rendering it indecipherable to anyone other than the person who possesses the key to unscrambling it.

37. *Dropbox Privacy Policy*, *supra* note 34.

38. *Amazon.ca Privacy Notice*, AMAZON.CA, https://www.amazon.ca/gp/help/customer/display.html/?ie=UTF8&nodeId=918814 (last visited Apr. 4, 2017).

39. *Welcome to the Google Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy/ (last visited Apr. 4, 2017) [hereinafter *Google Privacy Policy*].

40. *Advancing Our Encryption and Transparency Efforts*, MICROSOFT ON ISSUES BLOG (July 1, 2014), http://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/#sm.000xov96ootacq610ir1z56ynxqr0; Adam Langley, *Protecting Data*

data in transit in addition to "a minimum of 128-bit AES"[41] for data at rest, which is considerably less secure than its 256-bit counterpart.[42] That having been said, the latter is used by Apple to encrypt the iCloud keychain, which is used for the storage and transmission of passwords and credit card data along with other more sophisticated encryption methods.[43] These encryption keys are created directly on the user device that renders them inaccessible to Apple. However, while Apple retains the encryption keys of all other data at rest that does not use the iCloud keychain, it specifies that it *never* shares user encryption keys with third parties,[44] which would include law enforcement.

Despite these levels of protection offered, there is an aspect of these cloud services that could present serious privacy violations for users: the creation of trails of digital artifacts. Digital artifacts are essentially remains left behind on a person's digital devices, be they computers or mobile devices, that indicate that the individual owner stored data in the cloud of a particular CSP. These types of artifacts are left behind by Dropbox,[45] Amazon Cloud Drive,[46] Google Drive,[47] OneDrive,[48] and the iCloud[49] alike. Digital artifacts render it possible not only for law enforcement officers to know that one of these particular services has been used by an individual but may also enable them to locate the data in

---

for the Long Term with Forward Secrecy, GOOGLE: SECURITY BLOG (Nov. 22, 2011), https://security.googleblog.com/2011/11/protecting-data-for-long-term-with.html.

41. *iCloud Security and Privacy Overview*, APPLE, https://support.apple.com/en-ca/HT202303 (last visited Apr. 4, 2017).

42. *See* NAT'L INST. OF STANDARDS &TECH., FED. INFO. PROCESSING STANDARDS NO. 197, ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) 27-32 (2001), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

43. *iCloud Security and Privacy Overview*, APPLE, *supra* note 41.

44. *Id.*

45. *See* Darren Quick & Kim Kwang Raymond Choo, *Dropbox Analysis: Data Remnants on User Machines*, 10 DIGITAL INVESTIGATION 3 *passim* (2014); S. Mehreen & B. Aslam, *Windows 8 Cloud Storage Analysis: Dropbox Forensics*, *in* PROCEEDINGS OF 12TH INTERNATIONAL BHURBAN CONFERENCE ON APPLIED SCIENCES AND TECHNOLOGY (IBCAST) 312 (2015).

46. *See* Jason S. Hale, *Amazon Cloud Drive Forensic Analysis*, 10 DIGITAL INVESTIGATION 259 *passim* (2013).

47. *See* Darren Quick & Kim Kwang Raymond Choo, *Google Drive: Forensic Analysis of Data Remnants*, 40 J. NETWORK & COMPUTER APPLICATIONS 179, 179 (2014).

48. Darren Quick & Kim Kwang Raymond Choo, *Digital Droplets: Microsoft SkyDrive Forensic Data Remnants*, 29 FUTURE GENERATION COMPUTER SYSTEMS 1378, 1378 (2013). SkyDrive was the former name of OneDrive, which was changed for trademark infringement purposes; the services offered are the same. *From SkyDrive to OneDrive*, MICROSOFT, https://support.microsoft.com/en-us/help/17787/skydrive-to-onedrive (last visited Apr. 4, 2017).

49. *See* Kurt Oestreicher, *A Forensically Robust Method for Acquisition of iCloud Data*, 11 DIGITAL INVESTIGATION 106 *passim* (2014).

question within that cloud. Performing searches based on trails of digital artifacts, however, has serious implications for the privacy of innocent cloud users, as will be discussed in further detail in the next Part.

B. The Protection of User Privacy in the Terms of Service Agreements and Privacy Policies of Cloud Service Providers

This Section will be dedicated to the examination of the documents governing the relations between cloud users and five CSPs, namely Amazon Cloud Drive, Dropbox, Google Drive, OneDrive, and iCloud, so as to determine the extent to which each respects the privacy protection of its users.[50] This analysis will not, however, be accomplished in the traditional manner of viewing the terms of service agreements and privacy policies of these entities in light of their alignment with commonly held standards of privacy. Rather, it will be achieved by examining these documents based on whether they exude forensic readiness, meaning that the documents governing the relations of the user and the CSP would not inhibit any criminal investigations performed within that particular cloud service.[51]

Digital forensic specialists maintain that terms of service agreements must be robust in both the powers they provide law enforcement officers as well as the permissions they accord CSPs to search and seize cloud data so as to adequately ensure forensic readiness.[52] In order to provide law enforcement with as wide of a berth

---

50. The versions of all the Terms of Service Agreements and Privacy Policies available to both Canadian and U.S. users were accessed for the purpose of this analysis. The author possesses a device with a Canadian Internet Protocol address and thus accessed the version of these documents available to Canadian users. In an effort to compare these terms with the ones imposed upon U.S. users, so as to determine whether there are any differences between the two, the author connected to a proxy server that was rerouted through the United States. While the author was able to choose to connect through a U.S. server, the city through which such connection took place, namely Dallas, was done automatically. The author has no reason to believe, however, that accessing these agreements through Dallas would provide different content than accessing it through any other American municipality. That having been said, both the Canadian and U.S. versions of these documents were compared, and there was no difference between the two with respect to the substantial nature of the clauses discussed in this Section.

51. Stephen Biggs & Stilianos Vidalis, *Cloud Computing: The Impact of Digital Forensic Investigations*, *in* INT'L CONF. FOR INTERNET TECH. & SECURED TRANSACTIONS 3-4 (2009).

52. *Id.*; Lucia De Marco et al., *Formalization of SLAs for Cloud Forensic Readiness*, *in* PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON CLOUD SECURITY MANAGEMENT ICCSM-2014 42 (Barbara Endicott-Popovsky ed., 2014); DIANE BARRETT & GREG KIPPER, VIRTUALIZATION AND FORENSICS: A DIGITAL FORENSIC INVESTIGATOR'S GUIDE TO VIRTUAL ENVIRONMENTS 206-09 (2010); Mpho Percy Makutasoane & Awie Leonard, *A Conceptual Framework To Determine the Digital Forensic Readiness of a Cloud Service Provider*, *in*

as possible in their investigative capability, the terms of service agreements must: (1) clearly delineate the tools, procedures, accesses and services related to forensic investigations;[53] (2) outline the roles of both the client and the CSP within the confines of a forensic investigation; (3) take into account and clearly state the effects of the laws and procedures of the various jurisdictions where their data centers are located in regard to the performance of a forensic investigation;[54] and (4) ensure that "their policies do not just act as a smoke screen,"[55] but rather actually permit CSPs to police the conditions included in their agreements by both allowing them certain powers of surveillance over the manner in which their services are used as well as permitting their cooperation with law enforcement.[56] These criteria can reveal the extent of privacy protection afforded to users in the terms and policies of their CSPs. Essentially, the more forensically ready a cloud is, the more extensive the powers of the CSP and law enforcement to perform searches and seizures in the cloud and, in turn, the more potential violation of innocent users' privacy.[57]

While none of the terms of service agreements of the CSPs presently under analysis specifically refer to the performance of forensic investigations within their cloud, thus precluding satisfaction of the first criterion of forensic readiness, the agreements do clearly outline the roles of both the user and the CSP. To begin with, the roles of cloud users are clearly outlined by governing how they may use the cloud services. They essentially prohibit a range of actions, namely requiring that users must not: violate either the CSP's policies[58] or the law;[59] infringe upon the

---

PROCEEDINGS OF PICMET '14: INFRASTRUCTURE AND SERVICE INTEGRATION 3313 (Dundar F. Kocaoglu ed., 2014).

53. De Marco et al., *supra* note 52, at 46-47.

54. *See* BARRETT & KIPPER, *supra* note 52, at 206-09.

55. Biggs & Vidalis, *supra* note 51, at 3.

56. *Id.* at 3-4; De Marco et al., *supra* note 52, at 44; Makutasoane & Leonard, *supra* note 52, at 3313.

57. *See* Ruan et al., *Cloud Forensics*, *supra* note 5, at 21; Sameera Almulla et al., *A State-of-the-Art Review of Cloud Forensics*, 9 J. DIGITAL FORENSICS, SECURITY & L. 7, 8 (2014).

58. *Dropbox Terms of Service*, DROPBOX, https://www.dropbox.com/privacy#terms (last visited Apr. 4, 2017); *Amazon Cloud Drive Terms of Use*, AMAZON, https://www.amazon.ca/gp/help/customer/display.html?nodeId=201376540 (last visited Apr. 4, 2017); *Google Terms of Service*, GOOGLE, https://www.google.com/policies/terms/ (last visited Apr. 4, 2017).

59. *Amazon Cloud Drive Terms of Use*, *supra* note 58; *Conditions of Use*, AMAZON, https://www.amazon.ca/gp/help/customer/display.html?nodeId=918816 (last visited Apr. 4, 2017); *Dropbox Terms of Service*, *supra* note 58; *Dropbox Acceptable Use Policy*, DROPBOX, https://www.dropbox.com/privacy#acceptable_use (last visited Apr. 4, 2017); *Google Terms of Service*, *supra* note 58; *Microsoft Services Agreement*, MICROSOFT, https://www.microsoft.com/en-us/servicesagreement/ (last visited Apr. 4, 2017); *iCloud Terms and Conditions*, APPLE, http://www.apple.com/legal/internet-services/icloud/en/terms.html (last visited Apr. 4, 2017).

intellectual property[60] or privacy rights[61] of others; share inappropriate material (such as nude photos);[62] transmit any virus that would put the security of the CSP's system at risk or send spam;[63] engage in any activity that exploits or harms children,[64] is fraudulent,[65] defamatory,[66] false, or misleading;[67] stalk, harass, threaten, or harm another; ask a minor for personal information if the user is an adult; impersonate another person or misrepresent themselves; plan or engage in any illegal activity; or gather and store the personal data of other users, or otherwise use this data to act in a manner that is prohibited by the terms of service.[68] In accordance with the second requirement of forensic readiness, the terms of service agreements of each of these CSPs clearly delineate the roles of users, essentially notifying them as to the type of conduct likely to lead to an investigation of their use of the services.

The roles of the CSPs are then clearly outlined in both their terms of service agreements and privacy policies. Essentially, while the former delineates the CSP's manner of supervising users to ensure compliance with their own agreements, the latter designates the conditions under which the CSPs will divulge user information. To begin with, the terms of service agreements of four of the CSPs, excluding Amazon, clearly outline surveillance practices. Due to the extensive power that it accords itself to review its users' content, iCloud would likely be the most forensically ready and thus the least respectful of user privacy. iCloud's term to this effect is tremendously permissive, essentially:

> [reserving] the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may pre-screen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable.[69]

While neither Dropbox or Google articulate this sentiment in as many words as iCloud, they state that they allow themselves to review user

---

60. *iCloud Terms and Conditions*, *supra* note 59; *Microsoft Services Agreement*, *supra* note 59; *Dropbox Terms of Service*, *supra* note 58.

61. *Conditions of Use*, *supra* note 59; *Microsoft Services Agreement*, *supra* note 59; *iCloud Terms and Conditions*, *supra* note 59; *Dropbox Terms of Service*, *supra* note 58.

62. *Conditions of Use*, *supra* note 59; *Microsoft Services Agreement*, *supra* note 59.

63. *Microsoft Services Agreement*, *supra* note 59; *iCloud Terms and Conditions*, *supra* note 59.

64. *Microsoft Services Agreement*, *supra* note 59.

65. *Dropbox Terms of Service*, *supra* note 58.

66. *Id.*

67. *Id.*; *Microsoft Services Agreement*, *supra* note 59.

68. *iCloud Terms and Conditions*, *supra* note 59.

69. *Id.*

content to ensure that it is neither illegal or a violation of their terms of service agreement.[70] That they reserve this power *prior* to obtaining a reason to suspect the user's conduct could permit surreptitiously scanning through all their users' documents and seriously eroding their privacy. Arguably, the CSP most respectful of user privacy would therefore be OneDrive, as its policy holds that it will only review users' content once an investigation has been launched pursuant to alleged violations of its terms of service agreement.[71]

The privacy policies of these CSPs, generally acting as corollaries to their terms of service agreements, clearly specify the reasons that will lead them to disclose the personal information of their users to law enforcement. While these policies go further in identifying the role of CSPs within the confines of a criminal investigation against one of their users, thus further ensuring forensic readiness, they also maintain a certain level of transparency with respect to the measures taken to protect user privacy. In regard to the privacy policies examined, it is notable that each CSP employs a different standard to assess whether it will divulge the private data of its users. Essentially, while some will only do so where the release of user information is appropriate[72] or reasonably appropriate,[73] others will rely on a "good-faith belief" that it is either necessary,[74] reasonably necessary,[75] or appropriate.[76]

The privacy policies also specify a host of reasons that dictate the necessity of disclosing the information of its users, namely for the purposes of: complying with the law,[77] regulation,[78] and legal processes;[79] preventing fraud;[80] protecting property rights;[81] protecting others from death or serious bodily injury;[82] maintaining the security of their system;[83]

---

70. *Dropbox Terms of Service*, *supra* note 58.

71. *Microsoft Services Agreement*, *supra* note 59.

72. *Amazon.ca Privacy Notice*, *supra* note 38.

73. *Dropbox Privacy Policy*, *supra* note 34.

74. *Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement/ (last visited Apr. 4, 2017).

75. *Google Privacy Policy*, *supra* note 39; *Privacy Policy*, APPLE, http://www.apple.com/privacy/privacy-policy/ (last visited Apr. 4, 2017) [hereinafter *Apple Privacy Policy*].

76. *Apple Privacy Policy*, *supra* note 75.

77. *Amazon.ca Privacy Notice*, *supra* note 38; *Dropbox Privacy Policy*, *supra* note 34; *Google Privacy Policy*, *supra* note 39; *Microsoft Privacy Statement*, *supra* note 74.

78. *Google Privacy Policy*, *supra* note 39; *Microsoft Privacy Statement*, *supra* note 74.

79. *Google Privacy Policy*, *supra* note 39; *Microsoft Privacy Statement*, *supra* note 74.

80. *Amazon.ca Privacy Notice*, *supra* note 38; *Dropbox Privacy Policy*, *supra* note 34; *Google Privacy Policy*, *supra* note 39; *Microsoft Privacy Statement*, *supra* note 74.

81. *Amazon.ca Privacy Notice*, *supra* note 38; *Dropbox Privacy Policy*, *supra* note 34; *Google Privacy Policy*, *supra* note 39; *Microsoft Privacy Statement*, *supra* note 74.

82. *Dropbox Privacy Policy*, *supra* note 34; *Microsoft Privacy Statement*, *supra* note 74.

83. *Google Privacy Policy*, *supra* note 39; *Microsoft Privacy Statement*, *supra* note 74.

or enforcing their terms of service agreements.[84] It is noteworthy, however, that both Google[85] and Microsoft[86] specify that their disclosure of user data to comply with the law will be limited exclusively to *enforceable* government requests, thus maintaining that they will not voluntarily divulge the private information of their users.[87] In contrast, iCloud's privacy policy appears to be the least respectful of its users' data and is significantly more broad in that it allows access, use, disclosure, or preservation of the data of its users for purposes of law, national security, legal process, litigation, protection of property rights, fraud prevention or detection, to conform with a government request, or "other issues of public importance."[88]

Moreover, while none of these CSPs satisfy the third requirement of forensic readiness by accounting for the laws and procedures of the jurisdictions in which their data centers are located, four of them, excluding Dropbox, satisfy the last criterion by highlighting the way they will enforce and police their terms of service agreements. Several enforcement measures are outlined, including: the suspension or closing of an account,[89] the removal of user content or the refusal to publish it in the first place,[90] the discontinuance of the service, and the blocking of communications emanating from the user's account.[91] The iCloud is, however, the only service provider that does not specify the actions that it will take in response to a violation of its terms but rather simply includes yet another permissive clause, stating that it "reserves the right to take steps [it] believes are reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement."[92] Although the delineation of enforcement measures would thus qualify all four of these service providers as forensically ready, iCloud's term to this effect is by far the least favorable to user privacy.[93] While the other CSPs specify precisely which actions they will take, actions that could all be

---

84. *Amazon.ca Privacy Notice*, *supra* note 38; *Google Privacy Policy*, *supra* note 39; *Apple Privacy Policy*, *supra* note 75.

85. *Google Privacy Policy*, *supra* note 39.

86. *Microsoft Privacy Statement*, *supra* note 74.

87. This position is an important aspect of ensuring that the privacy of cloud users is protected, as will be discussed in more detail in the next Section.

88. *Apple Privacy Policy*, *supra* note 75.

89. *Conditions of Use*, *supra* note 59; *Microsoft Services Agreement*, *supra* note 59; *Google Terms of Service*, *supra* note 58.

90. *Microsoft Services Agreement*, *supra* note 59; *Google Terms of Service*, *supra* note 58.

91. *Microsoft Services Agreement*, *supra* note 59.

92. *iCloud Terms and Conditions*, *supra* note 59.

93. *See id.*

reasonable in the event of a violation of their terms, iCloud users are at the entity's mercy, essentially uninformed as to the measures that could be taken against them.

While only fulfilling two of the four criteria for forensic readiness, the above analysis demonstrates that the five CSPs in question convey relative openness toward assisting law enforcement in the pursuit of criminal investigations against any users who conduct themselves unlawfully or unacceptably. However, while the forensic readiness of the services of CSPs as exuded by their terms and policies does illustrate an increase in the investigatory powers of law enforcement, it does not necessarily preclude privacy protection. Essentially, it is not only the content of these documents that determines the extent to which these entities respect the privacy of their users, but it is also the practices that they adopt in reality. While the above analysis suggests that iCloud is the most forensically ready, and perhaps the least respectful of user privacy, a yearly report published by the Electronic Frontier Foundation[94] demonstrates that iCloud's adherence to industry-accepted best practices[95] actually provides a rather expansive protection to the privacy of its users.[96] Dropbox[97] was placed at the same level as the iCloud to this effect, but neither Amazon,[98] OneDrive,[99] or Google[100] were promoted to this rank, despite the fact that some of the clauses in their terms of service agreements and privacy policies did seem, on their face, to be largely respectful of user privacy, as outlined in the above analysis.

---

94. Cardozo et al., *supra* note 14, at 25-27.

95. *Id.* at 8. The Electronic Frontier Foundation, in its yearly report, outlined five criteria on which the level of protection afforded to user privacy by Internet-based companies can be measured, particularly based on whether: (1) they adhere to industry-accepted best practices, such as whether they require a warrant prior to providing law enforcement with access to user information, whether they publish a transparency report outlining the number of times user data was requested by law enforcement as well as how often the company complied with these demands, and whether the company publishes law enforcement guidelines explaining the manner in which they approach law enforcement data requests; (2) they notify their users that a government request has been made for their data *prior* to the company complying with that demand; (3) they publicly disclose their policies regarding their retention of user data in a format that is not accessible by the user but may still be accessible to law enforcement; (4) they disclose how often law enforcement makes either formal or informal demands that user content be removed or that an account be suspended, and how often these requests are complied with by the company; and (5) they adopt pro-user policies by opposing backdoors, which are "the compelled inclusion of deliberate security weaknesses or other compelled back doors" that make it easier for the government and law enforcement to access user information, but, in essence, that violates user privacy. *Id.* at 5-7.

96. *Id.* at 18-19.

97. *Id.* at 25-26.

98. *Id.* at 16-17.

99. *Id.* at 33-34.

100. *Id.* at 29-30.

III. CLOUD FORENSIC TECHNIQUES AND THEIR INCIDENTAL VIOLATION OF THE PRIVACY OF INNOCENT USERS

The term "cloud forensics" was first introduced in 2011 "to recognize the rapidly emerging need for digital investigation[s]" in the cloud—a need resulting from the increasing use of this environment for criminal purposes.[101] This recognition was quickly followed by another one: that the existing digital forensic techniques[102] were not adequate to apply to investigations performed in the public cloud.[103] This inadequacy is due to the fact that using these traditional techniques to identify and collect[104] data relating to criminal investigations in the cloud would render it impossible to protect the privacy of legitimate cloud users.[105] Despite this realization, little has been done to rectify this deficiency. As such, the cloud forensic tools currently being utilized in the process of criminal investigations within cloud environments essentially violate the privacy of legitimate users in a host of different ways.[106]

First, the identification of evidence generally commences through a forensic analysis of the electronic devices of the suspect, devices such as computers or mobile phones.[107] This analysis results in the detection of digital artifacts or remnants.[108] As discussed above, each public CSP

---

101. Keyun Ruan et al., *Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: An Overview of Survey Results*, 10 DIGITAL INVESTIGATION 34, 34 (2013).

102. *See* RODNEY MCKEMMISH, AUSTL. INST. OF CRIMINOLOGY, WHAT IS FORENSIC COMPUTING? 1 (Trends & Issues in Criminal Justice No. 118, June 1999), http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf.

103. *See* BARRETT & KIPPER, *supra* note 52, at 197-209; Ben Martini & Kim-Kwang Raymond Choo, *An Integrated Conceptual Digital Forensic Framework for Cloud Computing*, 9 DIGITAL INVESTIGATION 71, 75 (2012) [hereinafter Martini & Choo, *Integrated Conceptual Forensic Framework*]; Simson L. Garfinkel, *Digital Forensics Research: The Next 10 Years*, 7 DIGITAL INVESTIGATION S64, S67 (2010); Almulla et al., *supra* note 57, at 18.

104. *See* Martini & Choo, *Integrated Conceptual Forensic Framework*, *supra* note 103, at 75.

105. NIST Cloud Forensic Challenges, *supra* note 5, at 26.

106. *See* BARRETT & KIPPER, *supra* note 52, at 197-209; *see* Martini & Choo, *Integrated Conceptual Forensic Framework*, *supra* note 103, at 75; Garfinkel, *supra* note 103, at S67; Almulla et al., *supra* note 57, at 18.

107. *See* Robert Beverly et al., *Forensic Carving of Network Packets and Associated Data Structures*, 8 DIGITAL INVESTIGATION S78, S78 (2011). Although this can also be achieved through searching for artifacts within cloud servers, both the difficulty in locating them and the repercussions that would be experienced should servers be constantly shut down to aid in criminal investigations, make this difficult. *See* D. Reilly et al., Cloud Computing: Forensic Challenges for Law Enforcement 1, 7 (Nov. 2010) (conference paper, 2010 International Conference for Internet Technology and Secured Transactions) (on file with IEEE).

108. DARREN QUICK ET AL., CLOUD STORAGE FORENSICS 16 (2014); Keyun Ruan & Joe Carthy, *Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis*, *in* DIGITAL FORENSICS AND CYBER CRIME: 4TH INTERNATIONAL CONFERENCE—SELECTED REVISED PAPERS 1, 9 (Marcus Rogers & Kathryn C. Seigfried-Spellar eds., 2013).

leaves behind artifacts on devices that are unique to its own service.[109] Armed with these remnants, as well as the knowledge of the identity of the CSP, this information is then used to locate the suspect's cloud data.[110]

This process' implications for the privacy of innocent users is that the artifacts found do not always lead directly to the information of the person under investigation. Although artifacts sometimes lead to the discovery of usernames and passwords, which *may* render the immediate identification of the suspect's data more likely, the reality is that the accounts of innocent cloud users are often assumed by malicious users to perpetuate their criminal activities.[111] As such, when these trails of artifacts are followed, they frequently lead to the accounts of legitimate users who are victims themselves.[112]

Often, however, the only artifacts found relate to file names. If those files have been deleted by the person under investigation, which is a distinct probability if the CSP notifies the user that their cloud data has been sought by law enforcement,[113] this information may lead to a portion of cloud server space that has already been occupied by an innocent user's data as a result of the constant re-provisioning of cloud resources.[114] Due to the fact that deleted data still remains in the cloud for a certain period of time, law enforcement will likely have to sift through some of the other data contained in that shared environment to find the evidence they seek,[115] thus violating the privacy of innocent cloud users. The potential of such privacy violations is further exacerbated in cloud

---

109. Although, if the service provider cannot immediately be determined through these artifacts, CSPs can be identified by law enforcement using domain or IP addresses. QUICK ET AL., *supra* note 108, at 16.

110. Ben Martini et al., *Cloud Computing and Digital Forensics*, *in* INFORMATION SOCIETY AND CYBERCRIME: CHALLENGES FOR CRIMINOLOGY AND CRIMINAL JUSTICE 119 (Asian Regional Conference, 2013).

111. KIM-KWANG RAYMOND CHOO, AUSTL. INST. OF CRIMINOLOGY, CLOUD COMPUTING: CHALLENGES AND FUTURE DIRECTIONS 1, 3 (Trends & Issues in Crime & Criminal Justice No. 400, Oct. 2010), http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi400.pdf.

112. *Id.*

113. This practice is increasingly being adopted by CSPs to ensure transparency. *See* Cardozo et al., *supra* note 14, at 9.

114. Fred Cohen, *Challenges to Digital Forensic Evidence in the Cloud*, *in* CYBERCRIME AND CLOUD FORENSICS: APPLICATIONS FOR INVESTIGATION PROCESSES 65-66 (Keyun Ruan ed., 2013); Gertruida Meyer & Adrie Stander, Cloud Computing: The Digital Forensics Challenge 294-95 (2015) (conference paper, Proceedings of Informing Science & IT Education Conference 2015) (on file with Informing Science Institute), http://proceedings.informingscience.org/InSITE2015/InSITE15p285-299Meyer1562.pdf.

115. Ivan Orton et al., *Legal Process and Requirements for Cloud Forensic Investigations*, *in* CYBERCRIME AND CLOUD FORENSICS: APPLICATIONS FOR INVESTIGATION PROCESSES 186, 226 n.4 (Keyun Ruan ed., 2013); Farid Daryabar et al., *A Survey About Impacts of Cloud Computing on Digital Forensics*, 2 INT'L J. CYBER-SECURITY & DIGITAL FORENSICS 77, 86-87 (2013).

services that utilize de-duplication processes, as any file name can lead to cloud data that belongs to more than one user, making it difficult to determine the information's origin.[116]

However, even aside from the potential of malicious users or the inability to directly determine whether a particular piece of data emanated from a suspect, up to 20% of data in commercial cloud databases does not accurately reflect the individual from whom that information emanated.[117] When it comes to identifying cloud data, it is important to realize that just because the computer data appears to indicate a piece of information emanates from a specific person, it is not always a reflection of reality.[118] Therefore, following a trail of artifacts may sometimes lead to an entirely innocent person.

Seizing evidence in the cloud, on the other hand, is accompanied by its own host of privacy concerns. Seizure of cloud data can be achieved with or without the cooperation of CSPs. When a CSP cooperates, the privacy implications are less significant as the CSP will only access data that is already available to it and share it with law enforcement, while preventing a law enforcement agency itself from performing the search in the shared environment of the public cloud. This approach avoids the risk of law enforcement agents incidentally accessing the data of innocent users.[119]

When evidence is seized in the cloud without the cooperation of CSPs, on the other hand, law enforcement has two options. It could seize the servers of a CSP, allowing unfettered access to all the data contained in these servers. Using this method could pose serious risks with regard to the business continuity of entities that rely on the cloud service for their daily affairs, in addition to the CSP itself being the subject of negative publicity.[120] The other possibility is to use remote cloud forensic techniques that implicate an offsite general access to the cloud servers at issue. Remote access can be achieved by either installing traditional digital forensic software within the infrastructure of the cloud server where the suspicious data resides or by intercepting cloud

---

116. Meyer & Stander, *supra* note 114, at 292; Sean Thorpe, *An Experimental Survey Towards Engaging Trustable Hypervisor Log Evidence Within a Cloud Forensic Environment*, 4 INT'L J. COMPUTER SCI. & INFO. TECH. 125, 126 (2012).

117. *See* Cohen, *supra* note 114, at 63.

118. *See id.*

119. *See* Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 92 (2006).

120. Cindy Cohn & Julie Samuels, *Megaupload and the Government's Attack on Cloud Computing*, ELECTRONIC FRONTIER FOUND. (Oct. 31, 2012), https://www.eff.org/deeplinks/2012/10/governments-attack-cloud-computing.

communications. If the first method is used, this software will often capture information of innocent users whose data is stored alongside the individual under criminal investigation[121] because traditional forensic software is not adapted[122] to shared public cloud environments where there is no segregation between the data of various users.[123] If the second method is used, it is often difficult to isolate a single cloud communication due to the constant re-provisioning of cloud storage space.[124] As such, they risk intercepting the cloud signals emitted by the devices of innocent cloud users.

Despite that, as it now stands, digital forensic technology is not able to respond to the unique nature of the public cloud in a manner that adequately addresses the right to privacy of innocent cloud users, these techniques continue to be used by law enforcement. The next Part is dedicated to determining whether Canadian and U.S. law provide sufficient legal protections to ensure that such privacy violations occur as infrequently as possible in these digital environments.

IV. THE INVESTIGATORY POWERS OF LAW ENFORCEMENT: CONSTITUTIONAL AND STATUTORY LIMITATIONS VS. LEGAL LOOPHOLES AND EXTENSIONS

The extent to which the privacy of both Canadian and U.S. innocent cloud users will be respected during the use of cloud forensics during criminal investigations depends entirely upon the scope of powers accorded to law enforcement in these countries. The laws circumscribing these investigatory powers generally outline the obligation of law enforcement officers to respect the privacy of the suspect rather than addressing the privacy of innocent individuals. The way these laws are applied to investigations performed in the cloud, however, will inevitably affect the privacy of innocent cloud users because the suspect's data is not segregated.[125] This Part will describe both the limitations and extensions of the investigatory powers of law enforcement in Canada and

---

121. *See* Corrado Federici, *Cloud Data Imager: A Unified Answer to Remote Acquisition of Cloud Storage Areas*, 11 DIGITAL INVESTIGATION 30, 30 (2014); Josiah Dykstra & Alan T. Sherman, *Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques*, 9 DIGITAL INVESTIGATION S90, S90 (2012); Cohen, *supra* note 114, at 63; Thorpe, *supra* note 116, at 133.

122. Thorpe, *supra* note 116, at 126.

123. *See* Shahrzad Zargari & David Benford, *Cloud Forensics: Concepts, Issues, and Challenges*, *in* 2012 THIRD INT'L CONFERENCE ON EMERGING INTELLIGENT DATA AND WEB TECHNOLOGY 237 (2012); Almulla et al., *supra* note 57, at 12.

124. Ruan et al., *Cloud Forensics*, *supra* note 5, at 21-22.

125. *Id.* at 22; NIST Cloud Forensic Challenges, *supra* note 5, at 26.

the United States and how those powers may affect the privacy of innocent cloud users.

A. Limitations on Law Enforcement's Investigatory Powers

The limitations on the investigatory powers of law enforcement come in two forms, namely constitutional protections and statutory protections. The next two Sections will delineate these types of protections, which are available to both Canadian and U.S. citizens. This will be achieved by outlining how these protections would apply to the cloud, considering the particularities of the digital environment, as well as how these limitations might be extended to ensure the protection of the private data of innocent cloud users.

1. Constitutional Protections Against the Warrantless Search and Seizure of Digital Information

Both Canadian and U.S. laws provide constitutional protections against warrantless searches and seizures. Section 8 of the Canadian Charter of Rights and Freedoms provides that "everyone has the right to be secure against unreasonable search or seizure."[126] The Fourth Amendment of the U.S. Constitution, on the other hand, holds that:

> the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[127]

With the pervasiveness of new digital environments and the commission of crimes in these arenas, one of the most significant debates surrounds whether these constitutional protections could be extended to safeguard both Canadian and U.S. citizens from warrantless searches and seizures in cyberspace.[128]

As an initial point, it is significant that both countries' constitutional provisions effectively protect *all* U.S. and Canadian citizens from

---

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

127. U.S. CONST. art. IV.

128. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-64 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 212 (2006); Steven Penney, *The Digitization of Section 8 of the Charter: Reform or Revolution?*, 67 SUP. CT. L. REV. 505, 517 (2014); David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2206 (2009).

unreasonable searches and seizures. Whereas searching the data of a legitimate suspect of a criminal investigation may be considered reasonable, performing a similar search of the information of an innocent person may not qualify as such because there is no reasonable suspicion based on which to be accessing this person's data. When it comes to searches performed in cloud environments, however, one might question if the same conclusion would be reached where the data of an innocent person is inadvertently being accessed as a direct result of a legitimate cloud search that is crucial to the success of an investigation. It may not be practical to consider the privacy of innocent cloud users as paramount relative to their protection from criminals. While this debate is a significant one, and necessary to discuss, if only briefly, its intricacies extend well beyond the scope of this Article. The aim of this Article is rather to examine whether the data of innocent cloud users is effectively being protected by both Canadian and U.S. law through an in-depth analysis of the pervasiveness of warrantless searches and seizures performed in digital environments in each jurisdiction.

In the United States, the courts are divided on whether the personal information of individuals entrusted to an Internet Service Provider (ISP) or CSP enjoys constitutional protections, with many claiming that it has fallen through the gaps in Fourth Amendment protection.[129] The seminal Supreme Court case *Katz v. United States*[130] maintained that: "an individual enjoys a reasonable expectation of privacy if his conduct reflects 'an actual (subjective) expectation of privacy,' meaning an expectation that society would consider reasonable."[131] This reasonable expectation of privacy is, however, subject to the caveat that the Fourth Amendment's protection of data is lost when an individual entrusts his information to another[132]—a principle known as the "Third Party Doctrine."[133]

---

129. *See* Kerr, *Searches and Seizures*, *supra* note 2, at 568; Brenner & Frederiksen, *supra* note 2, at 40; Solove, *supra* note 2, at 1084; Winick, *supra* note 2, at 76; Lessig, *supra* note 2, at 1231; Kerr, *Fourth Amendment and Internet*, *supra* note 2, at 1006.

130. 389 U.S. 347 (1967).

131. *Id.* at 361 (Harlan, J., concurring).

132. *Id.* at 351 (majority opinion).

133. Elizabeth S. Gaffin, Friending Brandeis: Privacy and Government Surveillance in the Era of Social Media 10 (June 2012) (unpublished M.A. dissertation, Naval Postgraduate School) (on file with Dudley Knox Library, Naval Postgraduate School). The "Third Party Doctrine" was even further concretized by the decisions of the Supreme Court in *United States v. Miller*, where they maintained that, by entrusting ones banking records to a bank, one lost the protection of the Fourth amendment, and *Smith v. Maryland*, where it was held that using a pen register to record the phone numbers dialed from the residence of the defendant was not a search under the Fourth Amendment noting that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"; the same was held for telephone records. United States v.

While this doctrine has not precluded Fourth Amendment protection of information contained in the personal digital devices of individuals,[134] the extent of the constitutional protection afforded to personal data that is stored remotely, such as online or in the cloud, is questionable.[135] Subscriber information held by ISPs and obtained without a warrant has often been accessed by local, state, and federal officers in a significant amount of cases over the past ten years, and constitutional or statutory law has been unsuccessful to suppress use of this information.[136] Furthermore, due to the lack of certainty surrounding the extent of constitutional protection afforded to this data, its use is likely more extensive than is reflected by reported cases. This potential disparity occurs because the use of data obtained in such a manner is generally not challenged in criminal trials, either because it is not directly introduced as evidence, but is rather only used to obtain warrants to legally obtain other forms of evidence, or because it falls under an exclusionary rule of a relevant statute.[137]

Miller, 425 U.S. 435, 443-44 (1976); Smith v. Maryland, 442 U.S. 735, 744-45 (1979); *see also* United States v. White, 401 U.S. 745, 753 (1971) (no expectation of privacy when communication with a police informant who is wired); Couch v. United States, 409 U.S. 322, 336 (1973) (no expectation of privacy in business and tax records).

134. *See*, *e.g.*, Riley v. California, 134 S. Ct. 2473, 2479 (2014) (a cellular telephone held on the body of the detained cannot be searched incident to an arrest but rather requires a warrant to do so); United States v. Crist, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008) (removing a computer's hard drive and copying the data it contains is a Fourth Amendment search even if the copying did not involve a physical invasion); Trulock v. Freeh, 275 F.3d 391, 402, 403 (4th Cir. 2001) (digital files stored locally on an individual's hard drive enjoy Fourth Amendment protection).

135. *See* SLOBOGIN, *supra* note 128, at 151-64; Brenner & Clarke, *supra* note 128, at 212; Penney, *supra* note 128, at 517; Couillard, *supra* note 128, at 2206.

136. *See*, *e.g.*, Rehberg v. Paulk, 598 F.3d 1268, 1282 (11th Cir. 2010), *vacated and superseded on rehearing*, 611 F.3d 828 (11th Cir. 2010); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008); United States v. Perrine, 518 F.3d 1196, 1199 (10th Cir. 2008); United States v. Meeks, 290 F. App'x 896, 900 (6th Cir. 2008); United States v. Fuller, 77 F. App'x 371, 376 (6th Cir. 2003); United States v. Simons, 206 F.3d 392, 398-99 (4th Cir. 2000); *In re* United States, 534 F. Supp. 2d 585, 586 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010); *In re* United States, 665 F. Supp. 2d 1210, 1212 (D. Or. 2009); United States v. Ogden, No. 06-20033-STA, 2008 WL 4982756, at *3 (W.D. Tenn. Nov. 18, 2008); United States v. D'Andrea, 497 F. Supp. 2d 117, 123 (D. Mass. 2007); United States v. Jones, 364 F. Supp. 2d 1303, 1307 (D. Utah 2005); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Aldahondo, No. CRIM 03-0107(DRD), 2004 WL 170252, at *2 (D.P.R. Jan. 15, 2004); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002); United States v. Kennedy, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000); Washington v. Townsend, 57 P.3d 255, 265 (Wash. 2002) (en banc) (Sanders, J., dissenting); Hause v. Kentucky, 83 S.W.3d 1, 12 (Ky. Ct. App. 2001); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 589 (2011).

137. Tokson, *supra* note 136, at 589 n.45.

However, recent case law has demonstrated a slight shift in the approach of U.S. courts to the application of the Third Party Doctrine in modern digital environments. It has been implied that a claim to privacy may be available to an individual who places their data online if certain measures are taken to protect that information.[138] To this effect, the case of *United States v. D'Andrea* provides an intriguing analysis that is often cited due to its novelty in the digital context, despite that this decision emanates from a lower court with no binding authority. In this case, the United States District Court for Massachusetts analogized a password-protected website to a closed container,[139] which has generally received Fourth Amendment Protection.[140] However, the Court neglected to specify what steps an individual must take towards concealing such information in order for it to enjoy a reasonable expectation of privacy.[141] This case therefore "[has] limited predictive value"[142] to the public cloud context because, as discussed in the first section of this Article, documents stored in this environment are not always encrypted and those that are encrypted are usually done so by the CSP, who generally retains the encryption keys.[143]

In holding that government employees possess a reasonable expectation of privacy in the content of their text messages, however, the United States Court of Appeals for the Ninth Circuit's ruling in *Quon v. Arch Wireless Operating Co.* analogized this type of communication to an e-mail.[144] Furthermore, the Ninth Circuit held that "the fact that the service provider *could have* accessed the message contents for its own purposes was not enough to destroy the users' reasonable expectations of privacy in those contents."[145] While the Ninth Circuit's decision in this case was reversed by the Supreme Court,[146] the latter's decision was based on the fact that the search was reasonable, even if a reasonable expectation of privacy did exist, though they declined to rule on this aspect of the case.

---

138. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002), *vacated*, 90 Fed. App'x 3 (1st Cir. 2004); *see also* Bond v. United States, 529 U.S. 334, 338-39 (2000); United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005).

139. *D'Andrea*, 497 F. Supp. 2d at 122 n.16.

140. *See*, *e.g.*, *Bond*, 529 U.S. at 338-39; United States v. Bosby, 675 F.2d 1174, 1180 (11th Cir. 1982) ("Absent exigent circumstances, closed containers such as a briefcase or pieces of personal luggage even if unlocked cannot be searched absent a warrant.").

141. *D'Andrea*, 497 F. Supp. 2d at 122-23.

142. *Id.* at 122-23; Couillard, *supra* note 128, at 2210 n.35.

143. Couillard, *supra* note 128, at 2223-27.

144. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905-06 (9th Cir. 2008).

145. Couillard, *supra* note 128, at 2230.

146. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629-22 (2010).

> [However, the Supreme Court's] failure to dismiss the claim out of hand on the basis of the [T]hird [P]arty [D]octrine suggests that, in the long run, the Supreme Court is likely to hold that the mere fact of digital intermediation does not remove all reasonable expectation of privacy, at least in some important social contexts.[147]

To this effect, the United States Sixth Circuit Court of Appeals in *Warshak v. United States*[148] held that minimal access to content by an intermediary does not immediately preclude its Fourth Amendment protection. While this decision may implicitly recognize the protection of data stored by CSPs, as e-mails are generally stored in the cloud, the fact that information often reaches the cloud in readable form and is encrypted by the CSP itself may render it difficult to consider access to this data as "minimal."[149]

More recently, however, the application of the Third Party Doctrine to more modern digital concepts was expressly questioned by Justice Sotomayor in the Supreme Court case of *United States v. Jones*, where she notes that:

> People disclose the phone numbers that they dial or text to their cellular providers, the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers [. . .] But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public *for a limited purpose* is, for that reason alone, disentitled to Fourth Amendment protection.[150]

Sotomayor's perspective implies that, although the secrecy of cloud data relies upon the CSP encrypting this information, it may not be barred from a reasonable expectation of privacy. However, it remains unclear as to whether entrusting one's data to a CSP for remote storage could be considered a "limited purpose." While U.S. courts appear to be moving away from the application of the Third Party Doctrine to more modern technological concepts involving the entrustment of personal information, the possibility of extending this approach to cloud environments remains uncertain.

---

147. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 604, 618 (2011).

148. Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007) (en banc).

149. Couillard, *supra* note 128, at 2230 n.179.

150. United States v. Jones, 132 S. Ct. 945, 957 (2012) (emphasis added).

On the other hand, the Canadian discourse on the subject has approached this issue from a decidedly different perspective, though it is by no means more respectful of individual privacy than the United States' approach. While the Supreme Court of Canada has rejected the application of the Third Party Doctrine,[151] recently confirming that its stance on the matter is unaltered as it pertains to digital environments,[152] Canadian courts have adopted another method to circumvent the need for a warrant in digital environments. They have, in effect, often relied on the disclosure clauses of terms of service agreements that permit service providers to share subscriber information with law enforcement for the purpose of criminal investigations.[153] Although the data stored on personal digital devices has been recognized by Canadian courts on numerous occasions as enjoying a reasonable expectation of privacy,[154] the existence of these types of clauses in all standard service agreements imposed upon public cloud users by CSPs may affect the constitutional protection afforded to such remote storage services.

Two Supreme Court of Canada decisions that adopt this stance may, however, imply that the particular nature of the cloud precludes the possibility of relying on such clauses to deny individuals of section 8 protection. In *R. v. Plant*,[155] the Supreme Court of Canada held that the inclusion of such disclosure clauses in the agreement governing the relationship between the parties may prevent a reasonable expectation of

---

151. R. v. Dyment, [1988] 2 S.C.R. 417, 429-32 (Can.); R. v. Colarusso, [1994] 1 S.C.R. 20, 43 (Can.); R. v. O'Connor, [1995] 4 S.C.R. 411, 414 (Can.); Lavallee, Rackel & Heintz v. Canada, 2000 ABCA 54, paras. 73-74 (Can.); White, Ottenheimer & Baker v. Canada, 2000 NFCA 36, para. 7 (Can.); R. v. Fink, [2002] 3 S.C.R. 209, 213-14 (Can.); R. v. Dersch, [1993] 3 S.C.R. 768, 769 (Can.).

152. *See* R. v. Telus Communications, [2013] 2 S.C.R. 3, para. 53 (Can.).

153. *See*, *e.g.*, R. v. Ward, 2012 ONCA 660, para. 76 (Can. Ont. C.A.); R. v. Trapp, 2011 SKCA 143, para. 128 (Can.); R. v. Spencer, 2011 SKCA 144, para. 33 (Can.); R. v. Kwok, 2008 CarswellOnt 2634 (Can. Ont. C.J.) (WL); R. v. Friers, 2008 ONCJ 740, para. 21 (Can. Ont. C.J.); R. v. S.W.F., 2009 ONCJ 103, para. 4 n.1 (Can. Ont. C.J.); R. v. Verge, 2009 CarswellOnt 501, paras. 23-34 (Can. Ont. C.J.) (WL); R. v. Vasic, 2009 CarswellOnt 846, para. 54 (Can. Ont. S.C.J.) (WL); R. v. Cuttell, 2009 ONCJ 471, paras. 28-33 (Can. Ont. C.J.); R. v. Wilson, 2009 CarswellOnt 2064, paras. 43-44 (Can. Ont. S.C.J.) (WL); R. v. McNeice, 2010 BCSC 1544, paras. 43-44 (Can. B.C.); R. v. Brosseau, 2010 ONSC 6753, paras. 25-30 (Can. Ont. S.C.J.); R. v. Ballendine, 2011 BCCA 221, para. 78 (Can. B.C. C.A.).

154. *See* R. v. Cole, [2012] 3 S.C.R. 34, paras. 57-58 (Can.) (recognizing reasonable expectation of privacy in computer supplied by employer); R. v. Morelli, [2010] 1 S.C.R. 253, paras. 105-06 (Can.) (requiring a warrant for the search of a computer); R. v. Vu, [2013] 3 S.C.R. 657, para. 49 (Can.) (an additional warrant must be obtained to search a computer located on the premises for which the first warrant was obtained); R. v. Fearon, [2014] 3 S.C.R. 621, para. 83 (Can.) (while recognizing that searches of cell phones incident to arrest is necessary, they imposed certain limits on the ability of law enforcement to do so).

155. R. v. Plant, [1993] 3 S.C.R. 281 (Can.).

privacy from existing. However, it does note that if the records in question contain:

> personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state . . . [such as] information which tends to reveal intimate details of the lifestyle and personal choices of the [individual], the commercial nature of the relationship between the parties will not necessarily foreclose a s. 8 claim.[156]

Seeing as the cloud is a platform where individuals store intimate details about their lives such as e-mails, chats, photos, and videos, it is difficult to envision how the commercial relationship that prevented the application of section 8 in *R. v. Plant* could be used to achieve the same purpose in the context of the cloud.

In contrast, in the case of *R. v. Gomboc*,[157] the Supreme Court of Canada rejected the existence of a reasonable expectation of privacy in the defendant's consumption of electric power, which would have otherwise existed. This decision was based on the agreement governing the defendant's relation with the utility company that permitted this information's disclosure to law enforcement and considered that the defendant *had the opportunity to request that this clause not apply to him*.[158] When it comes to the terms of service agreements governing the relationships of public cloud users and CSPs, however, there is no opportunity to opt out of these clauses.[159] The Court's reasoning in this case is unlikely to extend to allowing the divulgence of a user's cloud data by merely turning to the agreement between the individual user and the CSP.

More recently, the Supreme Court of Canada's decision in *R. v. Spencer* rejected the permissibility of warrantless requests to ISPs for subscriber data because this data relates to "specifically observed, anonymous Internet activity [that] engages a high level of informational privacy."[160] This reasoning could extend to data stored in the cloud as it similarly affects the informational privacy of cloud users.

---

156. *Id.* at 293-94.

157. R. v. Gomboc, [2010] 3 S.C.R. 211 (Can.).

158. *Id.* at 235; Johnson, *supra* note 2, at 482.

159. The imposition of such standard form contracts has been rejected in the civil context. *See* Tilden Rent-a-Car Co. v. Clendenning (1978), 18 O.R. 2d 601, para. 32 (Can. Ont. C.A.); Interfoto Picture Library Ltd. v. Stiletto Visual Programmes Ltd. [1987] EWCA (Civ) 6, [1989] 1 Q.B. 433 [438]-[439] (Eng.); Matthew Nied, *Cloud Computing, the Internet, and the* Charter *Right to Privacy: The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy*, 69 ADVOC. VANCOUVER 701, 704 (2011).

160. R. v. Spencer, [2014] 2 S.C.R. 212, para. 51 (Can.).

However, although this decision may seem promising in its recognition of a reasonable expectation of privacy for subscriber information, it has not altered the Royal Canadian Mounted Police's (RCMP) practice of making warrantless requests for user data,[161] nor has it altered courts relying on terms of service agreements to admit this information as evidence.[162] Additionally, the application of *R. v. Spencer* to the protection of subscriber data has been seriously limited by inferior courts.[163] Although some courts apply *R. v. Spencer* in a manner that protects user privacy,[164] several courts either distinguished these cases from the Supreme Court's decision on various levels[165] or refused to exclude the evidence, reasoning that it would bring the administration of justice into disrepute, despite the finding of a section 8 Charter breach pursuant to *R. v. Spencer*.[166] Even more concerning is that one of these decisions concludes that no reasonable expectation of privacy exists in subscriber information but neglects to refer to *R. v. Spencer* altogether.[167] Furthermore, the *R. v. Spencer* decision is at risk of failing to have its desired effects in light of the recently passed Protecting Canadians from

---

161. Paul McLeod & Alex Boutilier, *Cops Still Ask Telecoms for Info Without Warrants Despite Court Ruling*, CHRONICLE HERALD (Sept. 17, 2014, 6:00 AM), http://thechronicleherald.ca/canada/1236873-cops-still-ask-telecoms-for-info-without-warrants-despite-court-ruling.

162. R. v. Graff, 2015 ABQB 415, paras. 77-78 (Can. Alta. Q.B.).

163. The search terms "subscriber information" AND "reasonable expectation of privacy" yielded sixty-nine results on CanLII.org. Sorting the result by "most recent" revealed that twenty-seven decisions on this subject had been decided following the Supreme Court's decision in *R. v. Spencer*. *See* R. v. Spencer, 2011 SKCA 144 (Can.). Each of these decisions was reviewed.

164. *See* R. v. Pelucco, 2015 BCCA 370, para. 71 (Can. B.C. C.A.) (maintains a reasonable expectation of privacy in a text message in the recipient's cellular telephone); R. v. Mills, 2015 NLPC 0112A01710, par. 22 (Can. N.L.R.) (maintains a reasonable expectation of privacy in IP addresses and online activity).

165. *See* R. v. Caza, 2015 BCCA 374, para. 32 (Can. B.C. C.A.) (the defendant was not considered to enjoy a reasonable expectation of privacy for his subscriber information as he used the account of his former roommate without consent); H.M.Q. v. TELUS Communications Co., 2015 ONSC 3964, paras. 29-31 (Can. Ont. S.C.J.) (maintaining that there is no reasonable expectation of privacy in the name and address associated with a cellular phone number as *Spencer* did not directly reverse the authorities to this effect); R. v. Ho, 2015 ONCJ 118, para. 28 (Can. Ont. C.J.); R. v. Khan 2014 ONSC 5664, para. 27 (Can. Ont. S.C.J.); R. v. Morrison, 2014 ONCJ 774, para. 25 (Can. Ont. C.J.) (maintaining that no reasonable expectation of privacy exists for cell phone subscriber information); R. v. Belcourt, 2015 BCCA 126, para. 55 (Can. B.C. C.A.) (maintaining that no reasonable expectation of privacy exists in historical text messages retained by telecommunications providers, ultimately allowing this information to be produced to law enforcement based on a mere production order rather than a warrant).

166. R. v. Capancioni, 2015 ONSC 7696, para. 38 (Can. Ont. S.C.J.); *Graff*, 2015 ABQB at para. 87.

167. R. v. Nurse & Plummer, 2014 ONSC 6004, para. 47 (Can. Ont. S.C.J.).

Online Crimes Act,[168] as will be discussed in further detail in the next Section.[169]

As illustrated, the positions of both U.S. and Canadian law on the constitutional protection of digital privacy are not entirely settled. Although U.S courts appear to be slowly but surely moving towards the protection of such data, it is not yet a foregone conclusion this data enjoys Fourth Amendment protection.[170] In Canada, on the other hand, while the Supreme Court of Canada has attempted to provide a wider berth of protection to the private digital information of its citizens, it has had very little practical effect on the inferior courts' and the RCMP's treatment of such data.[171]

Although the reasonable expectation of privacy of the *criminal suspect* is the main issue at hand in both the Canadian and U.S. cases regarding the constitutionality of searches and seizures performed in digital environments, two conclusions can be drawn from these decisions as they pertain to the privacy protection of innocent cloud users. Foremost, while it may be difficult to maintain that accessing data of an innocent cloud user as a necessary corollary to a legitimate search is unreasonable, as discussed above, the same cannot be said where the judiciary holds that digital investigations violate a suspect's reasonable expectation of privacy. In such cases, it stands to reason that the data of any innocent cloud user that was inadvertently accessed incident to an unreasonable search of a suspect's data would also be deemed unreasonable.

Additionally, where such searches are performed without a warrant, there is absolutely no judicial oversight to ensure that the repercussions of incidentally accessing cloud data of an innocent user in pursuit of a suspect's data (innocent users' data is not segregated from the contentious data) are reasonable and proportionate to the sought result.[172] As such, innocent cloud users are deprived of minimal privacy protection that may

---

168. Protecting Canadians from Online Crimes Act, S.C. 2014, c 31 (Can.).

169. GEIST, *supra* note 2, at 2.

170. *See* Couillard, *supra* note 128, at 2206.

171. McLeod & Boutilier, *supra* note 161; *Graff*, 2015 ABQB at paras. 77-78; R. v. Pelucco, 2015 BCCA 370, para. 71 (Can. B.C. C.A.); R. v. Mills, 2015 NLPC 0112A01710, par. 22 (Can. N.L.R.); R. v. Caza, 2015 BCCA 374, para. 32 (Can. B.C. C.A.); R. v. Khan 2014 ONSC 5664, para. 27 (Can. Ont. S.C.J.); H.M.Q. v. TELUS Communications Company, 2015 ONSC 3964, paras. 29-31 (Can. Ont. S.C.J.); R. v. Ho, 2015 ONCJ 118, para. 28 (Can. Ont. C.J.); R. v. Morrison, 2014 ONCJ 774, para. 25 (Can. Ont. C.J.); R. v. Belcourt, 2015 BCCA 126, para. 55 (Can. B.C. C.A.).

172. Michael Geist, *The Privacy Threats in Bill C-13, Part One: Immunity for Personal Info Disclosures Without a Warrant*, MICHAEL GEIST BLOG (Nov. 25, 2013), http://www.michaelgeist.ca/2013/11/c-13-privacy-threat-part-one/ [hereinafter Geist, *Part One*].

be afforded to their cloud data according to law enforcement officers' obligation to obtain warrants to search and seize a suspect's digital data.

2. Statutory Protections Against Warrantless Searches of Private Information and Their Extension to the Cloud

In addition to the constitutional protection of private information, both the United States and Canada possess statutory protections to this effect. For its part, the United States offers statutory protection in the form of the Electronic Communications Privacy Act (ECPA),[173] which provides a private right of action for most violations.[174] However, while possessing no obvious loopholes allowing government surveillance, "the ECPA's overall scheme of protection is weak and riddled with gaps and exceptions,"[175] which renders it nearly inapplicable towards the protection of much modern digital content,[176] such as cloud data.

For example, both e-mail and the Internet are not covered by the portion of this Act known as the Stored Electronic Communications Act (SCA).[177] The SCA was enacted in the 1980s and governs access to stored electronic data,[178] thus allowing the government to access e-mails and browsing histories without any statutory limitation.[179] Additionally, any data that this Act classifies as non-content, which does not "concern . . . the substance, purport, or meaning of [a] communication,"[180] is only marginally protected.[181] As long as certification is provided to the court to the effect that such non-content

---

173. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2012) [hereinafter ECPA].

174. *See id.* § 2520(a); Stored Communications Act § 2707(a), 18 U.S.C. 121 § 2701 (2012) [hereinafter SCA].

175. Tokson, *supra* note 136, at 592.

176. *Id.* at 589; Dera J. Nevin & Marc Jenkins, *Information, Knowledge, and the Pursuit of Privacy*, 38 AM. J. TRIAL ADVOC. 485, 513-14 (2015).

177. SCA § 2701.

178. *Id.*; Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail,* 2008 U. CHI. LEGAL F. 121, 123 (2008).

179. COMPUT. CRIME & INTELLECTUAL PROP. SEC. CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125-26, 128 (Office of Legal Education Litigation Series, 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [hereinafter DOJ, OBTAINING ELECTRONIC EVIDENCE]; Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1424 (2004) [hereinafter Bellia, *Cyberlaw's Lens*].

180. ECPA, 18 U.S.C. § 2510(8) (2012).

181. *See* Ilana R. Kattan, *Cloudy Privacy Protections: Why the Stored Communications Act Fails To Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 641 (2011); William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1207-09 (2010).

information is relevant to an ongoing investigation, real time government interception of this data, such as Internet Protocol address (IP) and e-mail addresses, is permissible.[182] While this provision might seem to provide some level of judicial review,[183] courts fail to inquire into the legitimacy of a certification.[184] This form of surveillance therefore falls short of judicial scrutiny.[185]

Although the ECPA does offer a stronger protection to the actual content of communications,[186] it still possesses several loopholes. For example, while law enforcement must obtain a warrant for e-mails that have been in electronic storage for fewer than 180 days,[187] they are entitled to dispense with this formality if they have been stored there for over 180 days and can access this data with a mere administrative or grand jury subpoena.[188] Even the 180-day rule is not set in stone, as the Department of Justice has interpreted the term "electronic storage" as applying only to e-mails that are in the process of being *transmitted*. As such, the servers of an individual's e-mail provider may be accessed through a subpoena as soon as an e-mail is opened by a user while it remains in their inbox, rather than having to wait 181 days after it has been sent to gain access.[189] Following this logic, law enforcement would have access to cloud data under the ECPA through a simple subpoena, regardless of the personal nature or the length of time for which it has been stored.[190] Although courts are still divided on the issue,[191] this argument is sufficiently plausible to permit law enforcement to access

182. 18 U.S.C. § 3123(a)(1)-(2) (2012).

183. Though, it must be noted that the constitutionality of this low threshold has been challenged with respect to the application of this law to modern technologies. *See generally* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

184. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 62 (2004).

185. Tokson, *supra* note 136, at 594.

186. *Id.* at 594.

187. SCA § 2703, 18 U.S.C. § 2701 (2012).

188. *Id.* §§ 2703(a), (b)(1)(B)(i). Note, however, that a bill has been tabled in Congress, the "Secure Data Act" that would remove this section from the ECPA, though it has not yet been passed. *See* Secure Data Act of 2015, S. 135, 114th Cong. (2015).

189. DOJ, OBTAINING ELECTRONIC EVIDENCE, *supra* note 179, at 128; Bellia, *Cyberlaw's Lens*, *supra* note 179, at 1419.

190. *See* SCA § 2703(b).

191. *See*, *e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008); Bansal v. Russ, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) *vacated in part*, *aff'd in part*, 352 F.3d 107 (3d Cir. 2004); Tokson, *supra* note 136, at 594.

opened e-mails in most jurisdictions that have not yet taken a stance on this issue.[192]

Rather than providing any true protection to the electronic communications of U.S. citizens, the ECPA serves to enable the performance of a significant number of warrantless searches and seizures in cloud environments. In addition to negating any reasonable expectation of privacy that criminal suspects might have of their information, the data of innocent cloud users will also inevitably be accessed with absolutely no judicial oversight to temper any nefarious effects that may result from such searches.[193]

Despite the lack of actual protections offered to digital data by the ECPA, several U.S. states' laws require warrants to access digital content as well as to utilize GPS location tracking.[194] The most comprehensive of these laws is enacted by the state of California. The California Electronic Communications Privacy Act (CalECPA),[195] signed into law on October 8, 2015, serves to protect location data, content, metadata, device searches, and basically any other digital data that would be considered

---

192. *See*, *e.g.*, Warshak v. United States, 631 F.3d 266 (6th Cir. 2010). The case in question, while maintaining that the acquisition of the e-mail content of the accused by compelling his ISP violated his Fourth Amendment rights, allowed the admissibility of this evidence under the SCA portion of the ECPA. *Id.* at 282-83. A case decided by the United States Court of Appeals for the Sixth Circuit instigated two proposed amendments to the ECPA, which were introduced in 2015 and would require a warrant for the search and seizure of the content of communications, in addition to abolishing the 180-day distinction, and would force law enforcement to acquire a warrant prior to requesting the personal data of a subscriber of a remote computing service, such as a CSP, or an electronic communication service. *See* Electronic Communications Privacy Act Amendments Act of 2015, H.R. 283, 114th Cong. (2015); Email Privacy Act, H.R. 699, 114th Cong. (2015); Mark Jaycox, *Seventy Public Interest Organizations and Companies Urge Congress To Update Email Privacy Law*, ELECTRONIC FRONTIER FOUND. (Jan. 23, 2015), https://www.eff.org/deeplinks/2015/01/more-x-public-interest-organizations-and-companies-urge-congress-update-email. In a similar vein, the *Law Enforcement Access to Data Stored Abroad Act*, which would also amend the ECPA, was introduced to force law enforcement to obtain a warrant prior to compelling the disclosure of subscriber data by a provider of electronic communication services or remote computing services, such as a CSP. Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015). If passed, these laws could add significantly more protections to digital data, especially information hosted by CSPs, than is currently offered on a federal level in the United States. As they are not yet enacted, however, they cannot presently contribute to the protection offered by the United States to digital data.

193. Tokson, *supra* note 136, at 592; Nevin & Jenkins, *supra* note 176, at 513-14.

194. Cyrus Farivar, *Cops Must Now Get a Warrant To Use Stingrays in Washington State*, ARSTECHNICA.COM (May 12, 2015, 8:49 PM), http://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/; VA. CODE ANN. § 19.3-70.3 (2016); MINN. STAT. § 626A.28 (2016); UTAH ANN. CODE §§ 77-23c-101, 77-23c-102, 77-23c-103 (LexisNexis 2016).

195. Electronic Communications Privacy Act, CAL. PENAL CODE §§ 1546.1-1546.4 (West 2017) [hereinafter CalECPA].

private by an average citizen, such as e-mails, text messages, and documents stored in the cloud.[196]

CalECPA prohibits law enforcement from compelling the production of an individual's metadata or digital communications without a warrant or court order.[197] A warrant will only be issued where the data to be seized is described with specificity. Additionally, the warrant must impose restrictions on law enforcement's manner of using the data once it is obtained, such as requiring that it be destroyed within the ninety days[198] following its seizure.[199] Moreover, direct physical or electronic access to information stored on an electronic device, such as a cell phone or wireless hard drive, is limited under this Act.[200] Finally, the target of a search must be contemporaneously notified of the request for data as well as be informed of the nature of the government's investigation. There is, however, a possibility for authorization delaying this notice to ensure that the target does not delete the data and render it entirely inaccessible to law enforcement.[201] While this Act is also subject to the exigent circumstances exception, as will be discussed in further detail below, the possibility of delaying notification to the suspect could prevent this exception from being used for the performance of warrantless seizures in the cloud and other digital environments.

While this Act offers significant protection for digital data, it only extends to citizens of California and does not go so far as to apply to federal law enforcement authorities. As such, if a resident of California is being investigated by the Federal Bureau of Investigation, for example, the person in question does not enjoy the protections afforded by this Act.[202] Despite this limitation to its application, this Act still serves to impose a certain level of proportionality between the searches performed

---

196. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/; Debra Cassens Weiss, *California Law Requiring Warrant for Digital Searches Is 'A Landmark Win For Digital Privacy*,' ABA J. (Oct. 9, 2015, 9:17 AM), http://www.abajournal.com/news/article/california_law_requiring_warrant_for_digital_searches_is_a_landmark_win_for; Adam Waks, *California Gives the Fourth Amendment a 21st Century Makeover,* PROSKAUER: PRIVACY L. BLOG (Nov. 10, 2015), http://privacylaw.proskauer.com/2015/11/articles/fourth-amendment/california-gives-the-fourth-amendment-a-21st-century-makeover/.

197. CalECPA § 1546.1(a)(1).

198. Note that this delay could be renewed.

199. CalECPA § 1546.1(1)(g) (though this delay could be renewed, as seen in section 1546.1(1)(g)(2)).

200. CalECPA § 1546.1(1)(3).

201. *Id.* § 1546.2(1)(b).

202. Laura Hautala, *New California Law Requires Police To Get Warrants for Online Data*, CNET (Oct. 8, 2015, 6:00 PM), http://www.cnet.com/news/new-california-law-requires-police-to-get-warrants-for-online-data/.

in digital environments and the results sought by law enforcement. Additionally, by requiring warrants for the search and seizure of the digital content of criminal suspects, this Act is offering a certain protection to the information of innocent cloud users by preventing the occurrence of unreasonable searches and seizures, and thus avoiding as much unreasonable incidental access of users' cloud data as possible.

Similarly to the ECPA, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) seeks to provide additional protections to the electronic data of Canadian citizens.[203] Section 7(3)(c.1) of this Act governs the disclosure of subscriber information by online service providers. This section permits a service provider "to disclose personal information without the knowledge or consent of the individual" in response to a government request based on "lawful authority"[204]—which courts often interpret as a lesser threshold than a warrant requirement[205]—*unless* the data is subject to a reasonable expectation of privacy, then prior judicial authorization must be sought.[206]

Although, as discussed above, the Supreme Court of Canada maintains that subscriber data enjoys a reasonable expectation of privacy,[207] its position has been counteracted by the recently adopted legislation on lawful access. This legislation allows for the disclosure of certain subscriber information and could pose serious privacy concerns, as will be discussed in more detail in the following Section. Additionally, it has been maintained that:

---

203. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5, art. 7 (Can.).

204. While there are three provinces, namely British Columbia, Alberta, and Quebec, in which the PIPEDA does not apply as they possess substantially similar legislation thus precluding its application, their provisions regarding the disclosure of personal information without consent to law enforcement does not provide any additional protections to user privacy than the PIPEDA and will not be discussed in the present. *See Overview of Privacy Legislation in Canada*, OFF. PRIVACY COMMISSIONER CAN. (May 2014), priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp; Personal Information Protection Act, S.B.C. 2003, c 63, arts. 18(1)(c), (i)-(j), (o) (Can. B.C.); Personal Information Protection Act, S.A. 2003, c P-6.5, arts. 20(e)-(f) (Can. Alta.); Act Respecting the Protection of Personal Information in the Private Sector, C.Q.L.R. 2016, c P-39.1, § 2 (Can.).

205. Some courts have maintained that simply commencing an investigation endowed police officers with "lawful authority." *See* R. v. Wilson, 2009 CarswellOnt 2064, paras. 43-44 (Can. Ont. S.C.J.) (WL); R. v. Verge, 2009 CarswellOnt 501, paras. 23-34 (Can. Ont. C.J.) (WL); R. v. Kwok, 2008 CasrwellOnt 2634, paras. 31-32 (Can. Ont. C.J.) (WL); R. v. Brosseau, 2010 ONSC 6753, para. 43 (Can. Ont. S.C.J.); R v. Croft, 2013 ABQB 665, para. 45 (Can. Alta. Q.B.); *cf.* Re S.C., 2006 ONCJ 343, paras. 9, 11 (Can. Ont. C.J.) (where the opposite conclusion was reached); *see also* Nied, *supra* note 159, at 701.

206. R. v. Cuttell, 2009 ONCJ 471, paras. 45, 48 (Can. Ont. C.J.); R. v. Ward, 2012 ONCA 660, para. 57 (Can. Ont. C.A.); *Kwok*, 2008 CarswellOnt at paras. 31-32; R. v. Trapp, 2011 SKCA 143, para. 11 (Can.).

207. R. v. Spencer, 2011 SKCA 144, para. 66 (Can.).

> [T]he fact that the *PIPEDA* imposes limits on the use and disclosure of personal information by private enterprises [does not necessarily result] in an extension of constitutional protection to all such information in the absence of clear language to that effect. The reasonable expectation of privacy required for constitutional protection remains to be determined on the totality of the circumstances.[208]

Canadian law enforcement has, however, often circumvented the obligation to obtain a warrant by merely requesting subscriber information from service providers. The pervasiveness of such warrantless requests was brought to light in April 2014, when University of Ottawa's Faculty of Law professor Michael Geist revealed that government agencies made 1.2 million data requests to nine of Canada's major telecommunications providers and social media sites in the year 2011 alone.[209] Only three of these providers kept track of the number of demands that were compiled among them, assessing disclosed user data in a total of 784,756 cases.[210] When asked to provide additional transparency regarding the number of requests it made for user data, the RCMP was unable to offer any information as it did not keep any records of this data.[211]

Professor Geist's inquiry also led to the startling discovery that two of the providers questioned use Deep Packet Inspection, a technology used to examine all user communications being transmitted through a network[212] in response to law enforcement requests. The use of Deep Packet Inspection technology is a seriously invasive practice that could provide significant amounts of user information that a subscriber would reasonably expect to be private.[213] As discussed above, despite the Supreme Court's decision in *R. v. Spencer*, the permissibility of using

---

208. R. v Chehill, 2009 NSCA 85, para. 23 (Can. N.S. C.A.); R. v Devloo, 2015 ABQB 345, para. 190 (Can. Alta. Q.B.) (citing R. v Chehill, 2009 NSCA 85, para. 23 (Can. N.S. C.A.)).

209. Michael Geist, *Canadian Telcos Asked To Disclose Subscriber Data Every 27 Seconds*, MICHAELGEIST.CA (Apr. 30, 2014), http://www.michaelgeist.ca/2014/04/telco-disclosures/.

210. Letter from Karen E. Hennessey, Gauling Lafleur Henderson LLP, to Jennifer Stoddard, Office of the Privacy Comm'r of Can. (Dec. 14, 2011) (on file with recipient), https://www.priv.gc.ca/media/1103/let_gowling_e.pdf.

211. OFFICE OF THE PRIVACY COMM'R OF CAN., ANNUAL REPORT TO PARLIAMENT 2013-2014: TRANSPARENCY AND PRIVACY IN THE DIGITAL AGE 20 (2014), https://www.priv.gc.ca/media/1672/201314_pa_e.pdf [hereinafter PRIVACY COMM'R ANNUAL REPORT 2013-2014].

212. *See* Christopher Parsons, *Literature Review of Deep Packet Inspection: Prepared for the New Transparency Project's Cyber-Surveillance Workshop* (Mar. 6, 2011) (unpublished manuscript), https://www.christopher-parsons.com/Main/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf.

213. *See* SARIT K. MIZRAHI, THE LEGAL IMPLICATIONS OF INTERNET MARKETING: EXPLOITING THE DIGITAL MARKETPLACE WITHIN THE BOUNDARIES OF THE LAW 19-24, 97-99 (2015).

this data in court is often based on a standard form contract governing the relationship between the parties. Furthermore, the *R. v. Spencer* decision risks having even less of a positive effect considering the recently passed Protecting Canadians from Online Crimes Act,[214] as will be discussed in further detail in the next Section.[215]

Both the Canadian and U.S. statutory protections intended to protect citizens from privacy invasions resulting from warrantless searches and seizures therefore present risks to the innocent users of modern digital technology, particularly the cloud, apart from a few U.S. states' laws that encompass more comprehensive legislation to this effect. Essentially, the statutes in both jurisdictions meant to protect the digital data of Internet and cloud users, whether users are suspects of a crime or entirely innocent, have seemingly very little practical effect in achieving this purpose. Not only are the statutes riddled with loopholes that are often taken advantage of by law enforcement, but whatever firm protections *are* offered by these statutes tend to be circumvented by law enforcement agents. By not respecting the limitations on their investigatory powers imposed by the obligation to obtain a warrant, law enforcement can easily access the data of both criminal suspects and entirely innocent cloud users who have done nothing to merit this form of surveillance. The judicial oversight provided by the warrant system is crucial, not only to protect the reasonable expectation of privacy of people under investigation, but also to protect that of unsuspecting citizens.

B. Statutory Extensions of Law Enforcement's Investigatory Powers and Their Effects on Legitimate Cloud Users

Both U.S. and Canadian law, as they currently stand, extend investigatory powers of law enforcement in a manner that could pose serious privacy risks for legitimate cloud users by allowing the police to access digital data containing the personal information of individuals. To begin, both countries possess an exception permitting the warrantless search and seizure of data for exigent circumstances, in addition to possessing legislation that obligates service providers to assist law enforcement in investigations *without* a warrant. Moreover, law enforcement officers are endowed with certain cross-jurisdictional powers, which affect cloud users worldwide as there is no segregation between their data and the data sought by these agencies.

---

214. Protecting Canadians from Online Crime Act, S.C. 2014, c 31 (Can.).

215. GEIST, *supra* note 2, at 2.

1. Exigent Circumstances, Preservation Orders, and What This Means for Cloud Users

While both Canadian and U.S. case law alike appear to provide some constitutional protection to the digital data of their citizens, as discussed above, it is questionable whether these protections could be extended to cloud environments. Essentially, there are several exceptions in the laws of both jurisdictions to the warrant requirement, the most relevant being that of "exigent circumstances." Section 487.11 of the Criminal Code of Canada states that law enforcement may perform warrantless searches[216] where reasonable and probable grounds exist such that "there is an imminent danger of the loss, removal, destruction or disappearance of the evidence if the search or seizure is delayed."[217] A similar exception exists throughout U.S. criminal law where there is probable cause to believe that the warrantless search and seizure of evidence is necessary to prevent the destruction of relevant evidence.[218]

In view of the nature of the cloud, however, exigent circumstances will *always* exist by these standards because the potential for the destruction of relevant evidence is heightened in this environment. This risk is due mainly to the new transparency policies of many CSPs to notify their subscribers if a request has been made for their data by law enforcement *prior* to the CSP's acquiescence to the demand, as outlined above. This prior notification gives the user under investigation the opportunity to delete all traces of contentious data.[219] In order to avoid providing this opportunity, all searches and seizures performed in the cloud may be warrantless, thus ultimately negating any minimal protection that might be afforded to the expectation of privacy of innocent cloud users whose data will incidentally be accessed throughout the cloud investigation.

Recent amendments to the Canadian Criminal Code, however, provide law enforcement with the "power to make preservation demands

---

216. Canada Criminal Code, R.S.C. 1985, c C-46, art. 487.11 (Can.).

217. R. v. Grant, [1993] S.C.R. 223, 224 (Can.). Within the digital context, it has been held that police may seize a computer to preserve the evidence, as long as a warrant is later acquired to actually search the computer's files, if there is a chance that the suspect would be notified that the police are investigating him and delete the data. *See*, *e.g.*, R. v. Seguin, 2015 ONSC 1908, paras. 39-40 (Can. Ont. S.C.J.); R. v. Winchester, 2010 ONSC 652, paras. 47-52 (Can. Ont. S.C.J.).

218. United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984); United States v. Martinez, 406 F.3d 1160, 1164 (9th Cir. 2005).

219. Josiah Dykstra, *Seizing Electronic Evidence from Cloud Computing Environments*, *in* CYBERCRIME AND CLOUD FORENSICS: APPLICATIONS FOR INVESTIGATION PROCESSES 162 (Keyun Ruan ed., 2013).

and orders to compel the preservation of electronic evidence."[220] While the United States' SCA also permits requests of this effect to be made,[221] the Canadian Criminal Code provisions go one step further by also allowing demands to delay notice of the court orders or administrative subpoenas to the target.[222]

Although it is arguable as to how much these measures actually protect privacy, as user data will still be accessed by service providers without any judicial oversight, they could effectively prevent warrantless searches and seizures in this environment. Essentially, by turning to service providers to preserve the data of the criminal alone, law enforcement agents will not have to perform cloud searches themselves and will therefore avoid inadvertently violating the privacy of innocent cloud users. As such, these types of provisions may be a good option to protect the cloud data of these individuals while allowing law enforcement sufficient flexibility to perform investigations. This approach further ensures that the constitutional rights of both Canadian and U.S. cloud users are ultimately respected because they can aid in preventing warrantless searches and seizures in this environment.

2. The Obligation Imposed Upon Service Providers To Assist Law Enforcement

The positive effects of the Supreme Court of Canada's decision upholding the protection of digital privacy in *R. v. Spencer*, which maintained that a reasonable expectation of privacy exists for subscriber data, were short-lived if they existed at all.[223] Not long after this decision was rendered, the government adopted Bill C-13,[224] known as the Protecting Canadians from Online Crimes Act, that entirely negates the Court's holding in this case.[225]

At the behest of Canadian law enforcement agencies' increasing difficulty to investigate crimes occurring in digital environments, Parliament has attempted to adopt laws that provide law enforcement

220. Canada Criminal Code, R.S.C. 1985, c C-46, arts. 487.012-487.013 (Can.).

221. SCA § 2703(f), 18 U.S.C. 121 § 2701 (2012).

222. *Id.* § 2705.

223. GEIST, *supra* note 2, at 2.

224. Julia Nicol & Dominique Valiquet, Bill C-13: An Act To Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act, Parliament of Canada 1 (Aug. 28, 2014) (Library of Parliament Legislative Summaries, Pub. No. 41-2-C13-E) (Can.), http://www.lop.parl.gc.ca/Content/LOP/Legislative Summaries/41/2/c13-e.pdf.

225. Josh Wingrove, *Cyberbullying Bill C-13 Moves on Despite Supreme Court Decision*, GLOBE & MAIL (Oct. 2, 2014), http://www.theglobeandmail.com/news/politics/cyberbullying-bill-c-13-moves-on-despite-supreme-court-decision/article20885941/.

with warrantless access to subscriber data for over a decade.[226] Since 2005, eight proposals for lawful access were introduced by the Canadian government, each met with fierce opposition by privacy advocates.[227] Bill C-13 is the version of this Bill that was ultimately enforced. Its adoption is claimed to address the pressing issue of cyberbullying in the wake of the tragic deaths of Rehtaeh Parsons and Amanda Todd, who both committed suicide after being bullied online.[228] The government capitalized on these tragedies to include sections of the Act that pertain very little to cyberbullying, thus shrouding this Bill in a great deal of controversy.[229] While only very briefly addressing the issue of cyberbullying,[230] the government took advantage of this opportunity to significantly extend the powers of law enforcement in the course of criminal investigations taking place in digital environments, thus considerably eroding user privacy.

Although this legislation does provide a certain protection to the privacy of cloud data by prohibiting law enforcement from accessing this information themselves, any protection this Act may offer is negated by the provision of immunity for criminal or civil liability to entities that voluntarily provide personal data of their subscribers to law enforcement.[231] Although the Canadian Criminal Code already possesses a provision permitting the voluntary disclosure of information to law enforcement officers for the purpose of "enforcing or administering this or any other Act of Parliament,"[232] Bill C-13 does not limit the nature of these requests, but rather permits any basis for this voluntary

---

226. PRIVACY COMM'R ANNUAL REPORT 2013-2014, *supra* note 211, at 17; Christopher Parsons, *Stuck on the Agenda: Drawing Lessons from the Stagnation of "Lawful Access" Legislation in Canada*, *in* GEIST, *supra* note 2.

227. Evan Dyer, *Cyberbullying Bill Draws Fire from Diverse Mix of Critics*, CBC NEWS (Oct. 20, 2014, 6:48 AM), http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637.

228. Nicol & Valiquet, *supra* note 224, at 2; *Communications Assistance for Law Enforcement Act*, FED. COMM. COMMISSION, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance (last visited Apr. 4, 2017).

229. 147 HOUSE OF COMMONS DEB. 1465, 1513 (2013) (Can.); 149 DEBS. OF SENATE 2409, 2417-18 (2014) (Can.); Kathryn Blaze Baum, *Bullying Victims' Families Split Over Crime Bill*, GLOBE & MAIL (May 13, 2014), http://www.theglobeandmail.com/news/politics/bullying-victims-families-split-over-crime-bill/article18653112/; Dyer, *supra* note 227.

230. Sunny Handa et al., *Bill C-13: Cyberbullying Bill Introduces New Lawful Access Measures*, BLAKES (Jan. 23, 2015), http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057.

231. Canada Criminal Code, R.S.C. 1985, c C-46, art. 487.0195(2) (Can.); Geist, *Part One*, *supra* note 172.

232. Canada Criminal Code, R.S.C. 1985, c C-46, art. 487.014 (Can.).

disclosure.[233] This provision thus "represents significant legal protection for intermediaries that is likely to lead to increased disclosures without court oversight."[234] Thereby, this provision exponentially increases the ease with which the private data of innocent cloud users may be rendered accessible to law enforcement, as service providers do not need a reasonable cause for supplying it. As such, they can provide law enforcement with access to the data of *any* of their subscribers, whether it be in pursuit of a criminal investigation or not, and they are entirely exempt from liability regardless of how unreasonable provision of this information may be.

In addition to permitting such voluntary disclosures, Bill C-13 also reduces the threshold that law enforcement must satisfy to obtain a warrant to search and seize transmission data, which includes metadata.[235] All that must be demonstrated is that there are reasonable grounds to *suspect* that the commission of an offense either has occurred or is imminent, and that the identification of a device or person associated with the transmission data will either aid the pursuit of the investigation or aid the identification of a person.[236] Although:

> [the] government would like Canadians to believe that invoking the existence of court oversight is enough to address the privacy concerns in Bill C-13 . . . with the privacy significance of metadata and the low threshold established by the proposed transmission data warrant, the bill's lawful access provisions are the source of genuine privacy concerns.[237]

Applying the standard of reasonable grounds of suspicion in such situations does not go far enough towards protecting the privacy of Canadian citizens, considering the deference to their protection that is generally provided in situations where a high privacy interest is implicated.[238] This standard only requires a *possibility* of criminal behavior, as opposed to a *probability* in its "reasonable grounds" counterpart.[239] The imposition of such a low threshold for the search and seizure of metadata could negatively affect innocent cloud users by

---

233. *Id.* art. 487.0195(1); Geist, *Part One*, *supra* note 172.

234. Geist, *Part One*, *supra* note 172.

235. Michael Geist, *The Privacy Threats in Bill C-13, Part Two: The Low Threshold for Metadata*, MICHAEL GEIST BLOG (Dec. 11, 2013), http://www.michaelgeist.ca/2013/12/c-13-metadata/ [hereinafter Geist, *Part Two*].

236. *Id.*

237. *Id.*; *see also* R. v. Vu, [2013] 3 S.C.R. 657, paras. 41-42 (Can.); Michael Geist, *Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era*, *in* GEIST, *supra* note 2 [hereinafter Geist, *Post-Snowden*]; Kerr, *Searches and Seizures*, *supra* note 2, at 542-43.

238. R. v. Chehil, 2013 SCC 49, para. 25 (Can.).

239. Geist, *Part Two, supra* note 235.

essentially expanding the number of searches permitted in the cloud, ultimately increasing the number of innocent users whose privacy will be incidentally breached as a result.

Like Canada, the United States enacted an exception to the ECPA in the form of the *Communications Assistance for Law Enforcement Act* (CALEA),[240] in an effort to aid law enforcement in light of technological hurdles experienced in the course of investigations.[241] The United States' approach to these obstacles are, however, decidedly different. The Canadian legislation achieved this purpose by reducing the threshold that must be achieved by law enforcement to obtain a warrant for digital environments, as well as by providing immunity to service providers who voluntarily share subscriber data with law enforcement. Conversely, the United States accomplishes this feat by forcing telecommunications companies to introduce known vulnerabilities, or backdoors, into their systems that allow law enforcement to wiretap the communications of an individual pursuant to a court order or other lawful authorization.[242]

When first enacted in 1994, this Act applied only to telephone companies, forcing them to redesign their networks' architecture so that law enforcement could more easily wiretap digital phone calls. It was, however, expanded in 2005 to extend to ISPs and Voice Over IP services such as Skype.[243] In order to comply with CALEA, entities providing these types of services are required to allow the government to: (1) isolate the content of the targeted communication; (2) isolate all "call identifying information"; (3) have the provider transfer all such information to law enforcement in a timely manner; and (4) conduct these interceptions without either notifying the target or invading the privacy of other users.[244]

Although there is strong emphasis on CALEA's lack of application to information services such as the storage functions of e-mail, Web hosting, or domain name lookup services,[245] it remains unclear how wiretapping communications emitted through an ISP's services could avoid capturing their content.[246] Due to the fact that CSPs are "engaged

240. 47 U.S.C. § 1001-10 (2012).

241. *Communications Assistance for Law Enforcement Act*, *supra* note 228.

242. Communications Assistance for Law Enforcement Act §§ 1001-10, 47 U.S.C. § 1001 (2012) [hereinafter CALEA].

243. *CALEA*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/calea (last visited Apr. 4, 2017).

244. CALEA § 1002.

245. The validity of this extension has been upheld in *American Council on Education v. FCC*, 451 F.3d 226 (D.C. Cir. 2006).

246. *FAQ on the CALEA Expansion by the FCC*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/calea-faq#2 (last visited Apr. 4, 2017).

in providing information services," they are not considered a telecommunications carrier under CALEA and, thus, need not adhere to this law.[247]

The application of CALEA to modern technologies like the cloud has been a challenge for the government and a victory for privacy advocates, because the law was designed to allow the interception of communications based on the technology of the telephone, which was the principal means of communication at the time the law was enacted. Canada's lawful access legislation, on the other hand, was enacted to respond specifically to modern technologies.[248] While it was not difficult to support the reasons to extend CALEA's application to ISPs and Voice Over IP providers, as they provide similar communications services to a certain extent, it would be difficult to extend this reasoning to cloud environments.[249]

This complication does not mean, however, that the data of cloud users is not available to U.S. law enforcement agencies. Rather, the Third Party Doctrine previously mentioned still provides comprehensive access to this information by allowing law enforcement to compel service providers to disclose this data. Additionally, law enforcement can still access the data of cloud users because it is stored in the cloud by using the services of an ISP, which are subject to CALEA-based wiretaps.[250] As such, CALEA will have certain implications for the privacy of cloud users, despite that CALEA-based wiretaps cannot be imposed directly in the cloud.

With the possibility of using CALEA to indirectly amass cloud data in this manner, the introduction of known vulnerabilities into ISP services can pose a significant risk to the private data of innocent cloud users. While law enforcement will be less likely to incidentally access the data of innocent cloud users since they will not be searching directly within the cloud, but rather intercepting a specific ISP transmission, the introduction of such backdoors renders the private data of *all* Internet users vulnerable to attacks from other online threats such as hackers.[251] Essentially, just as law enforcement can take advantage of these known vulnerabilities to gain access to the private data of individuals, so can

---

247. CALEA § 1001.

248. Handa et al., *supra* note 230.

249. Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government To Seek Access to the Cloud*, 2 INT'L DATA PRIVACY L. 200, 201 (2012).

250. *Id.*

251. Roberto J. Mejias, *An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk*, *in* PROCEEDINGS OF THE 45TH INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES 3258, 3260 (Ralph H. Sprague, Jr. ed., 2012).

anyone else. The private data of both suspicious and innocent cloud users alike is at risk of being accessed by such unscrupulous threats, even if not accessed directly in the cloud, posing a serious risk to privacy.

3. Acquiring Cloud Data Across Jurisdictional Borders

Both the Internet and the cloud increasingly blur jurisdictional lines, rendering it possible for someone to commit a crime in one jurisdiction while being physically located in another.[252] When such a cross-jurisdictional crime occurs, it becomes necessary for law enforcement to seek information relating to criminal investigations outside its jurisdiction. In order to ensure that such cross-jurisdictional searches performed between Canada and the United States do not violate the privacy of their citizens, these countries entered into Mutual Legal Assistance Agreements.[253] While still used,[254] this course of action is not favored by law enforcement in cybercrime investigations because it entails certain lengthy processes that prevent acquiring evidence in a timely manner, a crucial aspect of any investigation involving data residing on the Internet or in the cloud.[255]

Although Canadian and U.S law enforcement officers can make informal requests to one another for assistance with an investigation involving data residing in their counterpart's jurisdictions, these requests are often accompanied by a host of evidence admissibility issues.[256] As a result, officers generally tend to turn to two other options. The first option is to request that the service provider hosting the data voluntarily disclose that information to foreign law enforcement pursuant to its terms of service agreements with its subscribers.[257] The second possibility is to obtain a warrant from a judge within the law enforcement agency's jurisdiction to perform a "computer search," which significantly increases the scope of private information available to local law enforcement. The first option is riddled with the same privacy

252. *See*, *e.g.*, Bellia, *Chasing Bits*, *supra* note 1, at 39.

253. Mutual Legal Assistance in Criminal Matters Act, 1985 c 30 (Can.).

254. *See*, *e.g.*, United States v. Fafalios, 2012 ONCA 365, para. 10 (Can. Ont. C.A.); R. v. Faflios, 2010 ONSC 1994, para. 21 (Can. Ont. S.C.J.).

255. Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, *in* PRIVACY AND SECURITY FOR CLOUD COMPUTING 56 (Siana Pearson & George Yee eds., 2013) (ebook).

256. *See* Bellia, *Chasing Bits*, *supra* note 1, at 38-39; Susan W. Brenner, *Law, Dissonance, and Remote Computer Searches*, 14 N.C. J.L. & TECH. 43, 52-54 (2012); Anna-Maria Osula, *Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data*, 9 MASARYK U. J.L. & TECH. 43, 44-45 (2015).

257. Walden, *supra* note 255, at 58, 62-63.

implications discussed above, so this discussion will be limited to the second route.

Essentially, both Canadian and U.S. law permit their justices to issue search warrants for data that is accessible through a computer but is not necessarily located within their respective jurisdictions. The Canadian Criminal Code states that, upon judicial authorization, a person may use "any computer system . . . to search any data contained in or available to the computer system."[258] This provision has been interpreted by Canadian courts on several occasions to permit the remote seizure of digital data across jurisdictional lines,[259] stating that "in this day and age, with the development of computer technology and the so called "information highway," information exists where it is capable of being accessed, translated and recorded."[260] The Federal Court of Appeal maintained this position, holding that:

> with the click of a mouse, the appellants make the information appear on the screens on their desks in Toronto and Vancouver, or anywhere else in Canada. It is as easily accessible as documents in their filing cabinets in their Canadian offices. Hence, it makes no sense in my view to insist that information stored on servers outside Canada is as a matter of law located outside Canada.[261]

Under U.S. law, the situation is not so neatly delineated, as legislation is largely state-based, and the states tend to be divided on the matter, though most permit remote searches and seizures of computer data.[262] To this effect, in the recent case of *In re Warrant To Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, a magistrate judge in the Southern District of New York maintained that U.S. companies could be compelled to produce information stored in servers located outside the United States' borders by virtue of a warrant issued by national authorities.[263] Microsoft, however, appealed this decision to the United States Court of Appeals for the Second Circuit, which subsequently reversed the decision.[264]

---

258. Canada Criminal Code, R.S.C. 1985, c C-46, art. 487(2.1) (Can.).

259. *See* Casey W. Halladay & Joshua Chad, *A Database Too Far? Interpreting the Competition Bureau's Computer Search Powers*, 27 CAN. COMPETITION L. REV. 453, 457-58 (2014).

260. R. v. Edwards, 1999 CarswellOnt 3233, paras. 89-90 (Can. Ont. Sup. Ct. J.) (WL).

261. eBay Canada Ltd. v. M.N.R., 2008 FCA 348, para. 48 (Can.).

262. *See* Brenner, *supra* note 256, at 52-54.

263. *In re* Warrant To Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014).

264. Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016); Recent Cases, *Privacy Law—Stored Communications Act—District Court Holds that SCA Warrant Obligates U.S. Provider To Produce Emails Stored on Foreign Servers*—In re Warrant to Search a Certain

The controversy surrounding this case triggered an immediate response from Congress. Not wishing for the decision of the Second Circuit Court of Appeals to limit its jurisdictional reach, Congress introduced the Law Enforcement Access to Data Stored Abroad Act.[265] If passed, this Act would allow a warrant issued within the United States to compel the disclosure of electronic storage regardless of where this data is located as long as the target of the search is a U.S. citizen.[266] By only allowing law enforcement to request that service providers disclose information relevant to their investigations about their citizens (similar to the preservation orders discussed above), this approach is an interesting one, as it is much less invasive of privacy than permitting remote searches that render the cloud data of all users accessible to law enforcement.

While this solution might be more respectful of the privacy of other individuals whose data may be stored in shared environments, unfortunately it was never adopted. Rather, the route taken consists of an amendment to Rule 41 of the Federal Rules of Criminal Procedure, which recently came into force. These amendments allow magistrate judges to issue warrants permitting remote searches and seizures of technological information, regardless of whether it is located within their district, when there have been tools employed to purposefully conceal the location of the data in question.[267]

In this respect, both U.S. and Canadian law increase the scope of individuals whose data is accessible to law enforcement. While this heightened access may be reasonable where those individuals are citizens of one of these countries and store their data abroad attempting to avoid detection by local law enforcement agencies, the same logic cannot be applied when the private data being accessed belongs to innocent individuals or citizens of other countries altogether. Therefore, the approach taken in the United States remains less invasive than that of Canada because, rather than enabling remote searches and seizures of

---

Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), 128 HARV. L. REV. 1019, 1023 (2015) [hereinafter Recent Cases, *Privacy Law*].

265. Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. § 1 (2015).

266. *Id.* § 3(a)(2)(A).

267. Rainey Reitman, *With Rule 41, Little-Known Committee Proposes To Grant New Hacking Powers to the Government*, ELECTRONIC FRONTIER FOUND. (Apr. 30, 2016), https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government; Joseph Cox, *US Judges Can Now Sign Global Hacking Warrants*, MOTHERBOARD (Nov. 30, 2016, 11:00 PM), http://motherboard.vice.com/read/us-judges-can-now-sign-global-hacking-warrants.

any and all evidence, access is limited to contentious data that's location has been concealed via technological means.

The jurisdictional reach of both Canadian[268] and U.S.[269] law enforcement has, however, expanded further, and broadened with the enactment of numerous statutes meant to ensure national security. Although the "extensive [United States] surveillance programs appear to capture just about all communications: everything that enters or exits the United States, anything involving a non-US participant, and anything that travels through undersea cables,"[270] the surveillance powers that Canadian law accords to the government are not any more respectful of its citizens' privacy or the privacy of individuals of other countries.[271] Not only did the Canadian government recently expand the ability of different institutions of the federal government to share the personal data of Canadian citizens, but it also "enable[d] [the Canadian Security Intelligence Service (CSIS)] to apply secretly for judicial 'disruption' warrants that would permit CSIS agents to break Canadian law and violate Charter rights with impunity."[272]

These national security laws allow for the use of technology that not only captures private communications transmitted by criminals and suspected terrorists, but that also captures private data of all other innocent citizens. As such, the implementation of such laws violates the reasonable expectation of privacy of the entire populations of both countries. Whether such a violation is reasonable when facing the risk of catching criminals or preventing terrorist attacks is another issue, but the fact remains that the privacy of innocent citizens is still being significantly breached.

---

268. *See*, *e.g.*, Canadian Security Intelligence Service Act, R.S.C. 1985, c C-23, art. 21 (Can.) (permits secret court orders authorizing CSIS to intercept communications or to obtain any other information listed in the warrant); National Defence Act, R.S.C. 1985, c N-5 (Can.) (permits warrantless wiretapping); Anti-terrorism Act, S.C. 2015, c 20 (Can.).

269. *See*, *e.g.*, Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.) (The Act permits for the issuance of secret court orders to compel the production of anything tangible that is associated with an investigation of terrorism; these orders include a prohibition of disclosure. This Act also allows for warrantless wiretapping of international communications.); Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

270. Geist, *Post-Snowden*, *supra* note 237, at 234.

271. *Id.* at 234-35.

272. Reg Whitaker, *The Failure of Official Accountability and the Rise of Guerrilla Accountability*, *in* GEIST, *supra* note 2.

V. CONCLUSION

As is demonstrated by the foregoing Parts, the limitations imposed on the powers of both U.S. and Canadian law enforcement in performing criminal investigations in digital environments, including the cloud, are tremendously insufficient to ensure privacy protection of innocent cloud users. It appears as if the United States is slowly moving towards rectifying this state of affairs, whereas Canada seems to be heading in the opposite direction.

Although the Supreme Courts of both countries have been trying to more strongly enforce constitutional limitations on the power of law enforcement by reigning in the use of warrantless searches and seizures in digital environments, the Supreme Court of the United States seems to have met more success. Whereas the Supreme Court of Canada ascribed a reasonable expectation of privacy to subscriber data,[273] the government's immediate enactment of the new lawful access legislation[274] quickly circumvented any positive effect this attempt may have had to better protect the privacy of Canadian citizens in the digital context.[275]

On the other hand, the Supreme Court of the United States' endeavors to limit the application of the Third Party Doctrine within digital environments seems to have been met with less resistance and may therefore endure to achieve its desired outcome.[276] Even though the United States' shift in this respect is occurring slowly, it appears to be having more of a positive effect on privacy protection than the efforts made in Canada. Rather, the Supreme Court of Canada's attempts are constantly undermined by new permissive legislation,[277] by the law enforcement agencies themselves,[278] as well as by the country's inferior courts who demonstrate a resistance towards to the Supreme Court's authority on this matter.[279]

Additionally, when it comes to statutes meant to limit the powers of law enforcement to better protect individual privacy, it appears as if

---

273. *See* R. v. Spencer, [2014] 2 S.C.R. 212, para. 51 (Can.).
274. Protecting Canadians from Online Crimes Act, S.C. 2014, c 31 (Can.).
275. Wingrove, *supra* note 225.
276. *See* Couillard, *supra* note 128, at 2206.
277. *See*, *e.g.*, Protecting Canadians from Online Crimes Act, S.C. 2014, c 31 (Can.).
278. McLeod & Boutilier, *supra* note 161.
279. *See* R. v. Caza, 2015 BCCA 374, para. 32 (Can. B.C. C.A.); R. v. Khan 2014 ONSC 5664, para. 27 (Can. Ont. S.C.J.); H.M.Q. v. TELUS Communications Company, 2015 ONSC 3964, paras. 29-31 (Can. Ont. S.C.J.); R. v. Ho, 2015 ONCJ 118, para. 28 (Can. Ont. C.J.); R. v. Morrison, 2014 ONCJ 774, para. 25 (Can. Ont. C.J.); R. v. Belcourt, 2015 BCCA 126, para. 55 (Can. B.C. C.A.); R. v. Capancioni, 2015 ONSC 7696, para. 38 (Can. Ont. S.C.J.); R. v. Graff, 2015 ABQB 415, para. 87 (Can. Alta. Q.B.); R. v. Nurse & Plummer, 2014 ONSC 6004, para. 47 (Can. Ont. S.C.J.).

neither Canadian nor U.S. federal laws intending to achieve this purpose have been very successful. On the Canadian front, while the PIPEDA would require a warrant to demand that service providers disclose subscriber data, which was attributed with a reasonable expectation of privacy in *R. v. Spencer*, it has had very little practical effect to protect privacy due to the new lawful access legislation.[280] Even before this law was passed, however, the RCMP circumvented the obligations imposed upon them by *R. v. Spencer* by merely asking service providers for subscriber data without a warrant.[281] In the United States, on the other hand, while the ECPA and the SCA were enacted with the ultimate purpose of accentuating the privacy of citizens in their communications, they are riddled with loopholes that could ultimately allow law enforcement to access cloud data with a simple subpoena.[282]

Yet, even though the federal laws of both countries limiting the investigatory powers of law enforcement have been largely unsuccessful in providing more acute privacy protection, the United States' position appears more beneficial to innocent cloud users. Not only has Congress recently proposed amendments to the ECPA to tie up some of the loopholes that negatively affect the privacy of U.S. citizens,[283] but several states adopted comprehensive and effective legislation in this regard,[284] such as the recent CalECPA[285] discussed above. As such, significantly more steps have been taken in the United States to better protect the privacy of innocent cloud users, whereas Canada's newly adopted legislation only serves to further erode user privacy.

Moreover, while both U.S. and Canadian legislation extending the power of law enforcement provide similar safeguards to the privacy of innocent cloud users, the level of privacy protection offered remains slightly more accentuated in the United States. First, both jurisdictions have tempered the application of the exigent circumstances exception in digital environments by permitting preservation orders for subscriber

280. Dyer, *supra* note 227.

281. McLeod & Boutilier, *supra* note 161.

282. Tokson, *supra* note 136, at 592.

283. Electronic Communications Privacy Act Amendments Act of 2015, H.R. 283, 114th Cong. (2015); Email Privacy Act, H.R. 699, 114th Cong. (2015); Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. § 1 (2015).

284. Farivar, *supra* note 194; VA. CODE ANN. § 19.3-70.3 (2016); MINN. STAT. § 626A.28 (2016); UTAH ANN. CODE §§ 77-23c-101, 77-23c-102, 77-23c-103 (LexisNexis 2016).

285. Shahid Buttar, *California Leads the Way in Digital Privacy*, ELECTRONIC FRONTIER FOUND. (Oct. 21, 2015), https://www.eff.org/deeplinks/2015/10/california-leads-way-digital-privacy.

data.[286] This allowance may prevent warrantless searches and seizures in cloud environments that would otherwise always fall under an exigent circumstances exception. By requiring service providers to preserve only the contentious data, law enforcement can avoid personally performing searches within the shared environment of the cloud, ultimately preventing the data of innocent cloud users from being incidentally accessed.

Regarding the second form of statutes that serve to extend the investigatory powers of law enforcement, namely those obliging service providers to aid law enforcement in searches and seizures performed in digital environments, both Canadian and U.S. law appear to be equally invasive of the privacy of cloud users. In Canada, the Protecting Canadians from Online Crimes Act[287] provides full immunity to any service provider who voluntarily discloses subscriber data *for any reason whatsoever*.[288] Accordingly, the private data of any Internet or cloud user can be exposed to law enforcement to the same extent as that of a person being criminally investigated, whether it is reasonable to do so or not.

In the United States, on the other hand, CALEA forces companies to introduce backdoors so that law enforcement can wiretap communications pursuant to court orders or lawful authorization.[289] While this requirement would be tremendously invasive to the privacy of all cloud users, the fact that CALEA does not apply to the cloud prevents law enforcement from wiretapping these shared environments directly, thus avoiding incidental access of the private information of innocent cloud users.[290]

That having been said, CALEA still enables law enforcement to wiretap ISP services, and since all cloud communications are made using an Internet connection, this data is still ultimately available to them. Such a wiretap would, however, only allow law enforcement agents to access the private cloud data of a single subscriber in this manner, rather than inadvertently accessing the data of all cloud users as would normally occur when a search is performed directly in the cloud. Additionally, by requiring backdoors to be created within ISP services,

---

286. Canada Criminal Code, R.S.C. 1985, c C-46, arts. 487.012-487.013 (Can.); SCA, 18 U.S.C. 121 § 2703(f) (2012).

287. Protecting Canadians from Online Crimes Act, S.C. 2014, c 31 (Can.).

288. Canada Criminal Code, R.S.C. 1985, c C-46, arts. 487.0195(2) (Can.); Geist, *Part One*, *supra* note 172.

289. CALEA, 47 U.S.C. § 1002 (2012).

290. Swire, *supra* note 249, at 204-05.

the United States is making it significantly easier for unscrupulous hackers to gain access to this information as well.[291]

While the Canadian lawful access provisions are quite permissive, especially considering that they are not submitted to judicial review, nor do they impose any service provider liability for the unreasonable disclosure of subscriber information, the U.S. legislation in this regard is equally invasive in that it increases the risk that the data of *all* Internet and cloud users will be accessed by malicious users rather than just by law enforcement officers.

The last extension of law enforcement's investigatory powers, pertaining to acquiring data across jurisdictions, is somewhat less invasive of the privacy of innocent cloud users in the United States than in Canada. For its part, Canada permits warrants to be issued for the performance of remote computer searches in other jurisdictions, essentially allowing Canadian law enforcement to search shared cloud environments on their own.[292] While similar cross-jurisdictional searches are currently permitted in the United States, a decision of the Second Circuit Court of Appeals has somewhat tempered the extent of their use.[293] Although the recent amendments to Rule 41 of the Federal Rules of Criminal Procedure allow warrants to be issued for remote searches in situations where the location of data has been concealed using technological means,[294] it is still less invasive than permitting remote computer searches under any and all circumstances. Essentially, by limiting the situations in which such searches may be performed, U.S. law enforcement is less likely to incidentally access the cloud data of innocent third parties as often as it might if these searches were permitted for any purpose whatsoever.

While neither Canadian nor U.S. law entirely protects the private data of innocent cloud users when criminal investigations are being performed in this environment, the United States has taken significantly more steps to ameliorate this situation. These attempts include proposed

---

291. Mejias, *supra* note 251, at 3260.

292. R. v. Edwards, 1999 CarswellOnt 3233, paras. 89-90 (Can. Ont. Sup. Ct. J.) (WL); eBay Canada Ltd. v. M.N.R., 2008 FCA 348, para 48 (Can.); *see also* Halladay & Chad, *supra* note 259, at 457-58; Brenner, *supra* note 256, at 52-54.

293. Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016); Recent Cases, *Privacy Law*, *supra* note 264, at 1024-26.

294. Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, DEP'T JUST. ARCHIVES (June 20, 2016), https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

amendments to the ECPA by Congress,[295] the recent passing of CalECPA,[296] and even the Supreme Court of the United States' shift towards the recognition of the Fourth Amendment protection of digital information.[297] In contrast, not only has the Canadian government neglected to make any legislative proposals toward improving this state of affairs, but it has circumvented any attempts at positive changes to this situation by adopting legislation that further violates the privacy of its citizens.[298]

This Article suggests that Canada is in fact *not* more protective than the United States of the privacy of its citizens when criminal investigations are performed in the cloud and other digital environments. Rather, the safeguards offered to this effect are somewhat less accentuated in Canada than those extended by the United States. In this light, the praise often accorded to the former for its seemingly robust privacy protections appears unmerited, as does the international criticism of the latter for its implementation of laws that erode user privacy.

---

295. Electronic Communications Privacy Act Amendments Act of 2015, H.R. 283, 114th Cong. (2015); Email Privacy Act, H.R. 699, 114th Cong. (2015); *see also* Jaycox, *supra* note 192; Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

296. CalECPA, CAL. PENAL CODE §§ 1546.1-1546.4 (West 2017).

297. *See*, *e.g.*, United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002), *vacated*, 90 Fed. App'x 3 (1st Cir. 2004); *see also* Bond v. United States, 529 U.S. 334, 338-39 (2000); United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005); United States v. D'Andrea, 497 F. Supp. 2d 117, 122 n.16 (D. Mass. 2007); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905-06 (9th Cir. 2008); United States v. Jones, 364 F. Supp. 2d 1303, 1307 (D. Utah 2005).

298. *See*, *e.g.*, Protecting Canadians from Online Crime Act, S.C. 2014, c 31 (Can.).