Washington Law Review

Volume 93 | Number 2

6-1-2018

Privacy in the Cloud: The Fourth Amendment Fog

Sarah Aitchison

PRIVACY IN THE CLOUD: THE FOURTH AMENDMENT FOG

Sarah Aitchison*

Abstract: The Cloud has changed how individuals record, store, and aggregate their personal information. As technology's capacity for holding an individual's most intimate details and recording day-to-day experiences increases, Fourth Amendment privacy protections become less equipped to respond to technological advances. These advances allow private companies to store an immense amount of their consumers' personal information, and government entities to obtain that information. In response, tech companies have begun refusing to comply with government demands for information collected and stored in their devices and in the Cloud, and are increasingly ending up in court, fighting orders to disclose consumer information. A dynamic tension has developed between the United States government's desire and increased capacity to obtain information about consumers, and tech companies wanting to keep their consumers' information private. The relevant statute, the Electronic Communications Privacy Act (ECPA), is not equipped to address these technological advances. The Supreme Court's extensive Fourth Amendment jurisprudence and guidelines for addressing Fourth Amendment issues are similarly ill-suited to answer the novel and unique issues that accompany digital, remote storage of personal information. This Comment identifies the inadequacies of ECPA and the Fourth Amendment jurisprudence as they each apply to technological advances and the potential of Cloud data. It argues that Congress must revise the legislative scheme to adequately protect information stored in the Cloud, particularly addressing whether consumers have a right to know when their information is being accessed by the United States government. Further, it argues courts lack the tools to adequately amend, reframe, repeal, or apply ECPA, and thus should not be the primary body making decisions about the bounds of technologically based government collection under the Fourth Amendment. Alternatively, if the legislature does not act, courts will remain required to make findings related to whether the collection of information is a violation of the Fourth Amendment. Courts should, then, recognize that digital data deserves a fundamentally distinct analysis and discontinue the trend of finding attenuated connections between classic surveillance techniques and government surveillance using advanced technology.

INTRODUCTION

In the last five years, Amazon.com, Inc. (Amazon), Apple, Inc. (Apple), and Microsoft Corporation (Microsoft) have all been subject to controversies regarding the storage of private digital information via their Cloud-based data services.[1] The Cloud refers to internet-based

* J.D. Candidate 2018, University of Washington School of Law. Thank you to the phenomenal staff at *Washington Law Review* for all their hard work. Thank you to Professor Mary Fan for her thoughtful edits and fantastic suggestions. All errors are my own.

storage systems that, in recent years, have replaced local physical devices, such as hard drives, as the primary storage system for anything an individual may view, use, store, or save electronically.[2] The fight between the United States government for Cloud data related to ongoing criminal investigations and companies that want to protect the privacy of their consumers has become more contentious and more prevalent. These companies have been unwilling to turn over their customers' data to government agencies attempting to solve crimes or investigate suspects.[3] This resistance from tech companies directly challenges the government's broad authority to access this type of data, granted to it under the 1986 Electronic Communications Privacy Act (ECPA).[4]

Several recent cases demonstrate the rising tension between government agencies and tech companies. In 2015, an Arkansas man hosted a party for his friends where they watched a football game.[5] The next day one of his party guests was found dead in the backyard.[6] Police investigating the crime seized the host's Amazon Echo device. Amazon's Echo constantly records noises in a room and saves any communications recorded after an individual uses the Echo's "wake" word to call it into action. It then sends those communications to Amazon for storage in the Cloud. Investigators, hoping to find evidence implicating the host, repeatedly requested Amazon turn over access to

1. Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 887 (W.D. Wash. 2017); Devlin Barrett, *U.S. to Keep Pushing Apple to Unlock iPhone in New York Case*, WALL ST. J. (Apr. 8, 2016, 3:38 PM), http://www.wsj.com/articles/u-s-to-keep-pushing-apple-to-unlock-iphone-in-new-york-case-1460128066 [https://perma.cc/7N3P-B5KP] [hereinafter Barrett, *U.S. to Keep Pushing Apple*]; Alina Selyukh, *As We Leave More Digital Tracks, Amazon Echo Factors In Murder Investigation*, NPR (Dec. 28, 2016, 3:20 PM), http://www.npr.org/sections/alltechconsidered/2016/12/28/507230487/as-we-leave-more-digital-tracks-amazon-echo-factors-in-murder-investigation [https://perma.cc/95ZM-BJHD]. The government later dropped the iPhone case. Devlin Barrett, *Federal Prosecutors Drop Court Case to Force Apple to Unlock iPhone*, WALL ST. J. (Apr. 22, 2016, 10:36 PM), http://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-apple-to-unlock-iphone-1461377642 [https://perma.cc/UM8F-MDK5] [hereinafter Barrett, *Federal Prosecutors Drop Court Case*].

2. Joanna Stern, *What is the 'Cloud'?*, ABC NEWS (June 26, 2012), http://abcnews.go.com/Technology/cloud-computing-storage-explained/story?id=16647561 [https://perma.cc/Z7FD-9WKP].

3. *Microsoft Corp.*, 233 F. Supp. 3d at 894; Barrett, *U.S. to Keep Pushing Apple*, *supra* note 1; Barrett, *Federal Prosecutors Drop Court Case*, *supra* note 1; Selyukh, *supra* note 1.

4. Electronic Communications Privacy Act, 18 U.S.C. § 2705(b) (2012).

5. Barrett, *U.S. to Keep Pushing Apple*, *supra* note 1; Selyukh, *supra* note 1.

6. Selyukh, *supra* note 1.

the recordings.[7] After months of back and forth, Amazon agreed to hand over the Alexa data at the beginning of March 2017.[8]

In April 2016, Microsoft filed a complaint against the United States government alleging the government's use of ECPA violated the Fourth Amendment.[9] The Western District of Washington dismissed Microsoft's Fourth Amendment claim on standing grounds.[10] Apple has also had its own battles with the government regarding customer data. The Department of Justice tried to force Apple to unlock an iPhone related to a 2015 San Bernardino, California terrorist attack.[11] When Apple refused to cooperate, the government hired hackers to do the job for it.[12] In another case, the Department of Justice pursued a court order to force Apple to unlock an iPhone seized in relation to a drug investigation.[13] The government later dropped the case.[14] Most recently, in November 2017, after a gunman attacked a church in Sutherland Springs, Texas, the Federal Bureau of Investigation (FBI) served Apple with another warrant, this time for both the gunman's iPhone and Cloud data.[15] Apple has yet to respond to the warrant.[16]

---

7. *Id.*

8. *Id.* In response, the company released a statement: "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course." *Id.*

9. Complaint for Declaratory Judgment, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2016) (No. 2:16-cv-00538-JLR). The complaint also alleges the government's use of ECPA is a violation of the First Amendment. *Id.*

10. Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 887 (W.D. Wash. 2017) (stating that Microsoft did not have standing to bring this issue as a third party under the Fourth Amendment, but could bring the claim under the First Amendment).

11. Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0 [https://perma.cc/RV62-E8MS].

12. Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.859eee269aa0 [https://perma.cc/248F-ZN2U]. Before that, in September 2014, Apple made it "impossible for the company to turn over data from most iPhones or iPads to police—even when they have a search warrant." Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?tid=a_inl&utm_term=.4e49f7be96f1 [https://perma.cc/RWS4-TEYS].

13. Barrett, *U.S. to Keep Pushing Apple*, *supra* note 1.

14. Barrett, *Federal Prosecutors Drop Court Case*, *supra* note 1.

15. Rob Thubron, *Apple Served with Search Warrant to Access Texas Shooter's iPhone, iCloud Account*, TECHSPOT (Nov. 19, 2017, 1:47 PM), https://www.techspot.com/news/71947-apple-served-search-warrant-access-texas-shooter-iphone.html [https://perma.cc/X6GX-4CH9].

These cases all focus on the tension between the appropriate means through which consumer data can be accessed and who has a right to that information: whether it belongs to the consumer, the tech companies storing it, or the United States government. This tension presents dynamic challenges absent in previous jurisprudence: while courts have long examined technological capacity and privacy, the immense scope of data that can now be aggregated and stored in the Cloud is unprecedented. The impact of these kinds of cases is far-reaching. Amazon had sold more than eight million Echo devices by January of 2017.[17] More than 400 million devices are running Microsoft's Windows 10.[18] Apple's iPhones are used by more than 700 million people.[19] Most importantly, each of these technological services are Cloud-based, which means they automatically upload information inputted by consumers into the Cloud to be stored.[20] The sheer amount of private information stored and then uploaded to the Cloud through these devices is massive.

Courts have attempted to manage the tension between investigative agencies requiring access to private data and claims that the Fourth Amendment protects such data. But courts, including the Supreme Court, lack the tools to adequately engage in the type of technical analysis required when dealing with private data aggregation by third parties.[21] The existing jurisprudence fails to adequately address when the government's examination of information aggregated, disseminated, and stored on electronic devices and the Cloud is a constitutional violation of a person's right to privacy.[22] The relevant statute, ECPA, also does not

16. *Id.*

17. Taylor Soper, *More than 8M People Own an Amazon Echo as Customer Awareness Increases 'Dramatically,'* GEEKWIRE (Jan. 25, 2017, 10:57 AM), https://www.geekwire.com/2017/8-million-people-amazon-echo-customer-awareness-increases-dramatically/ [https://perma.cc/W2JH-DQSZ].

18. Tom Warren, *Apple Reveals Windows 10 Is Four Times More Popular Than the Mac*, VERGE (Apr. 4, 2017, 9:54 AM), https://www.theverge.com/2017/4/4/15176766/apple-microsoft-windows-10-vs-mac-users-figures-stats [https://perma.cc/JRL3-6FN8]. That does not include the number of people who use Microsoft products that do not use Windows 10. *Id.*

19. Don Reisinger, *Here's How Many iPhones Are Currently Being Used Worldwide*, FORTUNE (Mar. 6, 2017), http://fortune.com/2017/03/06/apple-iphone-use-worldwide/ [https://perma.cc/UUL8-95QG].

20. *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/P43Z-GAB9]; Russell Brandom, *Windows 10 Is the End of Cloud-Free Computing*, VERGE (Aug. 17, 2015, 4:59 PM), https://www.theverge.com/2015/8/17/9167203/windows-10-privacy-scare-cloud-privacy [https://perma.cc/TJ48-ZUYT]; *iCloud for Safekeeping. And Easy Sharing.*, APPLE, https://www.apple.com/icloud/ [https://perma.cc/5N3J-PMWJ].

21. *Infra* section II.A.

22. *Id.*

provide adequate guidance.[23] The overbroad nature of ECPA and the lack of judicial clarity on the issue demands congressional action.[24]

When enacted, ECPA's authors did not foresee the grand technological advances used today.[25] ECPA was created to deal with how the government could access the technology of the time,[26] which did not include the immense collection and storage of aggregated data through the Cloud.[27] While much has been written on the reformation of ECPA as it applies to the individual, there is little about the relationship between tech companies' capacity to store private information and the government's utilization of the Act to access such information. Furthermore, the Supreme Court has only heard one case regarding the government's search power under ECPA and has yet to issue an opinion.[28] Therefore, magistrate, district, and circuit court judges have been the primary administrators of ECPA. They often come to different opinions from each other, particularly regarding the protective strength and scope of court orders that determine in what scenarios the government can access stored information.[29] Congress must enact new laws or amend ECPA to adequately reflect the massive technological advances of the past thirty years. In the absence of legislative action, courts should recognize that digital data and storage is fundamentally distinct and demands different analysis than the classic tools used to identify whether a government search is constitutional. Justices have been reluctant to apply a consistent framework for analyzing searches of and by technological data—oscillating between recognizing technology as fundamentally distinct from classic surveillance techniques and applying the same traditional theories to digital data. The Court should consistently recognize data as fundamentally distinct and abandon attempts to bring digital searches in line with traditional surveillance methods.

Part I of this Comment reviews ECPA, section I.A explores ECPA's history, and section I.B discusses courts' application of ECPA. Part II

---

23. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

24. Electronic Communications Privacy Act, 18 U.S.C. § 2705(b) (2012).

25. Julie J. McMurry, Note, *Privacy in the Information Age: The Need for Clarity in the ECPA*, 78 WASH. U. L.Q. 597, 602 (2000).

26. *Id.*

27. *Id.*

28. *See* Carpenter v. United States, __ U.S. __, 137 S. Ct. 2211 (2018) (No. 16-402) (granting certiorari).

29. Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017). *See generally infra* section III.A.

examines the Supreme Court's Fourth Amendment jurisprudence. Section II.A focuses on the established framework for courts to analyze Fourth Amendment protections afforded to modern data storage and technology, and section II.B examines three seminal cases, as well as their concurrences, respectively. These cases indicate that the Court oscillates between two fundamental principles when dealing with digital information: first, that digital data searched by advanced technology is distinct from traditional methods of surveillance; and, alternatively, that it is simply an extension of traditional methods of surveillances. Part III analyzes possible solutions to this challenge. Section III.A analyzes ECPA's current protections and why it falls flat in the face of modern technology and aggregated data. Section III.B discusses why the judiciary is not the correct branch of government to make specific decisions regarding technology searches. This section further argues that Congress should amend ECPA or enact new legislation. Finally, section III.C argues that, if Congress fails to act, the courts should establish that digital data is fundamentally distinct and is due a new type of analysis under the Fourth Amendment.

I. ECPA CREATES AN UNWORKABLE STANDARD AMONG COURTS

Congress first enacted ECPA in 1986.[30] ECPA amended Title 18 of the U.S. Code, which primarily deals with criminal procedure and crimes, including when a search or seizure is valid.[31] The portion of the Act related to storing and retrieving digital data is also commonly referred to the Stored Communications Act (SCA). At the time of enactment, the primary purpose of ECPA was to "prevent unauthorized government access to private electronic communications"[32] even when that information was voluntarily provided by an individual to a third party. ECPA creates a set of procedures the government must abide by when seeking to obtain private consumer information stored by a third party, such as Amazon or Microsoft. First, the government can apply for a court order to access the content of a consumer's information and communications so long as the information is "relevant" to an ongoing

30. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

31. *Id.*

32. *What is the Electronic Communications Privacy Act?*, MINC: LEGAL RES. CTR., https://www.minclaw.com/legal-resource-center/what-is-the-electronic-communications-privacy-act/ [https://perma.cc/LKB4-3RK5].

investigation and has been stored by the company for more than 180 days.[33] If the information has been stored by the third party for fewer than 180 days, the government must obtain a warrant based on probable cause.[34] When the government is authorized to access information from third-party technology companies—regardless of whether the government obtains a court order or warrant—it may also prevent those companies from informing customers that their information is being searched and monitored by the government.[35] Although the government may only prevent notice to the subject of the search for ninety days at a time, it may request an extension as many times as it wants. This process of repeatedly getting court orders to prevent the subjects of searches to be notified of the search has become known as "secrecy orders" or "indefinite gags."[36]

A. ECPA Has Not Adapted to Modern Technology

When Congress enacted ECPA in 1986, less than one percent of Americans had cell phones,[37] let alone cell phones that could store significant amounts of personal information and automatically upload that information into discreet, electronic storage facilities. Since its enactment, ECPA has been amended more than ten times,[38] but none of these amendments addressed the standards through which the government can obtain either content information of private individuals or an indefinite gag order. As it currently stands, the Act has been criticized[39] for failing to protect consumers in a day and age where

33. 18 U.S.C. § 2703(a), (d).

34. *Id.* § 2703(a).

35. *Id.*

36. Complaint for Declaratory Judgment, *supra* note 9, at 6; Andrew Crocker, *New DOJ Policy on Gag Orders Is Good, but the Courts Could Have Done Better*, ELEC. FRONTIER FOUND. (Oct. 25, 2017), https://www.eff.org/deeplinks/2017/10/new-doj-policy-gag-orders-good-courts-could-have-done-better [https://perma.cc/49VY-48KX].

37. Petition for Writ of Certiorari at 33, Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016) (No. 16-402); CTIA, BACKGROUND ON CTIA'S WIRELESS INDUSTRY SURVEY 2 (2015), https://www.ctia.org/docs/default-source/default-document-library/ctia_survey_ye_2014_graphics.pdf [https://perma.cc/YJL9-82JB].

38. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871 (2004).

39. In response to ECPA, activist groups have popped up dedicated to the reformation of the Act in light of the developing technology. Digital4th is one such group. The organization describes its problem with ECPA in the digital world on its homepage: "[w]hen it passed in 1986, ECPA was intended to extend Fourth Amendment protections to online communications. However, this was long before most Americans had access to a home computer, before email was widely used, and before the invention of Facebook, Twitter, and other social media platforms." *A Summary of the*

sharing information is highly dependent on electronic communications. Although technology has changed dramatically in the last thirty years, ECPA has remained "virtually the same."[40] For example, ECPA provides stronger protections for content information (the body of the email) rather than non-content information (the subject line of the email) by creating different standards through which a magistrate may approve a court order to search the information.[41] But, ECPA does not differentiate between search implications for Cloud-based services and more traditional web-based services, even though the amount and type of data stored in each can be drastically different.[42] Because the Cloud provides an expansive online storage system for users, the government can now quickly and easily access information that would have traditionally been stored on a local hard-drive or in a desk drawer; information that would not be automatically shared with a third party. Therefore, under ECPA the government has broad power to access and seize information commonly stored online, such as emails or documents.[43] The immense information that can be stored on the Cloud and the potential to chip away at individuals' privacy calls for greater protections than are currently provided.

Before ECPA, federal wiretap and privacy standards only protected wire and oral communications.[44] Through ECPA, Congress sought to expand protections to cover stored electronic communication, such as emails, even when they were provided to a third party voluntarily.[45] Under ECPA, the government can require a company to turn over vast

---

Electronic Communications Privacy Act (ECPA), DIGITAL4TH, https://digital4th.org/ [https://perma.cc/A5SM-7EPS].

40. *Id.*

41. The distinction between content data and non-content data is at the crux of Fourth Amendment search jurisprudence. *See generally* Riley v. California, __ U.S. __, 134 S. Ct. 2473 (2014); Kyllo v. United States, 533 U.S. 27 (2001). The classic example distinguishing the two is a mailed letter: the information inside the letter is considered content and, therefore, provided greater Fourth Amendment protections; the information on the outside of the letter, such as the name and addresses of the correspondents, is considered non-content information. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (expanding the logic behind letter information to distinguish between IP addresses (content) and URLs (non-content)); Electronic Communications Privacy Act, 18 U.S.C. § 2703 *et seq.* (2012) (establishing the standard for obtaining content information).

42. *A Summary of the Electronic Communications Privacy Act (ECPA)*, *supra* note 39. This was also at the crux of Microsoft's complaint. Complaint for Declaratory Judgment, *supra* note 9.

43. Complaint for Declaratory Judgment, *supra* note 9, at 1; *A Summary of the Electronic Communications Privacy Act (ECPA)*, *supra* note 39.

44. Katherine A. Oyama, Note, *E-mail Privacy After* United States v. Councilman*: Legislative Options for Amendment ECPA*, 21 BERKELEY TECH. L.J. 499, 504 (2006).

45. *Id.*

amounts of information regarding any number of customers[46] as well as prohibit the company from telling customers their data is being shared with investigators.[47] Under the statute, the court issuing the order must allow the gag order if there is "reason to believe" the notification of a warrant, subpoena, or court order will result in "(1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial."[48] Every ninety days, a court may issue a new gag order as long as one of the criteria is met.[49]

A recent case involving Microsoft directly addresses the tension between ECPA as written and indefinite gag orders as applied to Cloud data. Microsoft alleged section 2705(b), which creates the indefinite gag order option, is unconstitutional because "[p]eople do not give up their rights when they move their private information from physical storage to the cloud."[50] When ECPA was written, Congress did not adequately consider the type of technology prevalent today and the changes made to

46. *See* Electronic Communications Privacy Act, 18 U.S.C. § 2705 *et seq.* (2012) (lacking clear limitations to the governments subpoena power).

47. *Id.* § 2705(b).

48. *Id.*

49. *Id.*

50. Complaint for Declaratory Judgment, *supra* note 9, at 2. The complaint also provides an excellent overview of why the transition from local hardware to Cloud storage implicates the Fourth Amendment.

> Before the digital age, individuals and businesses stored their most sensitive correspondence and other documents in file cabinets and desk drawers. As computers become prevalent, users moved their materials to local computers and on-premises servers, which continued to remain within the user's physical possession and control. In both eras, the government had to give notice when it sought private information and communications, except in the rarest of circumstances.
>
> Cloud computing has spurred another profound change in the storage of private information. Today, individuals increasingly keep their emails and documents on remove servers owned by third parties, i.e., in the cloud, using free web-based services . . . . Businesses have also migrated their information technology infrastructure to servers hosted by providers . . . which offer productivity software . . . and the ability to access correspondence and other documents from any device. But the transition to the cloud does not alter the fundamental constitutional requirement that the government must—with few exceptions—give notice when it searches and seizes the private information or communications of individuals or businesses.
>
> The government, however, has exploited the transition to cloud computing as a means of expanding its power to conduct secret investigations. As individuals and business have moved their most sensitive information to the cloud, the government has increasingly adopted the tactic of obtaining the private digital documents of cloud customers not from the customers themselves, but through legal process directed at online cloud providers like Microsoft.

Id.

the statute throughout the years have failed to address advances in technology.[51]

Despite these shortcomings, some jurisdictions have considered the issue and many have identified that the implication of new technology, particularly storage of data in the Cloud, warrants stronger protection than provided under ECPA. At least fifteen states have enacted legislation aimed at more strongly protecting digital information than the federal ECPA.[52] California, in particular, enacted comprehensive legislation that requires all law enforcement agencies to obtain a warrant before accessing content information of consumers, including location information.[53] In contrast, the federal government recently passed a bill that would allow federal law enforcement agencies to circumvent ECPA and the Fourth Amendment in accessing consumer data.[54] While the Clarifying Lawful Overseas Use of Data (CLOUD) Act does not explicitly amend ECPA, it allows foreign governments to access consumer information from technology companies without a warrant.[55] The United States government can then retrieve that data from the foreign government as it sees fit.[56] The tension between tech companies and the government on the federal and state level indicates that ECPA, as is, is an inadequate tool for courts analyzing protections under the Fourth Amendment.[57] Additionally, the movement of the states toward providing stronger protections similarly shows ECPA's failure to protect the privacy of individuals.[58]

---

51. *Id.*; Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1045 (2008).

52. 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/ [https://perma.cc/Z5TE-PM5H].

53. *Id.*

54. Tom Krazit, *President Trump Signs Omnibus Spending Bill Putting the CLOUD Act on the Books in Big Shift for Cloud Data*, GEEKWIRE (Mar. 23, 2018, 10:50 AM), https://www.geekwire.com/2018/president-trump-signs-omnibus-spending-bill-putting-cloud-act-books-big-shift-cloud-data/ [https://perma.cc/3PR5-VWTC].

55. Tom Krazit, *As Congress Considers the Tech-Backed CLOUD Act, Privacy and Human Rights Groups Raise Concerns*, GEEKWIRE (Mar. 18, 2018, 12:00 PM), https://www.geekwire.com/2018/congress-considers-tech-backed-cloud-act-privacy-human-rights-groups-raise-concerns/ [https://perma.cc/MNB3-U7V4].

56. *Id.*

57. Brief for Petitioner at 21, Carpenter v. United States, __ U.S. __, 138 S. Ct. 293 (2017) (No. 16-402), 2017 WL 3575179, at *21 ("In assessing whether an expectation of privacy is objectively reasonable, norms and expectation shaped by federal and state statutes are relevant considerations." (citing Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality opinion))).

58. Zetter, *supra* note 52.

B. Confusion and Inconsistent Outcomes: ECPA's Section 2705(b) Delayed Notification Requirement

Wide divergence in the interpretation by lower courts of one of ECPA's main provisions for the government's authorization to collect information exemplifies the confusing standards and inconsistent application among lower courts. Many legal scholars have written about effective ways to amend ECPA.[59] Currently, the Supreme Court is considering a case, *Carpenter v. United States*,[60] examining the validity of the government's acquisition of significant amounts of non-content information based on ECPA section 2703, which sets standards for when government entities may access information stored by a remote computing service.[61] By enacting section 2703(b), Congress explicitly intended to prevent the government from engaging in unregulated "fishing expeditions."[62] Despite scrutiny from academics and the nation's highest court, one provision of ECPA has been largely ignored in the discourse, even though litigation surrounding it has become more prevalent: section 2705(b)—the indefinite gag order exception. Courts throughout the country have imposed significantly different outcomes when it comes to the length of time customers can remain in the dark about whether their information is being searched.

Courts' inconsistent application of the indefinite gag order exception under the Fourth Amendment demonstrates the unworkability of ECPA. Under ECPA section 2703(a), the government can require companies to refrain from informing their customers that the government is obtaining their information when it uses a search warrant.[63] But, ECPA

---

59. *See, e.g.*, Kerr, *supra* note 23 (providing a detailed recommendation for changing ECPA to adequately address changing technology).

60. __ U.S. __, 138 S. Ct. 293 (2017) (No. 16-402).

61. *See generally* Transcript of Oral Argument, Carpenter v. United States, __ U.S. __, 138 S. Ct. 293 (2017) (No. 16-402).

62. Brief for Respondent at 31, Carpenter v. United States, __ U.S. __, 138 S. Ct. 293 (2017) (No. 16-402), 2017 WL 4311113, at *53 (quoting H.R. REP. NO. 827, pt. 1, at 31 (1994)).

63. Electronic Communications Privacy Act, 18 U.S.C. § 2703(a) (2012) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. 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.").

section 2703(b) does require disclosure to consumers when the government obtains an administrative court order to access their content-based information.[64] However, section 2705 creates a delayed notice loophole that allows the government to continue obtaining information on consumers indefinitely without notifying them, as long as the government gets a new court order every ninety days.[65] These extended section 2705(b) orders have become known as secrecy, or indefinite, gag orders. In October of 2017, the Department of Justice imposed the first limitation on the use of indefinite gag orders by implementing a one-year limit on the use of indefinite gag orders by federal agents.[66] However, the newly implemented policy can be revoked at any time.[67]

The recent changes to the government policies surrounding the use of indefinite gag orders do not resolve the larger issue at hand: the application of indefinite gag orders across jurisdictions results in different outcomes. The Microsoft case specifically focused on this issue, claiming that ECPA's indefinite gag order provision was unconstitutional under the Fourth Amendment.[68] In its complaint, Microsoft alleged that more than 3,250 secrecy orders were ordered against the company in fewer than two years.[69] The Fourth Amendment claim was ultimately dismissed on a standing issue, but the case still sheds light on the concerns over ECPA. The Western District of

---

64. *Id.* § 2703(b) ("A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or (ii) obtains a court order for such disclosure under subsection (d) of this section; *except that delayed notice may be given pursuant to section 2705 of this title*." (emphasis added)).

65. *Id.* § 2705(a)(4) ("Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.").

66. Memorandum from Rod J. Rosenstein, Deputy Attorney General, to Heads of Department Law Enforcement Components; Department Litigating Components; the Director, Executive Office for U.S. Attorneys; & all United States Attorneys (Oct. 19, 2017), https://www.documentcloud.org/documents/4116081-Policy-Regarding-Applications-for-Protective.html [https://perma.cc/3QWB-AJ2H] [hereinafter DOJ Memo].

67. Crocker, *supra* note 36.

68. Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 887 (W.D. Wash. 2017); *supra* notes 9–10 and accompanying text. Microsoft prevailed on its First Amendment claim when the Court held the use of indefinite gag orders was a limitation on the company's speech. *Id.*

69. *Microsoft Corp.*, 233 F. Supp. 3d at 896.

Washington Court maintained that Microsoft could not bring this case as a third party but indicated that ECPA searches were questionable in light of the Fourth Amendment. The judge opined, "[a]s Microsoft alleges, the indefinite nondisclosure orders allowed under Section 2705(b) mean that some customers may never know that the government has obtained information in which those customers have a reasonable expectation of privacy."[70] The opinion went on to state that some of Microsoft's customers will be unable to vindicate their own Fourth Amendment rights.[71]

In contrast to the Microsoft case, federal courts in California have twice recently determined that a finite period for gag orders is a commonsense application of ECPA.[72] In an order examining the validity of a warrant issued through ECPA, a magistrate judge held that the application of indefinite gag orders were unconstitutional in that they raised First Amendment concerns.[73] In that case, the court distinguished between prior cases where a gag order would expire after ninety days so long as the government did not request an extension and when the government asks for a gag order until further notice.[74] The court stated that the requirement of expiration was vital and without it, indefinite gag orders were unconstitutional.[75]

In a second recent case, a federal court from the Central District of California determined that ECPA's indefinite gag order violated Adobe Systems Incorporated's (Adobe) First Amendment rights.[76] The court discussed the lack of controlling precedent for dealing with ECPA's indefinite gag orders[77] and its inconsistent application across courts,[78] a sentiment echoed in this Comment. The opinion went on to examine the Microsoft case, as well as other cases from other jurisdictions where an indefinite gag order was considered constitutional.[79]

---

70. *Id.* at 916.

71. *Id.* at 915.

72. *In re* Grand Jury Subpoena for: [Redacted]@yahoo.com, 79 F. Supp. 3d 1091, 1091 (N.D. Cal. 2015); *In re* Search Warrant for [Redacted]@hotmail.com, 74 F. Supp. 3d 1184, 1184 (C.D. Cal. 2014).

73. *In re Grand Jury Subpoena*, 79 F. Supp. 3d at 1091.

74. *Id.* at 1093.

75. *Id.*

76. *In re Search Warrant*, 248 F. Supp. 3d at 970.

77. *Id.* at 978 ("The Ninth Circuit has not ruled on whether Section 2705(b) allows for indefinite NPOs, and authority on the question is scarce.").

78. *Id.*

79. *Id.*

The courts in these cases illustrate the privacy concerns implicated in the power ECPA provides the government. In *In re Grand Jury Subpoena for: [Redacted]@yahoo.com*,[80] the court said,

> [W]ere the court to grant the government's request [for an indefinite gag order], Yahoo! would be prohibited from ever sharing the existence of the subpoena with anyone—even years after the grand jury moved on to other things. In an era of increasing public demand for transparency about the extent of government demands for data from providers like Yahoo!, this cannot stand.[81]

Courts have largely deferred to Congress when dealing with statutory protections in the privacy realm, and ECPA is no exception.[82] Congress has left those protections untouched in recent years resulting in different courts doing different things with practically the same set of facts. With the increased litigation surrounding ECPA and Cloud data, Congress should act and create necessary changes to ECPA that can guide courts as they analyze the government's ability to access consumer information.[83] One reason why courts have inconsistently applied the statute is because the relevant jurisprudence is not particularly instructive.

C. Courts' ECPA Jurisprudence Is Inconsistent and Largely Unhelpful

Other judicial interpretations of ECPA provide little guidance for dealing with the types of issues relevant in the Microsoft case, and other government requests for data stored in the Cloud. Most federal court decisions surrounding ECPA deal with private communications provided first to a third-party employer, and then to the government. The relationship between employer and employee creates a situation that is utterly distinct from one in which the third party has no relationship—

---

80. 79 F. Supp. 3d 1091 (N.D. Cal. 2015).

81. *Id.* at 1094–95.

82. Oza, *supra* note 51, at 1054–55.

> Because Congress is in a better position than the courts to conduct fact-finding inquiries, courts, in deference to Congress, will typically avoid unnecessary determinations of constitutional questions where Congress has drafted an expansive statutory scheme regulating some aspect of constitutional rights. *The ECPA is one such statutory scheme*, and therefore, courts are often deferential to Congress in determining Fourth Amendment protection for electronic communications.

Id. (emphasis added) (footnote omitted).

83. *Infra* section III.A.

other than as a storage facility for information—with the individual who is the subject of the search.

There are only three cases where the Supreme Court has explicitly incorporated ECPA into its analysis. Most recently, in *City of Ontario v. Quon*,[84] the Court determined that city officials could access a police officer's text communications under ECPA.[85] The Court's analysis of the validity of ECPA rested on distinguishing between the role of the government as an employer, and the role of the government as a prosecutor and investigator of crimes.[86] Because the Court identified the government actor as an employer, rather than its more traditional role as government entity investigating crimes, the Court granted the government more leeway to access the employee's information under ECPA.[87] The Court's analysis renders this case unhelpful when applying it to the realm of personal information stored in a Cloud and managed by third parties.

In a case a few years prior, *Doe v. Chao*,[88] Doe claimed the government violated his right to privacy under the Fourth Amendment when the Department of Labor used his social security number to verify his request for benefits under the Black Lung Act.[89] Doe raised ECPA as a last resort to get damages when the Privacy Act he originally sued under, which regulated the government's storage of individual's records, did not allow for damages.[90] Doe attempted to compare the legislative history of ECPA, which does allow damages, and the Privacy Act to show that he could receive damages.[91] The Court was unconvinced by his attempts to draw comparisons between the statute at issue and ECPA.[92] The Court said that it was particularly unmoved by a legislative interpretation that looks beyond the text, history, and relevant case law; particularly when the records act was enacted after ECPA.[93] This analysis has dissuaded lower courts from using analogous legislation when identifying legislative purpose.

---

84. 560 U.S. 746 (2010).

85. *Id.* at 746–47.

86. *Id.*

87. *Id.*

88. 540 U.S. 614 (2004).

89. *Id.* at 614.

90. *Id.* at 626–27.

91. *Id.* at 626. ECPA's legislative history indicates a plaintiff could receive minimum damages without proving real damages, while the Privacy Act at issue in this case does not. *Id.* at 627.

92. *Id.* at 626–27.

93. *Id.*

The Court's other ECPA case—the 2001 case *Bartnicki v. Vopper*[94]—does not provide much guidance either.[95] In *Bartnicki*, the Court considered the validity of government use of information that had been illegally intercepted and then broadcast to the public.[96] However, the Court focused on whether the radio broadcast of illegally obtained information was a violation of the First Amendment, and did not substantially address the Fourth Amendment implications.[97] The relevant analysis of ECPA is inapplicable to the current state of electronic communication, access, and storage affairs because in *Bartnicki*, the issue revolved around a non-governmental person[98] accessing information and what was then done with that information.[99] There was no discussion of the role of governmental officials, who may have been able to legally obtain the information under ECPA, if they had properly requested it.[100] The government did not intercept the information at all, making the case wholly irrelevant to this Comment's analysis.[101] There was also no discussion of the initial acquisition of the information—the Court focused on what that electronically stored information was used for later.[102] Therefore, none of the Court's ECPA cases are illustrative for purposes of Fourth Amendment analysis and third parties who are not employers.

While the Supreme Court has yet to examine the validity of ECPA,[103] several of the circuit courts have. Most are employment cases that are irrelevant to the unique consumer-business relationships at issue in this Comment. *United States v. Councilman*,[104] *Garcia v. City of Laredo*,[105]

---

94. 532 U.S. 514 (2001).

95. *Id.*

96. *Id.* at 514. During contract negotiations between a union and their employer, part of a conversation was recorded and then played on the radio the next day. The union contended the recording was obtained in violation of the Wiretap Act, which is related to ECPA, and therefore, it was illegal to play it on the radio. *Id.*

97. *Id.*

98. It was unknown who intercepted the communication and leaked it to the radio reporter (or whether the radio reporter was the one who accessed the communication in the first place). *Id.* at 514–15.

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

103. Pending the Court's forthcoming opinion in *Carpenter v. United States*, __ U.S. __, 137 S. Ct. 2211 (2018) (No. 16-402).

104. 418 F.3d 67 (1st Cir. 2005).

105. 702 F.3d 788 (5th Cir. 2012).

Theofel v. Farey-Jones,[106] and *United States v. Warshak*[107] are all seminal cases examining ECPA outside the employment context. However, the courts decided *Councilman* and *Theofel* prior to 2008, before Cloud computing technology was widespread.[108] In *Councilman*, the First Circuit held that an Internet Service Provider (ISP) could conduct real-time surveillance of its customers' email exchanges when the communication was intercepted while transferring between storage locations.[109] The Fifth Circuit in *Garcia* determined that ECPA did not apply to information stored on a personal cell phone.[110]

In *Theofel*, the Ninth Circuit focused on ECPA's cause of action.[111] Although the case directly addressed the relevant issues and tension between government acquisition of information and third-party storage, it did not create enduring precedent. In *Theofel*, the government obtained "'[a]ll copies of e-mails sent or received by anyone' at [the company], with no limitation as to time or scope" after being granted an overbroad warrant.[112] The court made a broad ruling that created different warrant requirements for unopened emails and unopened emails that had "expired in the normal course."[113] Since the *Theofel* decision, lower courts in the Ninth Circuit have struggled to understand the distinction between unopened emails and unopened emails that are expired.[114] Other circuit courts have explicitly rejected that analysis as overbroad and unworkable.[115]

Most notably, in *United States v. Warshak*, the Sixth Circuit explicitly recognized that an individual has a reasonable expectation of privacy in the content of their email messages held by their third-party ISP.[116] The court held that a government agency could not compel email messages from a third party without a warrant.[117] Warshak was brought to court

106. 359 F.3d 1066 (9th Cir. 2004).

107. 631 F.3d 266 (6th Cir. 2010).

108. For example, Apple did not launch its customer cloud until 2011. Ross Rubin, *Switched On: Apple's Cloud Conundrum*, ENGADGET (June 12, 2011), https://www.engadget.com/2011/06/12/switched-on-apples-cloud-conundrum/ [https://perma.cc/FC83-R627].

109. *Councilman*, 418 F.3d at 67.

110. *Garcia*, 702 F.3d at 790 (declining to extend the determinations made by the First Circuit in *United States v. Councilman*).

111. *Theofel*, 359 F.3d at 1072 (referring to ECPA by its other name, the SCA).

112. *Id.* at 1071.

113. *Id.* at 1076.

114. Kerr, *supra* note 23, at 1214.

115. United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).

116. United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).

117. *Id.* at 286.

for conning people into purchasing herbal supplements, which promised—but failed to—significantly increase penis size.[118] During its investigation, law enforcement officers seized about 27,000 of Warshak's private emails from his ISP after obtaining a court order, but not a warrant, under ECPA.[119] The Sixth Circuit held that even though ECPA technically allowed for the acquisition of tens of thousands of emails with a court order, it was still a violation of the Fourth Amendment.[120] In its analysis, the court recognized that digital data is fundamentally distinct from traditional means of communication and information storage: "[i]n short, 'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities."[121] The court ultimately determined that, because of the government agents' good-faith belief that they did not need a warrant to access the content of Warshak's emails held by his ISP, the emails would not be excluded from the trial even though they were improperly gathered under ECPA.[122] However, the court's departure from the standard application of ECPA and the recognition of the strain between the statute and the Fourth Amendment makes the case particularly noteworthy, even when the court ultimately allowed the emails. Together, these four cases showcase the variance in court decisions when interpreting ECPA and the inconsistency across jurisdictions.

Other circuits have also taken up the issue, but never when the government was trying to access information about individuals, making the analysis distinct from cases where ECPA is used to obtain information in the Cloud.[123] In *Fraser v. Nationwide Mutual Insurance Co.*,[124] the Third Circuit held that a company's interception of an employee's email account to prove his disloyalty and consequently fire him was not a violation of ECPA.[125] In *Hall v. Earthlink Network*,

118. *Id.* at 277.

119. *Id.* at 283.

120. *Id.* at 274.

121. *Id.* at 284.

122. *Id.* at 274.

123. *See, e.g.*, Expert Bus. Sys., LLC v. BI4CE, Inc., No. 06-1265, 2007 WL 1381595, at *2 (4th Cir. May 9, 2007) (holding that ECPA was not violated when someone forwarded the emails to a third party because there was no government interception).

124. 352 F.3d 107 (3d Cir. 2003).

125. *Id.* at 109–11.

Inc.,[126] the Second Circuit summarily dismissed a case in favor of the ISP in which a plaintiff claimed the ISP intercepted his email and identified him as a spammer.[127] Because these cases deal primarily with the employee-employer relationship or relationships solely between private individuals, they fail to provide meaningful ECPA analysis for courts to apply when examining searches of Cloud data.

Guest v. Leis[128] is more illustrative of how the government acquires private information under ECPA. While most of the circuit court opinions regarding ECPA fail to address the relationship between private information and government seizure, in *Leis*, the Sixth Circuit held that information meant for public posting was not subject to a reasonable expectation of privacy.[129] Specifically, an online bulletin board system was seized as part of an obscenity investigation.[130] Users of the bulletin board brought a claim against investigators under ECPA, alleging that the investigation into the posts was a violation of a citizen's reasonable expectation of privacy.[131] The court determined that, because the users were planning to post their information to the public, they were not afforded protection under the Fourth Amendment.[132] *Leis* is particularly relevant to the issues at hand because of the court's explicit Fourth Amendment analysis and the government actors' seizure of the information of private officials.[133] However, the case is distinguishable from ECPA Cloud cases because the information the government officials seized was explicitly for public use, whereas the cases relating to tech companies, such as *Microsoft*, involve the search and seizure of information that is not explicitly intended for public posting.[134] The circuit court cases illustrate the many kinds of ECPA analyses courts can engage in and establish that whether the party seeking the information is a private person or a government actor is a threshold question for ECPA analysis.[135]

126. 396 F.3d 500 (2d Cir. 2005).
127. *Id.* at 508.
128. 255 F.3d 325 (6th Cir. 2001).
129. *Id.* at 326.
130. *Id.* at 330.
131. *Id.*
132. *Id.* at 333.
133. *Id.* at 334.
134. *Id.* at 333.
135. *Supra* section I.B.

II. THE SUPREME COURT'S FOURTH AMENDMENT JURISPRUDENCE FAILS TO ADDRESS THE FULL GAMUT OF TECHNOLOGICAL PRIVACY ISSUES

To understand the relationship between the Fourth Amendment and the Cloud, it is vital to understand the rights afforded to individuals under the Fourth Amendment and the breadth of power the government has in accessing private information from tech companies under ECPA. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[136] The Supreme Court has parsed this language into multiple tests. First, the government is conducting a "search" if they are seeking information that can only be found by penetrating an individual's reasonable expectation of privacy.[137] Second, warrantless searches are per se unreasonable absent a few specific exceptions.[138] Third, to analyze constitutional searches, courts have consistently examined the methods through which information was acquired, not necessarily the subject matter of the information.[139] Finally, courts apply different analyses when examining whether an individual's property has been seized under the Fourth Amendment.[140]

To understand how the Fourth Amendment interacts with ECPA and the subsequent impact on obtaining digital data, it is important to understand the Court's extensive Fourth Amendment jurisprudence. ECPA was meant to create clear digital protections under the Fourth Amendment when dealing with digital data[141] and was guided by foundational Fourth Amendment principles: examining how, not what, data is collected by the government, and whether an individual has a reasonable expectation of privacy in that data.[142] In conducting this analysis, the Court has echoed ECPA's creators in its desire to avoid "dragnet-type law enforcement practices."[143]

---

136. U.S. CONST. amend. IV.

137. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While the reasonable expectation of privacy test came originally from Justice Harlan's concurrence, it quickly became controlling law. *See* Florida v. Jardines, 569 U.S. 1, 11 (2013).

138. *Katz*, 389 U.S. at 361 (the defendant in *Katz* took and placed illegal bets over the phone while investigators listened in. Justice Harlan suggested the defendant had a reasonable expectation of privacy within the phone booth).

139. *Id.* at 361–62.

140. *See* United States v. Jones, 565 U.S. 400, 400–01 (2012).

141. Kerr, *supra* note 23, at 1209–19.

142. *Id.*

143. United States v. Knotts, 460 U.S. 276, 284 (1983); *see also supra* section I.A.

A. Early Cases in Modern Fourth Amendment Jurisprudence Created Vital Doctrines for ECPA Analysis

Beginning in the 1960s, the Supreme Court revamped its Fourth Amendment jurisprudence, introducing new ideas and doctrines that have become integral to Fourth Amendment analysis in both the traditional and technological realm. In his concurrence to the 1967 decision in *Katz v. United States*,[144] Justice Harlan created the reasonable expectation of privacy test.[145] This standard examines whether an individual has an intent to manifest information as private, and whether society deems that expectation of privacy reasonable.[146] For example, society finds it much more reasonable that a person manifest an intent for privacy in a conversation within their home compared to on a public street. In *Katz*, the Court held that the Fourth Amendment protects people, not places, from unreasonable search and seizure.[147] Therefore, for the government to obtain information on an individual without obtaining a search warrant, the government must do so in a way that does not violate an individual's reasonable expectation of privacy.[148]

In *United States v. Miller*,[149] the Supreme Court developed a second key factor in Fourth Amendment doctrine: the third party doctrine.[150] The third party doctrine mandates that once a person voluntarily provides information to a third party, that person no longer has a reasonable expectation of privacy regarding the content of that information.[151] Importantly, ECPA has been described as "a

144. 389 U.S. 347 (1967).

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

146. *Id.*

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

148. *See id.* at 361 (Harlan, J., concurring).

149. 425 U.S. 435 (1976).

150. *Id.* at 443. The defendant was convicted of multiple federal offenses and argued that checks and other documents he had sent to banks were improperly admitted as evidence against him because he had an expectation of privacy under the Fourth Amendment. *Id.* The Court said the action was not improper under the Fourth Amendment's third party doctrine. *Id.* By providing the checks and documents to banks, he no longer had a reasonable expectation of privacy in those documents. *Id.*

151. *Id.*; *see also* United States v. White, 401 U.S. 745, 745 (1971) (concealed radio transmitter on an informant was not a violation of the Fourth Amendment); Hoffa v. United States, 385 U.S. 293, 294 (1966) (using an individual's statements he made with a government informer, even in private, did not violate the Fourth Amendment); Lopez v. United States, 373 U.S. 427, 427–30 (1963) (federal agent entering the defendant's office with consent while carrying a recording device was not a violation of the Fourth Amendment).

Congressional attempt at applying third party doctrine to electronic communications in storage with third parties."[152]

Additionally, the Supreme Court has established important limitations, such as requiring warrants, or the use of court orders to authorize searches, including those issued under section 2703(b) and extended under section 2705(b).[153] These warrant limitations are meant to ensure that magistrate judges act as more than just a rubber stamp and limit the ability of police to conduct ad hoc and questionable searches. Under the Fourth Amendment, a subpoena or warrant for government officials to conduct a search must be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[154] This court order requirement is also echoed in the language and application of ECPA.[155]

B. The Supreme Court Gives New Technology Varied Considerations Under the Fourth Amendment

Two seminal cases, *United States v. Karo*[156] and *United States v. Knotts*,[157] first established the traditional analysis for technology and the Fourth Amendment. Both cases dealt with whether the police could, without a warrant, attach a beeper to track the location of cans of chloroform[158] and ether,[159] respectively. In both cases, the Court drew a clear line regarding the application of Fourth Amendment principles to new technology: if visual surveillance would have provided the same information as high-tech surveillance, the new technology was not subject to new or different Fourth Amendment analysis.[160] Although the cans were each tracked for multiple days, in *Knotts* the Supreme Court found no search implicating the Fourth Amendment because the can was only tracked in public locations where there was no reasonable expectation of privacy, and where the police, hypothetically, could have

152. Oza, *supra* note 51, at 1054; *see also infra* section II.A.

153. Donovan v. Lone Steer, Inc., 464 U.S. 408, 415 (1984).

154. *Id.* (citing See v. City of Seattle, 387 U.S. 541 (1967)).

155. Electronic Communications Privacy Act, 18 U.S.C. § 2703 (2012). However, under ECPA, law enforcement agents may also receive a non-warrant court order to access third-party consumer information. *Id.*

156. 468 U.S. 705 (1984).

157. 460 U.S. 276 (1983).

158. *Id.* at 277.

159. *Karo*, 468 U.S. at 708.

160. *Id.* at 721; *Knotts*, 460 U.S. at 282.

tracked the individual with the naked eye.[161] In contrast, in *Karo*, the Court found there was a search.[162] In that case, the beeper tracked the can—and, therefore, the individual—to specific rooms inside a home.[163] Because the police would not have been able to gather that information through traditional surveillance methods, the court found the collection of that information violated an individual's reasonable expectation of privacy.[164]

Since *Karo* and *Knotts*, the Supreme Court's Fourth Amendment jurisprudence has expanded and modernized. Not only has the Court increasingly considered technological advances, but it has also considered the amount of information that modern devices have the capacity to collect—a clear departure from the analysis used in *Knotts* and *Karo*. In 2001, the Court first acknowledged the important relationship between technological advances and privacy protections.[165] In *Kyllo v. United States*,[166] the Court held a police department violated the Fourth Amendment when it used heat-sensing technology to see the contents of a home.[167] The Court reasoned that when the government used technology that significantly enhanced the ability of police to search a home without notice to the individuals inside, it violated the reasonable expectation of privacy test.[168] The type of technology and specific issues in *Kyllo* are distinct from the constitutional implications of Cloud-based storage. However, the case is instructive in its consideration of advancing technology in the realm of the Fourth Amendment because the Court gave deference to the power of technology: "[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[169] Furthermore, in *Kyllo*, the dissent discussed the importance of assuring individuals that advanced technology would not erode the Fourth Amendment protections first considered by the Founders.[170]

161. *Knotts*, 460 U.S. at 282.

162. *Karo*, 468 U.S. at 714–16.

163. *Id.*

164. *Id*.

165. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

166. 533 U.S. 27 (2001).

167. *Id.* at 34.

168. *Id.*

169. *Id.* at 28.

170. *Id.* at 46 (Stevens, J., dissenting); *see also* United States v. Jones, 565 U.S. 400, 405 (2012) (stating that the expansion of Fourth Amendment protections through the reasonable expectation of privacy test was unnecessary because the fundamental protection against governmental trespass had been violated).

The decision from *Kyllo* directs lower courts to engage in a technological analysis when considering Fourth Amendment protections.[171] During oral argument, Justice Stevens acknowledged the Court was hesitant to create precedent that would anticipate issues with future technological advances.[172] Additionally, in the opinion, majority-writer Justice Scalia recognized the inadequacy of using history to analogize to the modern use of technology when he held, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[173]

United States v. Jones[174] and *Riley v. California*[175] are two important, modern cases for analysis of ECPA. In both cases, the Justices were divided on how to reconcile technological advances and traditional Fourth Amendment doctrines.[176] The collection of aggregate information was a major issue in both cases.[177] Noted Fourth Amendment legal scholar Orin Kerr has dubbed this type of data collection Mosaic Theory.[178] Mosaic Theory is the idea that modern data collection involves the use of a significant number of data points to paint a detailed

171. *Kyllo*, 468 U.S. at 46.

172. Transcript of Oral Argument at 10, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-508), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2000/99-8508.pdf [https://perma.cc/THA4-9CV8]. When the appellant's lawyer suggested the Court should rule on what technology is capable of, Chief Justice Rehnquist responded, "I don't think you're correct in that. I think in a Fourth Amendment case we decide what was actually done, not what something is capable of." *Id.*

173. *Kyllo*, 533 U.S. at 33–34.

174. 565 U.S. 400 (2012) (the government suspected a man of running a drug ring and attached a GPS tracking device to the bottom of his wife's car, after its warrant authorization had expired, for four weeks to track him).

175. __ U.S. __, 134 S. Ct. 2473 (2014).

176. In *Jones* the Court unanimously held that the Fourth Amendment was violated. However, Justice Sotomayor and Justice Alito each wrote a concurrence hinging on the reasonable expectation of privacy test; Justice Alito's concurrence was joined by three other justices. *Jones*, 565 U.S. at 400 (majority opinion); *id.* at 413 (Sotomayor, J., concurring); *id.* at 418 (Alito, J., concurring). In *Riley*, the Court unanimously determined that the search of an individual's cell phone contents incident to arrest was an unconstitutional search. *Riley*, 134 S. Ct., at 2484–85.

177. *Jones*, 565 U.S. at 429 (Alito, J., concurring); *Riley*, 134 S. Ct. at 2489–91. Furthermore, in November 2017, during the oral argument in *Carpenter v. United States*, many of the questions posed by the Court seemed to reflect continued skepticism of immense data aggregation. For example, Justice Sotomayor went as far as to ask the government's attorney, "[h]ow would – would you like to lose?" *Supra* note 61, at 66.

178. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 311 (2012).

picture of an individual's life that would otherwise be protected in the traditional application and spirit of the Fourth Amendment.[179]

Riley consolidated two cases in which officers searched the cell phones of suspects without warrants and found information that ultimately led to each suspect being charged with serious crimes.[180] The Supreme Court held the warrantless search of cell phones was unconstitutional even under the relevant exceptions, such as search incident to arrest.[181] Departing from traditional Fourth Amendment application, the opinion relied heavily on the technological advances and immense data aggregated in cell phones.[182] The Court held, "[b]efore cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences."[183] The Court recognized that cell phones today are vastly different from other effects, those that would have been constitutional to search incident to arrest in earlier days (e.g., a pocket book someone was carrying at the time of arrest).[184] This is particularly true when the ability of cell phones to upload information into remote storage facilities makes them fundamentally different from traditional personal storage devices.[185]

Two years before *Riley*, the Supreme Court rejected the opportunity to explicitly analyze the government's collection of aggregate information using unprecedented technological advances in *United States v. Jones*. *Jones* dealt with a government actor who followed a suspect by attaching a device to the suspect's car and analyzing the Global Positioning System (GPS) data.[186] The Court's analysis hinged on an entirely distinct type of Fourth Amendment analysis separate from the reasonable expectation of privacy standard.[187] The majority did not engage in any reasonable expectation of privacy analysis, and instead determined the government acted unlawfully because attaching the GPS to the car was considered a trespassory search of property under the

179. *Id.* at 313.

180. *Riley*, 134 S. Ct. at 2480–82.

181. *Id.* at 2493. However, other warrant excepts may still apply. *Id.* at 2494.

182. *Id.* at 2489–91.

183. *Id.* at 2478.

184. *Id.* at 2490.

185. *Id.* at 2491.

186. United States v. Jones, 565 U.S. 400, 403 (2012).

187. *See id.* at 406–08 (relying on the Fourth Amendment trespass analysis, rather than reasonable expectation of privacy analysis).

Fourth Amendment.[188] In the majority opinion, Justice Scalia implied that when drafting the Fourth Amendment, the Founders had the capacity to address future scenarios that are based on rapid technological advancement.[189] This assertion directly contradicts Scalia's position in *Kyllo*.[190] The Court recognized that without the physical seizure, the reasonable expectation of privacy test would not have protected Jones, because it would have been acceptable for a police car to physically follow him around.[191] In rejecting the necessity of the reasonable expectation of privacy analysis, Justice Scalia did not consider advanced technology and instead compared the ability of a GPS device and data storage to that of an old-fashioned stakeout.[192] He refused to identify that the physical collection of data, traditionally done with the naked eye, and the electronic collection of aggregate data, using advanced technology, have different implications under the Fourth Amendment.[193] The majority opined,

> There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation . . . . We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had

188. *Id.* at 404–05.

189. *See id.* at 410–11 ("What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted." (emphasis in original)).

190. Kyllo v. United States, 533 U.S. 27, 34 (2001).

191. *Jones*, 565 U.S. at 412.

192. *Id.* at 411–12. Of this analysis and the concurrences' disdain of it, Scalia wrote:

> The concurrence faults our approach for "present[ing] particularly vexing problems" in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. We entirely fail to understand that point . . . even assuming, that the concurrence is correct to say that 'traditional surveillance' of Jones for a 4-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

Id. (emphasis omitted) (citations omitted).

193. *Id.*; *cf. id.* at 427 (Alito, J., concurring) (discussing the importance of recognizing technological advances in Fourth Amendment jurisprudence).

> to *Katz* analysis; but there is no reason for rushing forward to resolve them here.[194]

These seminal cases show the Supreme Court's inconsistency when considering the implications of the Fourth Amendment on new technology. The Court oscillates between acknowledging that the ease, convenience, and discreteness of collecting an aggregate amount of data, such as that in the Cloud, requires a different kind of analysis, and attempting to square traditional doctrines with new surveillance techniques.

C. *The* Jones *Concurrences Show Skepticism When Applying the Reasonable Expectation of Privacy Standard and Third Party Doctrine Standard to Modern Technology*

Although the *Jones* majority did not engage in a reasonable expectation of privacy analysis, both concurrences did and their reasoning shows a Court without a clear of idea of where to go next. In *Jones*, the two concurrences written by Justice Alito and Justice Sotomayor applied a reasonable expectation of privacy analysis and third party doctrine analysis to the attachment of the GPS device.[195] Furthermore, both Justices Alito and Sotomayor expressed concern over whether the Fourth Amendment doctrines provided adequate protection of digital data.[196] Both concurrences determined that collecting large amounts of information by attaching a GPS device to a person's car was an unconstitutional search.[197] Further, they determined it may have been a violation of an individual's reasonable expectation of privacy, even when the car was in a public place where an individual would not traditionally have a reasonable expectation of privacy.[198]

Justice Alito's concurrence, joined by three members of the Court, stated that the warrantless aggregate collection of data was unconstitutional.[199] But he did not explicitly address the boundaries of

---

194. *Id.* at 412–13.

195. *Id.* at 419 (Alito, J., concurring); *id.* at 416 (Sotomayor, J., concurring).

196. *Id.* at 420 (Alito, J., concurring); *id.* at 414 (Sotomayor, J., concurring).

197. *Id.* at 420 (Alito, J., concurring); *id.* at 414 (Sotomayor, J., concurring).

198. *Id.* at 420 (Alito, J., concurring); *id.* at 414 (Sotomayor, J., concurring); *cf.* United States v. Knotts, 460 U.S. 276, 282 (1983) (finding that an individual did not have a reasonable expectation of privacy when traveling on public roads).

199. *Jones*, 565 U.S. at 430 (Alito, J., concurring). In considering technological advances and the reasonable expectation of privacy, Justice Alito said it "rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in

collecting aggregate information. Rather, he determined that because the issue in *Jones* was clearly past that line, it was unnecessary to create those boundaries.[200] Justice Alito argued, "[w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[201] Justice Alito's analysis indicates that the constitutionality of the issue directly depends on the length of time of the surveillance.[202] His skepticism applying established doctrines to new technological capacities is echoed in his request that the legislature act. In his *Jones* concurrence, Justice Alito tipped his hat at the legislature's quick enactment of federal wiretap laps after the *Katz* decision established the reasonable expectation of privacy test: "Congress promptly enacted a comprehensive statute . . . and, since that time, the regulation of wiretapping has been governed primarily by statute and not by case law."[203] Justice Alito asked for a similar legislative response post-*Jones*.[204]

Justice Sotomayor's concurrence also briefly addressed the related privacy issues:

> I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year. . . . 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.[205]

Justice Sotomayor's opinion does not align with the third party doctrine as explained in *United States v. Miller*, where the Court held voluntary disclosure to a third party removes an individual's reasonable expectation of privacy.[206] Instead, her concurrence indicates the third party doctrine is not conducive to analyzing an individual's reasonable expectation of privacy in a modern age where a third party, such as an ISP, has collected and stored aggregate amounts of information.[207] The

---

which popular expectations are in flux and may ultimately produce significant changes in popular attitude." *Id.* at 427.

200. *Id.* at 430.

201. *Id.*

202. *Id.* at 430–31.

203. *Id.* at 427–28.

204. *Id.* at 429.

205. *Id.* at 418 (Sotomayor, J., concurring).

206. *Id.* at 417–18.

207. *Id.* at 417.

Jones concurrences show that the Court's application of traditional Fourth Amendment doctrines has logical limitations even without explicit, controlling action by the Supreme Court.

III. ANALYZING THE FAILURES OF ECPA AND A POSSIBLE SOLUTION FOR COURTS

Neither Fourth Amendment jurisprudence nor ECPA is equipped to regulate the constitutionality of government searches in a time when so much personal data is held in the Cloud.[208] Modern technology, particularly the Cloud, requires a new analysis because the way technology is used today is vastly different than how it's been used in earlier times. For example, while analogies may be drawn between the government's ability to intercept a letter and the government's ability to intercept an email, the comparison to letters fails to acknowledge the increasing ease with which parties can identify and locate specific pieces of data about specific individuals in the Cloud.[209] Tech companies continue to have increased capacity to store, aggregate, and locate specific consumer data.[210] As one commentator noted,

> What does all this mean in terms of the Fourth Amendment? It's simple: the technological and human factors that constrained the gathering and processing of data in the past are fast disappearing. Prior to these "advances," even the most ill-intentioned government urges to intrude on and do away with the privacy of citizens were held in check by the possible. The techno-gloves are now off and the possible is increasingly whatever an official or bureaucrat wants to do. That means violations of the Fourth Amendment are held in check only by the goodwill of the government, which might have qualified as the ultimate nightmare of those who wrote the Constitution.[211]

A. ECPA in Its Current Form Is Not the Answer

Although the original intent of ECPA—and of subsequent amendments to ECPA—was to bring privacy law into the digital age, it has largely failed to address the implications of technological advances

---

208. Peter Van Buren, *4 Ways the Fourth Amendment Won't Protect You Anymore*, MOTHERJONES (June 26, 2014, 9:44 PM), http://www.motherjones.com/politics/2014/06/how-fourth-amendment-not-protect [https://perma.cc/734J-P2NA].

209. *Id.*

210. *Id.*

211. *Id.*

and privacy protections in a way that provides adequate guidance for courts.[212] ECPA's language reflects the type of technology that was available in the 1980s when it was first enacted.[213] The massive leaps in technology between the 1980s and now goes without saying. Even at that time, ECPA was playing catch-up, trying to update the previous act to keep the relationship between law enforcement and private citizens modern in light of advancing technology.[214] ECPA is not only ill-equipped to address technological changes since its enactment, it is also incapable of addressing technological changes that are still to come.[215]

Technological inadequacies aside, the law also fails in other ways. Although ECPA was written to deal with electronic searches, it provides less protection than similar statutes that deal with physical searches.[216] While section 2705(b), guiding the use of indefinite gag orders, is just one provision of ECPA, it is vital because it regulates the fundamental warrant, consumer notification, and access requirements.[217] Microsoft's 2016 complaint challenging the government's use of ECPA's indefinite gag orders strongly highlights this dynamic when it identifies that ECPA section 2705(b) is different from physical search regulation statutes because the analogous physical search statute requires a notification of search within thirty days without indefinite gag orders.[218] Therefore, the

---

212. McMurry, *supra* note 25, at 598–99.

> While the ECPA represented significant progress for privacy general when it was passed in 1986, technology has continued to outpace the law. The ECPA was required to update the 1968 Act in order to preserve privacy rights in light of advances in technology. Similarly, the ECPA has been made less relevant and less effective due to subsequent advances in technology which have occurred even more rapidly [than] between the passage of the 1968 Act and the ECPA. Laws concerning privacy must be clear, easily applicable, and up-to-date so as to safeguard this valuable right. Because the ECPA has proven itself to be unclear and confusing, especially in light of advances in technology, it needs to be amended to promote privacy in an increasingly technological world.

Id. ECPA has been amended since this article was published but arguably not to the extent necessary to make McMurry's statement out-of-date.

213. Oza, *supra* note 51, at 1045.

214. McMurry, *supra* note 25, at 614.

215. Alyson Shontell, *The Next 20 Years Are Going to Make the Last 20 Look Like We Accomplished Nothing in Tech*, BUS. INSIDER (June 16, 2014, 2:54 PM), http://www.businessinsider.com/the-future-of-technology-will-pale-the-previous-20-years-2014-6 [https://perma.cc/E3JV-FBNS] ("[T]he next 20 years are going to make this last 20 years just pale . . . . We're just at the beginning of the beginning of all these kind of changes. There's a sense that all the big things have happened, but relatively speaking, nothing big has happened yet." (citing Kevin Kelly, founder of Wired)).

216. Grounds for Issuing Search Warrants, 18 U.S.C. § 3103 (2012).

217. Electronic Communications Privacy Act, 18 U.S.C. § 2705(b).

218. Complaint for Declaratory Judgment, *supra* note 9, at 8–9, 11. The statute that deals with physical searches requires a person whose documents are being searched to be notified within thirty

law provides government investigators with significantly more leeway (an extra two months of search time with significantly better search techniques) when searching an individual's digital rather than physical storage.

The recent changes to the laws affecting access to consumer data are a mixed bag. Taking the lead from the Department of Justice's new policy,[219] implementing limitations for indefinite gag orders as a statutory scheme is a good first step to cure ECPA's failures. Particularly through the indefinite gag order loophole, the Act provides fewer protections for consumers.[220] However, the introduction of the CLOUD Act[221] undermines ECPA and the newly implemented DOJ Policy. The CLOUD Act is ultimately a move backward. The recent and directly conflicting proposals for ECPA guidance from the federal government demonstrate how strongly comprehensive data protection reform is needed.

Compounding ECPA's shortcomings is the fact that technology typically evolves exponentially.[222] Using ECPA as a privacy protection in 2018 is akin to using a fax machine to send an email. Congress's lack of affirmative action enables lower courts to enact significantly different standards, particularly related to indefinite gag orders. This leaves the fundamental element of Fourth Amendment law—how data is collected—inadequately addressed. Congress's failure to enact comprehensive reform has left the door open for patchwork policies[223] and new laws[224] that conflict with each other and are peripheral to, but do not explicitly fix, the recognized problems with ECPA.[225]

---

days of the search happening. 18 U.S.C. § 3103a(b)(3). This statute permits limited exceptions under which that notification period can be extended. *Id.* § 3103a(c).

219. DOJ Memo, *supra* note 66.

220. 18 U.S.C. § 2705(b); Andrew Crocker & Nate Cardozo, *Here's How We're Fighting Back Against "Secret" Search Warrants*, ELEC. FRONTIER FOUND. (July 5, 2017), https://www.eff.org/deeplinks/2017/07/eff-access-now-cdt-and-oti-fight-back-against-secret-search-warrants [https://perma.cc/C7MR-HZMY].

221. Tom Krazit, *As Congress Considers the Tech-Backed CLOUD Act, Privacy and Human Rights Groups Raise Concerns*, GEEKWIRE (Mar. 18, 2018, 12:00 PM), https://www.geekwire.com/2018/congress-considers-tech-backed-cloud-act-privacy-human-rights-groups-raise-concerns/ [https://perma.cc/MNB3-U7V4].

222. Peter Diamandis, *Why Tech Is Accelerating*, HUFFPOST (Dec. 6, 2017), http://www.huffingtonpost.com/peter-diamandis/why-tech-is-accelerating_b_8951550.html [https://perma.cc/9Y2J-NKAC] (referring to the exponential evolution of technology as the Law of Accelerating Returns).

223. DOJ Memo, *supra* note 66.

224. Krazit, *supra* note 55.

225. Kerr, *supra* note 23, at 1214–16.

B. Courts Are Ill-Equipped to Draw Arbitrary Lines Related to Constitutional Provisions and Technology; the Legislature Must Act

Courts' inconsistent analysis and the differing outcomes applying section 2705(b) show that the statute is practically unworkable and inconsistently applied. The cases examined throughout this Comment[226] show that judges making these rulings are hyper-aware of public opinion and growing concerns over government surreptitiously accessing large swaths of consumer data. Without action by the legislature, courts are left without adequate tools to examine the constitutionality of ECPA in relation to the acquisition of extensive consumer data stored in the Cloud, and individuals are left with inconsistent search outcomes across jurisdictions. Throughout the Supreme Court's seminal cases on technology and the Fourth Amendment, the majority ping-pongs between failing to give technology special examination and recognizing that technology demands a distinct analysis with stronger Fourth Amendment protections.[227] This inconsistent analysis shows a larger fault in the Court's ability to understand and aptly apply technological differences.

While the majority in *Riley* based its decision on the Fourth Amendment implications of advances in technology, Justice Alito was not convinced the Court was the best entity to decipher the relationship between advanced technology and the Fourth Amendment. In his concurrence, Justice Alito said he would reevaluate the matter if Congress created "reasonable distinctions" relating to privacy and technology:[228] "I would reconsider the question presented here if either Congress or state legislatures . . . enact legislation . . . ."[229] Most recently, the government's brief in the *Carpenter* case reflects a similar sentiment:

> If Congress and state legislatures share petitioner's concern about the type and quantity of information collected by cell-service providers and other third parties, those legislators can pass laws to limit the collection, use, or dissemination of that data. Rather than distort or arbitrarily limit Fourth Amendment doctrine, "[i]n circumstances involving dramatic technological

226. *Supra* section I.B.; *supra* Part II.

227. Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2487–89 (2014); *cf.* United States v. Jones, 565 U.S. 400, 412 (2012); *supra* notes 156 to 194 and accompanying text.

228. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring).

229. *Id.*

> change, the best solution to privacy concerns may be legislative."[230]

The legislature is well-equipped to create comprehensive reform. First, the legislature can take input from concerned and affected parties and adjust its laws accordingly.[231] Second, it has the power to engage in extensive debate and listen to more voices.[232] The affected tech companies may have more impact on the Senate floor than the court room through lobbying efforts, particularly when the consumers have no idea they are subject to searches.[233] Third, it has the power to create laws based on policy, not just interpret them.[234] Taking into account diverse opinions and considerations is vital to enacting a complex statutory scheme, such as an ECPA update. This is something courts simply do not have the tools, time, or resources to do. Therefore, the legislature should govern the complex relationship between the Fourth Amendment and technology. It should not leave the courts to decipher a thirty-year-old statute ill-equipped to provide adequate guidance to courts, companies, and consumers.

This call to action has been echoed before. Academics,[235] judges,[236] lawyers[237] have all recognized the legislature as the right branch of government to reform ECPA and advocated it to do so. Indeed, Professor Orin Kerr provides a comprehensive guide to amending the statute.[238] In *Jones*, Justice Alito established that congressional response to courts issuing holdings about complicated areas of constitutional law was not without precedent. After *Katz*, the legislature acted. The same comprehensive legislative action must happen now. As written, ECPA's regulations do not adequately address societal expectations in 2018.

---

230. Brief for Respondent, *supra* note 62, at 31.

231. U.S. CONST. art. I.

232. *Id.*

233. Sarah Aitchison, *Tech Execs Fear Continuing Government Surveillance*, PUGET SOUND BUS. J. (Oct. 9, 2014, 12:43 PM), http://www.bizjournals.com/seattle/blog/techflash/2014/10/tech-execs-fear-continuing-government-surveillance.html [https://perma.cc/E8EQ-A5Y4].

234. U.S. CONST. art. I.

235. Kerr, *supra* note 23, at 1233.

236. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

237. Brief for Respondent, *supra* note 62, at 40 ("Ultimately, if the quantity of information now available in third-party business records raises novel privacy concerns, the proper body to address them is the legislature.").

238. Kerr, *supra* note 23, at 1233.

C. The Court Should Treat Digital Data as Fundamentally Distinct Rather than Drawing Attenuated Comparisons to Traditional Surveillance Techniques

Courts throughout the country are left in a predicament. As recent history has demonstrated, the judiciary is not the correct branch of government to create detailed and comprehensive rules relating to technology.[239] The legislature has also not provided adequate guidance for dealing with Cloud technology in the Fourth Amendment realm. As Professor Orin Kerr wrote,

> The SCA [ECPA] is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer networks. Unfortunately, some judges have had a difficult time realizing this, and have twisted the statute to do things it was never intended to do.[240]

If Congress fails to act on ECPA,[241] courts can still take some positive action, despite the problems outlined above. One solution could be for courts to explicitly acknowledge that technology deserves distinct analysis under the Fourth Amendment.[242]

Courts should first recognize that digital Cloud data is fundamentally different than any other type of data previously obtained by the government.[243] Following the trend established by the Sixth Circuit in *Warshak*, and as opined in *Riley*, the fundamental difference between the capacity of cell phones to store, search, aggregate, and analyze data, and the capacity of an individual to write down a few names in an address book illuminates the need for digital data to be analyzed differently.[244] The *Warshak* opinion lays out the fundamental distinction well:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based

---

239. *Supra* Part III.

240. Kerr, *supra* note 23, at 1214.

241. Devlin Barrett & Ellen Nakashima, *Texas Gunman's iPhone Could Reignite FBI-Apple Feud over Encryption*, WASH. POST (Nov. 8, 2017), https://www.washingtonpost.com/world/national-security/texas-gunmans-iphone-could-reignite-fbi-apple-feud-over-encryption/2017/11/08/0c2b3eb6-c48f-11e7-aae0-cb18a8c29c65_story.html?utm_term=.4206a64a887a [https://perma.cc/4NAH-DPB9] ("While FBI Director Christopher A. Wray has warned that there are nearly 7,000 phones that cannot be opened and said that such technologies are making it harder to fight terrorism and crime, Congress has shown little interest in tackling the issue.").

242. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

243. *See supra* section I.A.

244. Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2490–91 (2014).

> communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. . . . Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment.[245]

The use of the Cloud only increases that technological capacity and strengthens the argument for digital data to be treated differently under the Fourth Amendment.

Justice Alito has further alluded to this important distinction in his push to treat data different when collected in the aggregate compared to when collected as individual data points.[246] As Justice Alito stated in his *Jones* concurrence, "[f]or such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[247] The use of technology should not usurp this expectation of privacy, and courts should explicitly find Cloud data searches using advanced technology are fundamentally distinct from the searches of the past.

Justice Alito's sentiment, for example, directly relates to the use of indefinite gag orders under ECPA. Although indefinite gag orders cannot be directly compared to the issue in *Jones* because they require some level of judicial scrutiny and, in each scenario, the government acquired different kinds of information, the use of indefinite gag orders to obtain a continuous and significant amount of consumer data is exactly the type of concern Justice Alito addresses in his *Jones* concurrence.[248] Under Justice Alito's reasoning,[249] also echoed by Justice Sotomayor,[250] a limitation on the amount of data gathered through indefinite gag orders would be required under the Fourth Amendment. When the acquisition of nearly four weeks of individual

245. United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).

246. *Jones*, 565 U.S. at 429–30 (Alito, J., concurring).

247. *Id.* at 430.

248. *Id.*

249. *Id.*

250. *Id.* at 418 (Sotomayor, J., concurring).

location data is beyond the reasonable expectation for continuous acquisition,[251] nearly a year's worth of the information from an individual's ISP must also be beyond the limit, particularly when it was obtained without a warrant. Echoing concerns over the acquisition of significant amount of customer data obtained through indefinite gag orders and the desire to treat digital data differently, the Electronic Frontier Foundation has noted, "[t]here are strong arguments that Section 2705 nondisclosure orders are unconstitutional all or nearly all of the time."[252] Recognizing that digital data is fundamentally distinct from traditional forms of surveillance because of its unprecedented acquisition and storage capacity is vital if courts are to create outcomes consistent with the Fourth Amendment and across jurisdictions.

CONCLUSION

The tangled mess of ECPA and the Fourth Amendment provide inadequate guidance to lower courts on the government's ability to collect and disseminate consumer information stored in the Cloud by technology companies. Simply put, ECPA is antiquated when it comes to modern technology.[253] Neither the drafters of the Constitution nor the authors of ECPA had any way to know that nearly every individual in the United States would constantly carry a computer more powerful than those that launched the Apollo rockets[254] and then passively provide all that information to third parties without any affirmative action on the part of the consumer. Courts' inconsistent application of ECPA's indefinite gag order provision show they are not well-equipped to engage in technological analysis without up-to-date legislative tools.[255] The Supreme Court's Fourth Amendment jurisprudence fails to address the important technological and privacy issues that are becoming more commonplace.[256] Courts are left trying to cut through a Fourth Amendment fog with only outdated statutes and inconsistent jurisprudence to guide them. Comprehensive regulation of digital data searches should be the legislature's job.[257] In the meantime, courts

251. *Id.* at 430 (Alito, J., concurring).

252. Crocker & Cardozo, *supra* note 220.

253. *A Summary of the Electronic Communications Privacy Act (ECPA)*, *supra* note 39.

254. David Grossman, *How Do NASA's Apollo Computers Stack Up to an iPhone?*, POPULAR MECHS. (Mar. 13, 2017), https://www.popularmechanics.com/space/moon-mars/a25655/nasa-computer-iphone-comparison/ [https://perma.cc/BCJ2-LNVV].

255. *Jones*, 565 U.S. at 429–30 (Alito, J., concurring).

256. *Id.*

257. *Id.*

should at least recognize the fundamental difference in scope between collecting digital data and physical data—illustrated in *Riley v. California*[258] and *United States v. Warshak*[259]—when examining the validity of government entities gathering private citizens' data from third-party private companies.

258. __ U.S. __, 134 S. Ct. 2473, 2489–91 (2014).

259. 631 F.3d 266, 284–85 (6th Cir. 2010).