The Problem of Privacy: A Legal and Legislative Analysis of the Anticipated Precedent of the CLOUD Act on Data Collection and Access

By

Jaren Walker

A capstone project presented for partial fulfillment of the degree requirements for the

Masters of Arts in Policy Studies
Interdiscipline Arts and Sciences

University of Washington Bothell

2018

Table of Contests:

Abstract

The generation of cloud computing has revolutionized the world we live in but the legislation governing these technologies has lagged far behind. This matter has becoming increasingly problematic as we see a growing number of cases before the Supreme Court questioning the processes and principles of access to consumer data stored internationally. The Clarifying Lawful Overseas Use of Data (CLOUD) Act, while a long overdue refresh of electronic privacy legislation, doesn't go far enough to amend the holes in the Electronic Communications Privacy Act (ECPA) and leaves questions concerning the effectiveness of implementation going forward. This study examines the significance of the act and recommends two policy amendments to strengthen its protections as well as identifies additional areas of study as the Act is fully implemented.

Chapter 2: Purpose of the Study

Statement of the Problem:

As technology has changed and data cloud services have become more prevalent, legislation has lagged behind. The fundamental dilemma is the misconception that data is a localized entity that can be regulated as such. However, the nature of web services makes it effectively impossible to know exactly where data is stored despite how courts have resolved this issue previously. Updated policies have been proposed in the last two sessions of Congress (International Communications Privacy Act being one example) and just this year the Clarifying Lawful Overseas Use of Data (CLOUD) Act has been passed into law as part of the March 2018 Omnibus. Consequently, further research on implementation and potential ramifications of this legislation are still needed.

Background:

Electronic Communications Privacy Act

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA).[1] Under the ECPA, it is a federal crime to wiretap or use any machine meant to capture the communications of others without court approval, unless one of the targeted parties has given prior consent. Likewise, it is also a federal crime to use or disclose any information acquired by illegal means.[2] The ECPA protects wire, oral, and electronic communications

[1] 100 Stat. 1848 (1986).
[2] Doyle, C. (2013). Privacy: An overview of the electronic communications privacy act. In Privacy: Select Issues and Laws for the 21st Century (pp. 111-205). Nova Science.

while those communications are being made, are in transit, and when they are stored on computers.

These protections extend to email and telephone conversations in addition to data stored electronically.[3] The crux of this study revolves around Title II of the ECPA: the Stored Communications Act (SCA). The SCA protects the privacy of the content of files stored by service providers and of records held about the subscribers of those providers (such as name, billing records, or IP addresses.)[4]

The SCA allows for two avenues for law enforcement to access this data: permissible provider disclosure and required provider access.[5] Relevant to this study are the nuances of section 2703 of the SCA where distinctions are drawn between recent communications and those that are considered "abandoned." If electronic communications are less than 180 days old, government entities must have a search warrant in order to access any of the data. However, if that data is left in electronic storage for more than 180 days it is considered abandoned and opens government entities to utilize a warrant, subpoena or a court order to force content disclosure (significantly less strict judicial proceedings).[6]

[3] DHS/Office for Civil Rights and Civil Liberties, DHS/Privacy Office, & DOJ, Office of Justice Programs, Bureau of Justice Assistance. (2013, July 30). Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22. Retrieved November 12, 2017, from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

[4] Ibid

[5] 18 U.S.C. 2701-2712.

[6] 18 U.S.C. 2703(a)(" ... A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section").

These court orders may be issued by any federal magistrate or judge qualified to do so under Title III and need not be issued in the district in which the provider is located.[7]

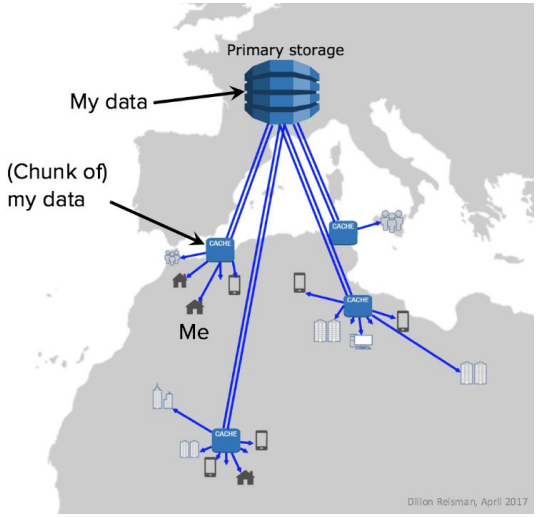
How Data Storage Works

When data was something as simple as a file on a machine in a specific location, this policy was reasonable. However, now that data has been splintered and multiplied to spread across devices and backed up into "clouds," geographical regulation is no longer relevant. Before delving into this issue, it is important to understand the nature of data storage by well-developed web services (eg. Google, Facebook, etc.) Some examples of these storage techniquest include[8]:

"Edge caches" across borders: This system of caching data allows the most in-demand content to be rapidly available to users by keeping copies of these data chunks in separate locations--shortening the trip data travels across the network. The cache system updates the chunks of data being stored based on changing demand and other factors. Thus, the expense of data can be kept in a centralized location while smaller machines (possible in different locations) can more quickly distribute high demand data to locals.

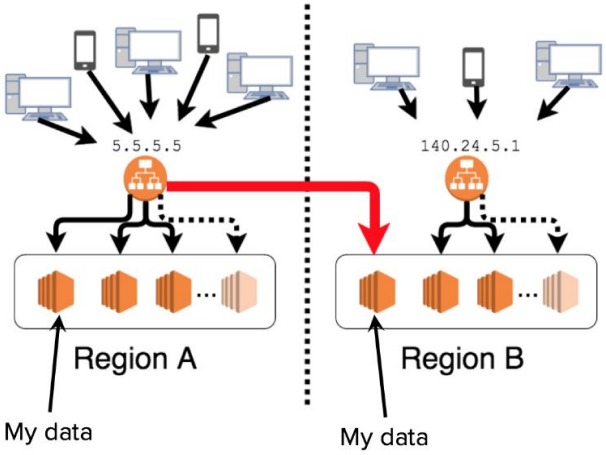
[7] United States v. Berkos, 543 F.3d 392, 397 (7th Cir. 2008), quoting 18 U.S.C. 2703(a), ("[W]hen 'a court with jurisdiction over the offense' issues an out-of-district warrant for the seizure of electronic communications, it must do so 'using the procedures described in the Federal Rules of Criminal Procedure'")

[8] Reisman, D. (2017). Where Is Your Data, Really?: The Technical Case Against Data Localization [Abstract]. Lawfare, surveillance, privacy, and data across borders: trans-atlantic perspectives.



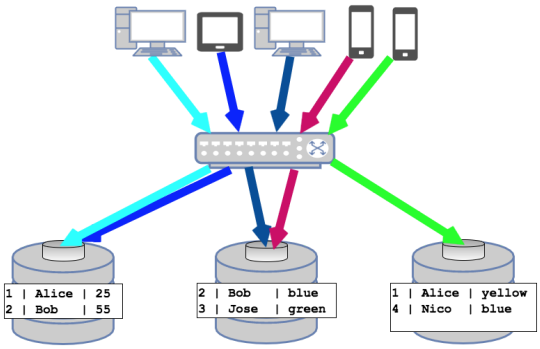
(Graphic by: Reisman, D. (2017). Where Is Your Data, Really?: The Technical Case Against Data Localization)

Load balancing replication: To increase efficiency on servers, web services may replicate user data across various data centers in different regions to better balance regions with higher demand. For instance if one region has higher activity and has trouble meeting the demand, the network may route the data to a replica server in a different region.



(Graphic by: Reisman, D. (2017). Where Is Your Data, Really?: The Technical Case Against Data Localization)

Data "sharing" across multiple machines in multiple datacenters: To store the millions of gigabytes of data, web services store data across "shards" with each individual device holding a shard of data. An individual's data can be split between any number of shards; allowing it to be distributed, copied and backed up across multiple machines.



(Graphic by: Reisman, D. (2017). Where Is Your Data, Really?: The Technical Case Against Data Localization)

Data backup in case of system failure: If you've ever accidently deleted a file or experienced a hardware crash that corrupted a hard drive, you know how horrible data loss can be. Even the most mature web services can be susceptible to these malfunctions (like Gmail in 2011 who lost millions of users' inboxes due to a software bug.[9]) As a result, these providers tend to keep regular backups to prevent such data losses in case of malfunction, natural disasters, or other unforeseen situations.

As these examples indicate, pushing for data localization (meaning certain user data files be kept within national borders) would render web services largely unviable.[10] Thus, the question becomes, as data is spread out, replicated, multiplied and splintered across various centers and devices in multiple locations - Whose laws for access and regulation does the data fall under? Is the data restricted to the laws of the country of nationality of

[9] "Gmail Back Soon for Everyone." Official Gmail Blog, Google, 28 Feb. 2011,
[10] Reisman, D. (2017). Where Is Your Data, Really?: The Technical Case Against Data Localization [Abstract]. Lawfare, surveillance, privacy, and data across borders: trans-Atlantic perspectives.

the individual user? Is it subject to the laws of the provider's country of origin? Or is it controlled by the jurisdiction of whichever country it is stored in? The CLOUD Act proposes a formalized process to answer these questions.

Significance of Study:

As we will discuss later, under the overarching problem of regulation highlighted above is a deeper problem of monitoring governments' access to individual's data. In particular under what conditions should governments' have access to stored data and what processes should be imposed to protect consumers. Furthermore, experts have suggested that the localization debate is relevant to issues ranging from intellectual property law to global anti-censorship efforts. The implementation of the CLOUD Act needs to be closely monitored and continuously updated just as the technologies it seeks to regulate will change and develop.

Chapter 3: Literature Review

Problems Within Current Legislation

The passage of the CLOUD Act has reconciled the long outdated Electronic Communications Privacy Act (ECPA). The inappropriate use of the ECPA to regulate access to data stored in cloud services promoted two problems: 1) American law enforcement access to data held abroad and 2) international law enforcement access to data held by American firms. [11] The ECPA does not specify whether American government has jurisdiction to compel U.S. providers to produce content stored abroad and it has been used to prohibit American firms from complying with foreign governments' requests for user data.

United States v. Microsoft

The first issue above on law enforcement was epitomized by the United States v. Microsoft or the "Microsoft-Ireland" case. In December 2013, federal law enforcement agents applied to the United States District Court for the Southern District of New York for a warrant mandating Microsoft to disclose all emails and other information associated with a particular account.[12] Satisfied with the probable cause associated with the account being used to further illegal drug trafficking, a Magistrate Judge issued the warrant.

After receiving the warrant, Microsoft determined that the requested information was stored solely in Microsoft's datacenter in Dublin, Ireland. Microsoft then moved to

[11] Woods, Andrew Keane, and Peter Swire. "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems." *Lawfare*, 6 Feb. 2018,
[12] Derek Hawkins. "Disclosure of Electronic Communication." Wisconsin Law Journal, 2018, pp. Wisconsin Law Journal, May 2, 2018.

quash the warrant with respect to the information being subject to Ireland's law. However, the Magistrate Judge denied the motion.[13] The District Court then adopted the Magistrate Judge's ruling and ultimately held Microsoft in civil contempt of court for failing to comply with the warrant.[14] Upon appeal, a panel of the Court of Appeals for the Second Circuit reversed the denial of the motion to quash and vacated the civil contempt charge by holding that requiring Microsoft to disclose the requested data would be an unauthorized extraterritorial application of the warrant.

Shortly after, the Government obtained a new warrant, pursuant to the CLOUD Act, requiring Microsoft to disclose the data. Currently, no live dispute remains between either party and the case before the Supreme Court regarding the old warrant has become moot.

This case hinged less on the procedures of the trial, and more on the international relations and corporate reputation for Microsoft. Had Microsoft turned over the data to the U.S. government no questions asked, the company would have lost competitive advantage in foreign markets who would likely question the protections provided to foreign consumers of U.S. providers.

Significance of the CLOUD Act

By amending the ECPA, the CLOUD Act has accomplished two things: 1) It has specified that an order under the SCA applies to all data that is in the "possession, custody, or control" of the provider regardless of the location of the server where the data is stored. More specifically, the addition of 18 U.S.C. §2713 states that:

[13] In re Warrant to Search a Certain E-Mail Account, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).
[14] In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F. 3d 197, 204 205 (CA2 2016)

> "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.' (Emphasis added.)"[15]

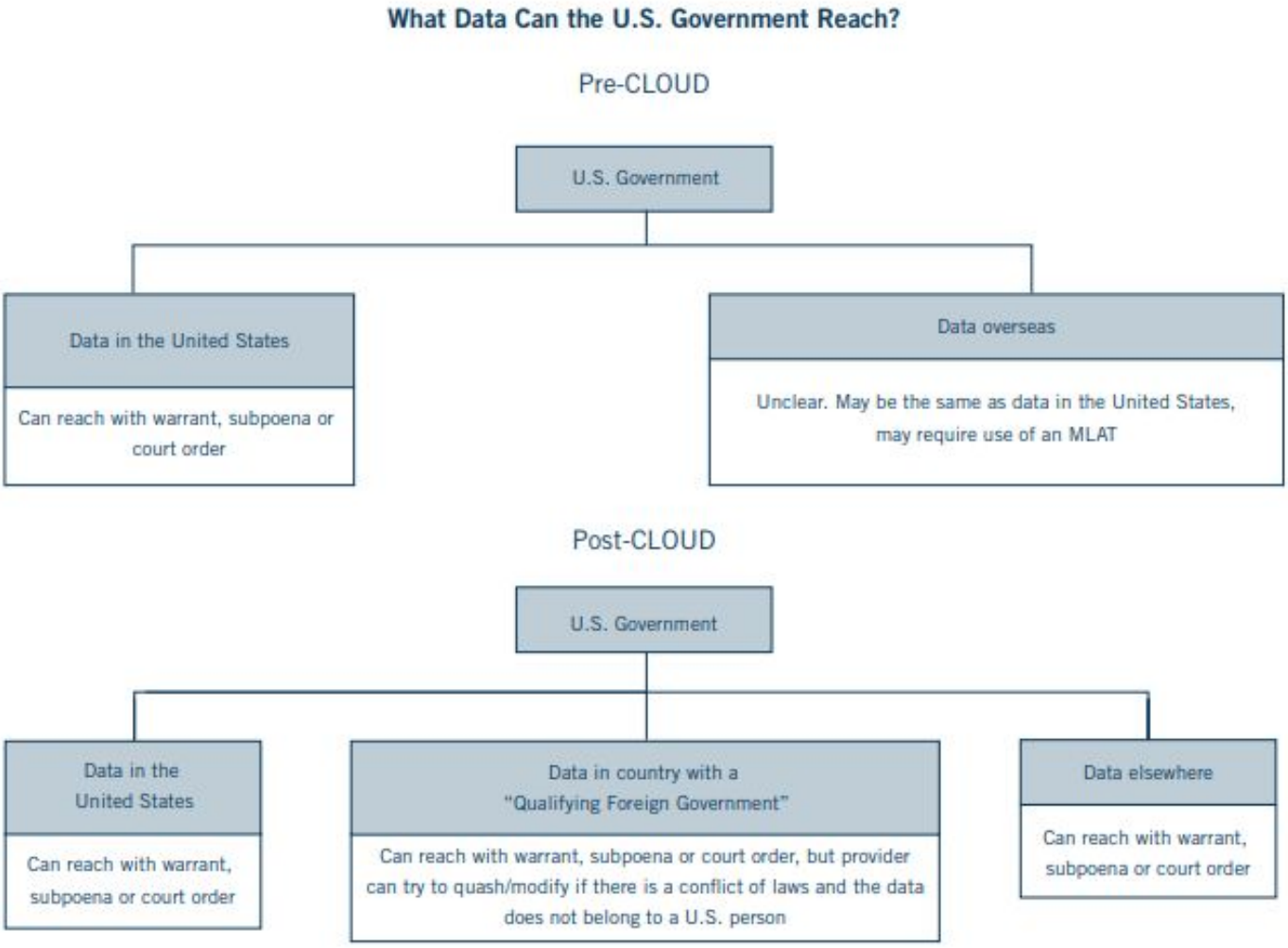
Furthermore, 2) the CLOUD Act allows for governments to engage in executive agreements to allow foreign governments to request content directly from American providers. These agreements are not available to every country but rather are restricted to those that meet a stringent set of requirements and only then "if the Attorney General, with the concurrence of the Secretary of State," determine that:

> (1) The country has "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" (to be determined by reference to a laundry list of human rights and rule of law standards); (2) The foreign government has adopted minimization procedures regarding information concerning US persons; and (3) The agreement has protections to prevent the foreign government from targeting or collecting information about US persons or persons located in the US, and to prevent the US government from requesting the foreign government to use the agreement as a runaround on current restrictions on data collection.[16]

These agreements replace the existing precedent of the Mutual Legal Assistance (MLA) process. Currently, requests for evidence or data are governed by international agreements known as "mutual legal assistance treaties" where one country agrees to abide by another country's court system under certain conditions. However, the system has become antiquated as foreign countries grow frustrated with invoking international diplomacy to prosecute local crimes involving American cloud-based services.[17] The

[15]In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F. 3d 197, 204 205 (CA2 2016)
[16] Woods, Andrew Keane, and Peter Swire. "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems." *Lawfare*, 6 Feb. 2018,
[17] Daskal, Jennifer, and PEter Swire. "Why the CLOUD Act Is Good for Privacy and Human Rights." Lawfare, 18 Mar. 2018,

CLOUD Act streamlines this process by providing that once both countries enter into the Executive Agreement then the foreign law-enforcement requests for data can be responded to directly by providers.[18]



(Graphic by: Barnett, Ben, et al. "Forecasting the Impact of the New US CLOUD Act." Dechert, 13 Apr. 2018)

[18] Loeb, Robert, et al. "The CLOUD Act Explained." Orrick Edit, 6 Apr. 2018

Chapter 4: Methodology

In order to understand the potential implications of the CLOUD Act, it is necessary to decipher the nuanced concerns of the opponents of this legislation as well as its proponents. With the basic overview of the legislative holes in the ECPA and the foundational understanding of the *Microsoft v. Ireland* case, this researcher delved into the legal opinions of scholars familiar with this matter. These opinions highlighted areas of improvement from present legislation and of concern which informed the recommendations to follow relevant to the implementation of the CLOUD Act going forward.

This study relied mostly on the Program Evaluation model[19] to accomplish this analysis with the differing stakeholder opinions as the main unit of analysis. This method was chosen largely due to the newness and nature of this topic; being that the CLOUD Act just passed in March 2018 and implementation is still in the works, this researcher found the matter timely but also necessary to skeptically, qualitatively analyze.

Data Collection

Due to the nature of this study, primary data was collected through legal documents and court briefings. Additionally, several secondary source data originated from the writings of experts and academics familiar with the nuances of the CLOUD Act and the subsequent legislation prior to its passage. These sources highlighted the voids left by current legislation and the potential precedent of the CLOUD Act going forward.

[19] O'Sullivan, Rita G. "Collaborative evaluation within a framework of stakeholder-oriented evaluation approaches." Evaluation and program planning 35.4 (2012): 518-522.

Chapter 5: Results and Discussion

Proponents of the CLOUD Act

At its core, the CLOUD Act is "a logical solution for governing cross-border access to data," according to major bill sponsors (Microsoft, Google, Facebook, Apple and Verizon subsidiary Oath) as stated in a Letter of Support dated February 6, 2018 to Senators Hatch, Coons, Graham, and Whitehouse.[20] The letter argues further that the bill provides adequate protections for customer privacy, highlighting a provision that would require the U.S. to account for a country's human rights, privacy and rule of law before discussing data sharing agreements (a procedure meant to alleviate tensions concerning the shift away from MLA agreements).

Furthermore, other supporters have highlighted that while the CLOUD Act expands the geographic scope of the ECPA, it does not change who is subject to its orders or what type of data is subject to the law-enforcement requests.[21] Same as before, the Actapplies only to providers of "electronic communication services" and "remote computing services" (think businesses that offer email, electronic messaging, or cloud storage services to the public.)[22] Also unchanged is the restriction that access is limited to only content of electronic communications and cloud-stored documents as well as non-content data relating to electronic communications (such as user account information) and not other types of personal or business data. The Act simply updates and clarifies the previous rules governing U.S. law-enforcement access.

---

[20] Apple, et al. "Letter to Senators Hatch, Coons, Graham, and Whitehouse ." The Official Microsoft Blog, Microsoft , 6 Feb. 2018

[21] Loeb, Robert, et al. "The CLOUD Act Explained." Orrick Edit, 6 Apr. 2018

[22] 18 U.S.C. §§ 2510(15) (defining electronic communications services), 2711(2) (defining remote computing services)

Opponents of the CLOUD Act

Contrarily, groups such as the Center for Democracy & Technology (CDT) and the Electronic Frontier Foundation (EFF) are concerned that the CLOUD Act doesn't do enough to protect consumers. CDT Vice President for Policy, Chris Calabrese, has said, "The Electronic Communications Privacy Act balances the interest of consumers, providers, and the government. The CLOUD Act throws the balance off-kilter by accommodating providers and the government but leaving consumers behind."[23] The CDT is specifically concerned about the CLOUD Act's omission of the requirement of a warrant, issued on the basis of probable cause, for disclosure of communications to government entities in the U.S.

Furthermore, civil liberty groups have highlighted similar concerns about the Act. In particular, the matter of warrants versus subpoenas to obtain content information of non-U.S. persons abroad. The CLOUD Act doesn't address the outdated principle in the ECPA that content older than 180 days and held by remote computer services are available to law enforcement with just a subpoena instead of meeting the higher evidentiary requirements of a warrant.[24] As a reminder, this is significant because warrant requirements provide substantially more procedural and substantive privacy protections than subpoena requirements. Subpoenas are issued without judicial authorization upon determination that the evidence sought is merely relevant to the crime while warrants

[23] "CLOUD Act Would Erode Trust in Privacy of Cloud Storage - Center for Democracy & Technology." Privacy Policy | Center for Democracy & Technology, Center for Democracy & Technology, 6 Feb. 2018

[24] Nojeim, Craig. "Cloud Act Implementation Issues." Lawfare, 10 July 2018, www.lawfareblog.com/cloud-act-implementation-issues.

require strong evidence of probable cause that the information sought pertains to the crime. Additionally, only a judge independent of the investigation can issue a warrant.[25]

Finally, there have been some objections to the Act based on the potential use of information obtained bilaterally through agreements under the CLOUD Act that could lead to prosecution of foreigners abroad in U.S. cases in which the death penalty may be sought. Because 146 countries have abolished the death penalty including many U.S. allies (Australia, Canada, New Zealand, the U.K. and most of Europe)[26] some countries may insist on provisions that allow them the right to refrain from providing such information in cases that could lead to such verdicts.

Discussion

While privacy hawks may condemn the Act as another example of the U.S. overstepping with extraterritorial jurisdiction, the amendment is consistent with standards of state authority to legislate in areas that have domestic effects, or notions of jurisdiction that are grounded in both domestic and international law.[27]

Furthermore, unlike prior legislation, safeguards are built into the Act to address the warrant vs. subpoena debacle within the ECPA and preserve the right of providers to challenge U.S. law-enforcement demands for data. Specifically there are processes included that allow providers to quash or modify legal process if they "reasonably believe" the subscriber in question "is not a U.S. person and does not reside in the U.S" and/or

[25] Slobogin, Christopher. "Subpoenas and privacy." DePaul L. Rev. 54 (2004): 805.
[26] "Abolitionist and Retentionist Countries." Battle Scars: Military Veterans and the Death Penalty | Death Penalty Information Center, Death Penalty Information Center, 31 Dec. 2017
[27] Woods, Andrew Keane, and Peter Swire. "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems." *Lawfare*, 6 Feb. 2018,

disclosure would "create a material risk that the provider would violate the laws" of the foreign government[28]

A court can than modify or quash if it finds the following : disclosure would cause the provider to violate the laws of the foreign government; granting the challenge would serve "the interests of justice"; and the customer or subscriber is not a U.S. person and does not reside in the U.S.[29] Determining what "the interests of justice" requires the court to consider the interests of the U.S. and foreign government, the likelihood and nature of the penalties that would be imposed and the person and provider's connections to the U.S., or the importance of the information to the investigation and the availability of other means to obtain it. [30]

Finally, the bill protects providers and consumers from requests for data stored outside of the country by requiring a court to conduct a comity analysis in the event a motion to quash is filed. This "comity analysis" allows courts to evaluate factors such as: the importance of the information requested, the degree of specificity of the request, whether the information originated in the U.S., the availability of alternative means to obtain the information and the U.S. and foreign interests at stake.

Relevant to the concerns about the Executive Orders, it is important to note the following limitations: specifically, they cannot be used to require companies to decrypt data stored on its systems. After the San Bernardino, CA shooting in December 2015, when 14 people were killed and 22 others were seriously injured during a terrorist attack, the heated debate between national security and individual electronic privacy intensified when

[28] CLOUD Act §103(b)
[29] Id
[30] Id

the FBI insisted that Apple decrypt the suspects iPhone 5c for evidence and Apple refused. Apple and their supporters insisted that even though the diseased suspect had been a known terrorist, the precedent unlocking the phone would have set an unethical standard for criminal investigations going forward; a precedent for both U.S. Government and foreign government requests.[31] Ultimately the FBI was able to access the data without Apple's assistance, but the debate about privacy over national security still remains. Thus, while legislators and judiciaries continue to battle that one out--the CLOUD Act does not provoke the argument.

Another important consideration is the limitation of the types of orders that may be issued by foreign law enforcement under these agreements. For example, orders must: be for the purpose of obtaining information related to "serious crime, including terrorism," "Identify a specific person, account, address, or personal device," be limited in time and scope," be justified by "articulable and credible facts," and remain "subject to review or oversight by a court" or "other independent authority."[32]

[31] Etzioni, Amitai. "Apple: Good Business, Poor Citizen?" Journal of Business Ethics, vol. 151, no. 1, 2018, pp. 1–11.
[32] CLOUD Act § 105

Chapter 6: Conclusion and Policy Recommendations

The CLOUD Act offers privacy advocates an alternative option to a world of a growing number of foreign governments requiring providers to localize their data to comply with local laws and preventing foreign intervention. If you compare the due process protections of the Act with those under the Fourth Amendment, privacy and human rights groups will argue that foreign governments will get access to more information on American consumers than they do currently. However, after the aforementioned procedural changes are juxtaposed to the informal and outdated processes utilized currently, one can conclude that governments are not gaining anymore access than they currently had. Rather, it can be suggested that both foreign allies (as dictated by the Executive Agreements) and the U.S. Government will benefit from the newly formalized process while better protecting providers and consumers alike.

Questions remain, however, about transparency under the CLOUD Act and jurisdiction of its agreements: Will the Justice Department give the public notice of the countries with which it plans to negotiate bilateral agreements? How will the Justice Department require companies to report on real-time surveillance orders they receive from foreign governments? How they will interpret and implement the prohibition of data requests that infringe freedom from foreign governments? Will the CLOUD Act protect providers' right to notify U.S. government or foreign countries of problematic data requests? What happens to agreements with foreign government that undergo dramatic regime changes that may result in data being used to threaten human rights? Who will be

consulted to determine possible human rights violations prior to entering CLOUD Act agreements?

These and others are but a few of the major concerns regarding implementation of the CLOUD Act procedures for which the recommendations to follow seek to address:

Recommendation #1: "Exclusive Means"

Because the Executive Agreements under the CLOUD Act will replace the diplomatic requirements for data sharing through mutual legal assistance treaties, the gap in voluntary disclosures needs to be closed. Specifically, under current law, U.S. providers can voluntarily disclose non-content information to foreign governments. Under MLA treaties and CLOUD Act Executive agreements formal requests must meet the aforementioned criteria; yet, these informal voluntary disclosures have no legal standard they must meet. Therefore, additional regulation is needed to ensure further consumer protections via provider oversight or another means of third party review.

Additionally, clarification is needed to address whether Executive Agreements under the CLOUD Act apply to specific offices or agencies of a nation.[33]Privacy groups have suggested that a designated entity in each agreement country is needed to control for the quality of demands on providers, ensure their lawfulness, establish authenticity and serve the demand properly.[34] This ensures accountability for execution of these demands should mistakes occur or questions arise.

[33] Woods, Andrew Keane, and Peter Swire. "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems." *Lawfare*, 6 Feb. 2018,

[34] Nojeim, Craig. "Cloud Act Implementation Issues." Lawfare, 10 July 2018

Recommendation #2: Warrants for Content

The CLOUD Act does not address the fundamental problem with modern computing services highlighted above within the ECPA and the SCA specifically; the matter of content older than 180 days and held remotely is still available to law enforcement with only a subpoena. Adding the pending Email Privacy Act (currently in Congressional Committee) to the CLOUD Act would reconcile this problem by imposing a warrant for content blanket rule for these communications.

It is worth noting that most major U.S. providers, despite the language of ECPA, follow the rule established by the Sixth Circuit in *U.S. v. Warshak* by demanding warrants for content—no matter the content's age and no matter whether it is held by a "remote computing service" or an "electronic communication service."[35] However, because *Warshak* was a constitutional decision, law enforcement may take the position that the rule doesn't apply for content of non-U.S. persons abroad as they are outside of the jurisdiction of the Constitution. Thus, the CLOUD Act needs to be rectified considering it's strong implications for consumers abroad.

[35] Nojeim, Craig. "Cloud Act Implementation Issues." Lawfare, 10 July 2018

Chapter 7: Looking Ahead

Limitations

As with any newly passed legislation, it is difficult to gauge how effective this Act will be at mitigating future conflict regarding access to data with foreign stakeholders. Because the CLOUD Act was passed in March of 2018, as of this writing scholars are still speculating at the implementation and ramifications of the agreements and procedures the bill proposes.

Specific to this study, this meant that the data utilized to underscore the significance of this bill were also largely speculative. As the bill moves into procedural process and more negotiations with foreign governments begin, a clearer view of the precedent of the CLOUD Act will be available and, subsequently, additional suggestions for adaptation.

Future Research

As highlighted above, there are still many questions posed about how the CLOUD Act will work in the framework of current policy, especially regarding the agreements with foreign governments. Once more data is available regarding how the Justice Department has engaged with these agreements and quantitative figures can be collected to assess the effectiveness of mitigating conflict between governments and providers internationally, further study should be given to the following areas in no particular order of importance:

1. Impact on data localization laws in international markets post-CLOUD Act implementation

2. Qualitative review of the Justice Department's process to establish agreements with Foreign Governments (with special attention to the department's transparency during negotiations)
3. Analysis of how the Executive Agreements influenced providers plans to develop or move data centers into/out of countries with/without these agreements (to prevent irreconcilable obligations under two countries' laws)
4. Any review of consumer response to the change in legislation/concern over provider loyalty
5. International effectiveness of the CLOUD Act and EU countries beholden to the GDPR Standard

Works Cited

- 18 U.S.C. §§ 2510(15) (defining electronic communications services), 2711(2) (defining remote computing services)

- "Abolitionist and Retentionist Countries." Battle Scars: Military Veterans and the Death Penalty | Death Penalty Information Center, Death Penalty Information Center, 31 Dec. 2017, deathpenaltyinfo.org/abolitionist-and-retentionist-countries.

- Apple, et al. "Letter to Senators Hatch, Coons, Graham, and Whitehouse ." The Official Microsoft Blog, Microsoft , 6 Feb. 2018, blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.

- Barnett, Ben, et al. "Forecasting the Impact of the New US CLOUD Act." Dechert, 13 Apr. 2018, www.dechert.com/content/dam/dechert%20files/publication/2018/4/White%20paper%20-%20Cybersecurity%20-%20Cloud%20Act%20-%2004-18.pdf.

- "CLOUD Act Would Erode Trust in Privacy of Cloud Storage - Center for Democracy & Technology." Privacy Policy | Center for Democracy & Technology, Center for Democracy & Technology, 6 Feb. 2018, cdt.org/press/cloud-act-would-erode-trust-in-privacy-of-cloud-storage/.

- CLOUD Act §103(b)

- CLOUD Act § 105

- Daskal, Jennifer, and PEter Swire. "Why the CLOUD Act Is Good for Privacy and Human Rights." Lawfare, 18 Mar. 2018, www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

- Derek Hawkins. "Disclosure of Electronic Communication." Wisconsin Law Journal, 2018, pp. Wisconsin Law Journal, May 2, 2018.

- Etzioni, Amitai. "Apple: Good Business, Poor Citizen?" Journal of Business Ethics, vol. 151, no. 1, 2018, pp. 1–11.

- "In Re Grand Jury Proceedings the Bank of Nova Scotia.united States of America, Plaintiff-Appellee, v. the Bank of Nova Scotia, Defendant-Appellant, 740 F.2d 817 (11th Cir. 1984)." *Justia Law*, 14 Aug. 1984, law.justia.com/cases/federal/appellate-courts/F2/740/817/233788/.

- “Gmail Back Soon for Everyone.” Official Gmail Blog, Google, 28 Feb. 2011, gmail.googleblog.com/2011/02/gmail-back-soon-for-everyone.html.

- In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F. 3d 197, 204 205 (CA2 2016)

- In re Warrant to Search a Certain E-Mail Account, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

- Loeb, Robert, et al. “The CLOUD Act Explained.” Orrick Edit, 6 Apr. 2018, www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained.

- Nojeim, Craig. “Cloud Act Implementation Issues.” Lawfare, 10 July 2018, www.lawfareblog.com/cloud-act-implementation-issues.

- O'Sullivan, Rita G. "Collaborative evaluation within a framework of stakeholder-oriented evaluation approaches." Evaluation and program planning 35.4 (2012): 518-522.

- Reisman, D. (2017). Where Is Your Data, Really?: The Technical Case Against Data Localization [Abstract]. Lawfare, surveillance, privacy, and data across borders: trans-atlantic perspectives. Retrieved June 16, 2018, from https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.

- Slobogin, Christopher. "Subpoenas and privacy." DePaul L. Rev. 54 (2004): 805.

- Woods, Andrew Keane, and Peter Swire. “The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.” *Lawfare*, 6 Feb. 2018, www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.