Fall 2016

Log in to Danger Zone: Data Privacy Under The SCA and Microsoft

Brian Tuinenga
Valparaiso University

LOG IN TO THE DANGER ZONE: DATA PRIVACY UNDER THE SCA AND *MICROSOFT*

I. INTRODUCTION

The year is 2018 and the United States government suspects Frank of operating "Velvet Boulevard," an elaborate and infamous black market hosted over the dark web.[1] Frank uses an email account and briefly visits the United States. During his trip, Microsoft migrated Frank's email data to a server in Chicago to decrease the time it takes him to access his emails. When Frank returned to his native land of Russia, his email data is again migrated, but Microsoft may retain some of his subscriber information in the United States. Assuming Microsoft re-migrates Frank's data, § 2703(d) of the Stored Communications Act ("SCA") empowers the government to effortlessly compel Microsoft, the Internet service provider ("ISP"), to hand over his stored non-content data no matter its location.[2] Furious

---

[1] This is a hypothetical scenario that is solely the work of the author. The facts of this situation closely parallel the facts from *In re* Warrant to Search, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) (holding the Stored Communications Act ("SCA") obligates domestic Internet service providers ("ISPs") to turn over to the government data located abroad on a Microsoft server). The government sought email data stored by Microsoft and linked to an unidentified individual's account in relation to a federal criminal investigation. *Id.* at 467–68. The government issued a warrant authorized by the SCA, compelling Microsoft to retrieve the data and surrender it to the government. *Id.* Microsoft moved to quash the warrant because the email data was located in Dublin, Ireland. *Id. But see* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016) (invalidating the warrant approved by the lower courts because the data was in Ireland); Joseph Cox, *Court Rules to Extradite Suspected Silk Road Admin from Ireland to the US*, MOTHERBOARD (Aug. 12, 2016), http://motherboard.vice.com/read/court-rules-to-extradite-suspected-silk-road-admin-from-ireland-to-the-us [https://perma.cc/25SY-EFTT] (alleging that the unnamed individual at the center of Microsoft is an operator of the notorious dark web organization known as Silk Road). Recently, an Irish court approved the individual's extradition to the United States. *Id.*

[2] *See* Stored Communications Act, 18 U.S.C. § 2703(d) (2012) (providing the requirements for a court order under the SCA). The statute states:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Id.

over the United States's data seizure, the Russian government refuses to honor the United States's extradition request.[3] After a failed covert operation by United States Special Forces to extract Frank from Moscow, Russia dispatches warships to Chinese waters. Within hours, the eyes of all humankind are upon what could be the beginning of the World War III. Though this is an unlikely situation, it exists as an example of a worst-case scenario when domestic law enforcement spills over into the international theatre.

Because Microsoft is already collecting all of Frank's data for advertisement purposes, the government's task to obtain that data is simple: obtain a SCA court order or subpoena.[4] A SCA court order or subpoena is unique because it allows the government and its agents to obtain the non-content data of wire or electronic communications related to a crime without physically traveling to the facility that houses the information.[5] This functionality is different from the traditional operation of a search warrant under the Federal Rules of Criminal Procedure ("F.R.C.P.") 41, which require the seized materials to be located in the district that the warrant is issued.[6] Despite the government's nascent ability to obtain data that is located abroad, the SCA does not expressly authorize extraterritorial application of its mechanisms.[7]

Further, SCA § 2703(d) ("§ 2703") empowers the government to compel disclosure of non-content user data without proving probable cause.[8] Along with email, the government may compel disclosure of any incidental records of stored electronic communication, including: bank and hospital records, information stored in the cloud, information transmitted via wearable health technology ("Fitbits"), or content

---

3 *See* In re *Warrant to Search,* 15 F. Supp. 3d at 477 (upholding a court order authorized by SCA § 2703(d) ("§ 2703") to compel disclosure of data controlled by Microsoft and stored in Ireland).

4 *See infra* Part II.B (detailing how the government compels disclosure by ISPs through mechanisms authorized in the SCA).

5 *See infra* Part II.B (examining the process by which the government obtains and executes a court order under § 2703(d)).

6 *See* FED. R. CRIM. P. 41(b)(1) ("[A] magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district . . . .").

7 *See infra* Part II.B (discussing the specific text of the SCA regarding territorial limits on jurisdiction and enforcement). Since *Microsoft* is a unique case involving extraterritorial implications of data privacy, future courts, especially those not within the Second Circuit, may choose to follow or ignore its principles. *Id.*

8 *See infra* Part II.B (providing a framework of the discreet mechanisms of § 2703 that assign a specific standard of proof required to compel disclosure of different amounts of customer data).

accessed by a child on the family tablet.[9] With the SCA, law enforcement agencies enjoy unbridled access to data shared by millions of individuals and stored by their ISPs on a daily basis.[10]

To fortify modern email privacy, this Note proposes an amendment to § 2703(d) to restrict the federal government's ability to compel disclosure from ISPs. First, Part II explores the history and the language of the SCA, the *Microsoft* case with respect to extraterritorial application and the reduced standard of proof, and the recently enacted California Electronic Communications Privacy Act ("CalECPA") by the California legislature in an attempt to cure the issues with the current SCA apparent in *Microsoft*.[11] Next, Part III examines the constitutional weaknesses of the SCA, assesses potential privacy issues users of stored communications may face following *Microsoft*, analyzes the strengths and weaknesses of the CalECPA, and proposes an amendment that integrates requirements from the CalECPA into § 2703(d).[12] Finally, Part IV recapitulates and concludes this Note.[13]

---

9 *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 366 (2015) (examining the scope of the SCA regarding real time and stored Google Chat and FaceTime data); Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables,* 103 GEO. L.J. 1641, 1644 (2015) (examining privacy concerns with data transmitted by products such as Apple Watch and Fitbit); Steven R. Morrison, *What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents,* 16 VA. J.L. & TECH. 253, 270 (2010) (concluding that ISPs may freely search and seize email data without being subject to the constitutional limitations imposed on the government); Ned Schultheis, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 662 (2015) (summarizing the corporate interests in cloud computing in the wake of *Microsoft*); Reema Shah, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L.J. 543, 553–54 (2015) (discussing that companies including Facebook and WhatsApp voiced concerns regarding the government's reach under the SCA).

10 *See* 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, 1211 (2004) [hereinafter Kerr, *User's Guide*] (noting that the government does not need to prove probable cause to compel disclosure of a wide array of data); Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 664 (2016) (noting that consumers today expect technology to resist modern surveillance techniques).

11 *See infra* Part III.B–D (expounding on the relationship between the Fourth Amendment, the SCA, *Microsoft*, and the California Electronic Communications Privacy Act ("CalECPA")).

12 *See infra* Part III.C (examining privacy issues resulting from *Microsoft* and potential solutions observable in the CalECPA).

13 *See infra* Part IV (concluding that constitutional considerations should be added to § 2703(d)).

II. BACKGROUND

How far the U.S. government's authority extends in bringing criminals to justice is often an issue of legal and scholarly debate.[14] Today, the government compels ISPs to disclose individual users' data under the authority of the SCA.[15] In 2014, the Southern District of New York attempted to compel Microsoft to disclose email data stored in Ireland under the SCA in *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corporation*.[16] Recently, the Second Circuit overturned the Southern District of New York in what is already being haled as a landmark ruling for data privacy.[17] Still, *Microsoft* sparked

---

[14] *See* TianRui Grp. Co. Ltd. v. Int'l Trade Comm'n, 661 F.3d 1322, 1337 (Fed. Cir. 2011) (finding the International Trade Commission ("ITC") had authority to regulate conduct concerning intellectual property occurring in China); Kerrilyn Russ, *On the Wrong Side of the Tracks: An Analysis of the U.S. Court of Appeals for the Federal Circuit's Non-Application of the Presumption against Extraterritoriality [*TianRui Grp. Co. v. Int'l Trade Comm'n*, 661 F.3d 132 (Fed. Cir. 2011)]*, 52 WASHBURN L.J. 685, 695–98 (2013) (examining *TianRui* and resultant arguments for and against limiting the reach of the government through the ITC); Viki Economides, TianRui Group Co. v. International Trade Commission*: The Dubious Status of Extraterritoriality and the Domestic Industry Requirement of Section 337*, 61 AM. U.L. REV. 1235, 1245 (2012) (cautioning extraterritorial application of the ITC's domestic regulatory authority due to international considerations).

[15] *See infra* Part II.B (summarizing the provisions of § 2703); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1566 (2004) (concluding the Wiretap Act, the Pen Register Statute, and the SCA all function similarly with respect to email by generally prohibiting unsanctioned disclosure of information while providing exceptions, such as compelling an ISP to turn over data related to a criminal investigation).

[16] *See* 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) (upholding the government's SCA warrant and requiring Microsoft to retrieve and surrender email content data in a storage facility in Dublin); *see also* Russell Hsiao, *Implications for the Future of Global Data Security and Privacy: The Territorial Application of the Stored Communications Act and the Microsoft Case*, 24 CATH. U.J.L. & TECH. 215, 240–41 (2015) (describing the potential global effects of *Microsoft* in that the United States and Ireland maintain a Mutual Legal Assistance Treaty ("MLAT") that normally governs international requests for persons or property).

[17] *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016) (concluding that Congress did not intend for the SCA's warrant provisions to apply extraterritorially); *see also* Jonathan Stempel, *Microsoft Wins Landmark Appeal over Seizure of Foreign Emails*, REUTERS (July 14, 2016), http://www.reuters.com/article/us-microsoft-usa-warrant-idUSKCN0ZU1RJ [https://perma.cc/X9Y4-HK4N] (framing the 3–0 decision by the 2nd Circuit Court of Appeals as a defeat for the Department of Justice ("DOJ") and a victory for privacy advocates and technology companies). Dozens of technology companies filed briefs leading up to the appeal, including Amazon, Apple, Cisco Systems, and CNN. *Id. See also* Sam Thielman, *US Cannot Force Microsoft to Hand over Emails Stored Abroad, Court Rules*, GUARDIAN (July 14, 2016), https://www.theguardian.com/technology/2016/jul/14/microsoft-emails-court-ruling-us-government [https://perma.cc/W9NJ-DDE7] (conveying the wishes of Brad Smith, president and chief legal counsel for Microsoft, that the ruling would usher in new legislative discussion of digital privacy). Smith stated, "[t]he U.S. government has a decision

discussion on both the government's territorial warrant authority according to F.R.C.P. 41 regarding searches and seizures and the appropriate standard of proof the government must show to compel disclosure of email data.[18] Against this backdrop, California enacted a state-specific analog to the Electronic Communications Privacy Act ("ECPA") in October of 2015, including a corresponding SCA signifying a shift in future laws governing a globally connected world.[19]

First, Part II.A discusses the geographic origins of the Fourth Amendment and the cases forming this framework.[20] Next, Part II.B offers an account of the legislative development of the SCA with regard to communications privacy.[21] Then, Part II.C explores two key cases that defined email privacy expectations pursuant to the SCA.[22] Finally, Part II.D presents recent legislation enacted by California in an attempt to resolve the lingering questions of data privacy under the SCA.[23]

---

to make: we can even [sic] spend the next two years arguing about a law that was passed thirty years ago, or we can talk about a law that is focused on the future." *Id.*

18 *See* U.S. CONST. amend. IV (restricting the government's ability to conduct searches and seizures on citizens). The Amendment mandates:

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

Id. See also FED. R. CRIM. P. 41(b)(1) ("[a] magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district . . ."); Joy L. Backer, *Stop Waiting on the World to Change: Compelled Disclosure of Email Content under the Stored Communications Act*, 48 SUFFOLK U. L. REV. 379, 397 (2015) (arguing the Supreme Court must rein in the authority of the SCA by requiring probable cause for all warrants seeking email correspondence).

19 *See* Larry Magid, *California Electronic Communications Privacy Act Protects Privacy AND Children*, HUFFINGTON POST (Sept. 8, 2015), http://www.huffingtonpost.com/larry-magid/california-electronic-com_b_8101848.html [https://perma.cc/4C2S-QQWS] (reporting the CalECPA strengthens privacy expectations of email users and helps further protect children from online abuse); *In Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communication Privacy Act into Law,* ACLU OF N. CAL. (Oct. 8, 2015), https://www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy [https://perma.cc/TSY8-R2P9] [hereinafter *Landmark*] (announcing the passage of CalECPA and its aim to secure data privacy for Californians); *see also* Jim Halpert & Michelle Anderson, *BNA Insights: State Privacy & Security Developments – Looking Back and Looking Ahead,* 20 ELECTRONIC COMM. L. REP. 8, 19 (2015) (examining the proposed CalECPA before its enactment and initial public reaction).

20 *See infra* Part II.A (introducing the origins of the Fourth Amendment).

21 *See infra* Part II.B (examining the SCA and its problematic provisions).

22 *See infra* Part II.C (summarizing *United States v. Warshak* and *Microsoft*).

23 *See infra* Part II.D (presenting the history and text of the CalECPA as a state statute focused primarily on individual privacy).

A. The Fourth Amendment in the Age of Data

Before the 1950s, courts primarily limited the protections of the Bill of Rights to apply only within the national and territorial borders.[24] Searches and seizures conducted by the government primarily concerned the physical world.[25] For example, in *Blackmer v. United States*, the government served a subpoena on a U.S. citizen living in Paris, France, compelling him to return to the United States to testify in relation to a criminal investigation.[26] Blackmer claimed because he was outside of United States jurisdiction, he was not subject to its laws or demands.[27] The Supreme Court found that because Blackmer retained U.S. citizenship, the United States retained jurisdiction over him.[28] *Blackmer* expanded the

---

[24] *See* United States v. Dorr, 23 S. Ct. 859, 864 (1900) (holding the constitutional right to a jury trial does not extend to non-U.S. citizens living in a territory acquired by the United States). The Court stated that citizens of the Philippines were entitled to basic individual rights "by inference and the general spirit of the Constitution," but not a right to a trial by jury. *Id. See also* Territory of Haw. v. Mankichi, 21 U.S. 787, 791 (1903) (finding the right to a habeas corpus hearing does not extend to inhabitants of the territory of Hawaii); *see also* Emlin McClain, *The Hawaiian Case*, 17 HARV. L. REV. 386, 387–88 (1904) (elaborating upon the distinctions between provisions of the Bill of Rights as applied to different classes of U.S. territories); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 292 (2015) [hereinafter Kerr, *Global Internet*] (describing the nexus between the geographic location of the individual or materials and the corresponding level of Fourth Amendment protection).

[25] *See Search*, BLACK'S LAW DICTIONARY 672 (10th ed. 2014) (categorizing a search as: "[a]n examination of a person's body, property, or other area that the person would reasonably be expected to consider as private, conducted by a law enforcement officer for the purpose of finding evidence of a crime"); *Seizure*, BLACK'S LAW DICTIONARY 678 (10th ed. 2014) (defining seizure as: "[t]he act or instance of taking possession of a person or property by legal right or process; esp. a . . . confiscation or arrest that may interfere with a person's reasonable expectation of privacy"); *see also* Amy E. Pope, *Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches*, 65 FLA. L. REV. 1917, 1919 (2013) (suggesting a rise in transactional organized crime led the government to blur the lines between territorial and extraterritorial searches under the Fourth Amendment); Backer, *supra* note 18, at 382 (noting the language of the Fourth Amendment focuses on physical intrusions similar to those imposed by British soldiers onto American colonists); Daskal, *supra* note 9, at 336 (laying out the foundation of the pre-Internet Fourth Amendment that relied heavily on the physical location of either the individual or materials to be searched); Kerr, *User's Guide*, *supra* note 10, at 1209 (discussing the Fourth Amendment's origination as a protection of the physical home).

[26] *See* 284 U.S. 421, 443 (1932) (upholding a contempt decree of a U.S. citizen for failing to return to the United States after being served a subpoena in France). The court noted the interaction between a U.S. court and one of its citizens involves only those two parties, even if the citizen is located in another country. *Id*. at 437.

[27] *See id.* at 436 (summarizing Blackmer's location-based argument).

[28] *See id.* (finding the government may look abroad to bring wrongdoers to justice but must do so in accordance with the Constitution); Ronald S. Betman & Jonathan R. Law, *The (Too) Long Arm of the S.E.C.: When a Foreign Employee of a U.S.-Based Multinational Financial Services Client is Threatened with a Subpoena*, 10 BERKELEY BUS. L.J. 1, 10 (2013) (positing

government's capability to regulate private activity occurring outside of the United States.[29] As demonstrated in *Blackmer*, geographic location dominated Fourth Amendment analyses before the creation of the Internet.[30] In 1967, the Court handed down another landmark decision in *Katz v. United States*, finding that the government must obtain a warrant supported by probable cause to conduct surveillance on a public telephone booth.[31] There, the government sought wiretap content linked to a particular telephone booth.[32] In his concurring opinion, Justice John Marshall Harlan advanced the "reasonable expectation of privacy" standard under the Fourth Amendment and articulated a two-prong test for determining whether the government must obtain a warrant before tapping a phone.[33]

---

individuals retain certain constitutional rights abroad because the government must still go through specific processes to compel an individual's return).

29 *See* Robert A. Leflar, *Extrastate Enforcement of Penal and Governmental Claims*, 46 HARV. L. REV. 193, 196 (1932) (describing the early rationales for pursuing criminals located beyond a nation's borders); Kevin A. Meehan, *The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. INTL. & COMP. L. REV. 345, 347 (2008) (citing the nation's ability to exert power over a citizen regardless of location as a prelude to early international Internet regulations).

30 *See Blackmer*, 284 U.S. at 438 (implementing geography as a key factor in determining whether U.S. courts retain jurisdiction over individuals); P. Sean Morris, *"War Crimes" against Privacy – the Jurisdiction of Data and International Law*, 17 J. HIGH TECH. L. 1, 36 (2016) (describing the jurisdictional debate in *Microsoft* as the clashing of two legal cultures); *see also* Kerr, *User's Guide*, *supra* note 10, at 1209 (connecting the right to privacy to the right to property in terms of the expectation against unreasonable intrusions). The most hallowed example of property is one's home. Kerr, *User's Guide*, *supra* note 10, at 1209. Because most property is tangible, an intrusion close in proximity to one's property results in a violation of one's personal privacy. *Id.*

31 *See* 389 U.S. 347, 359 (1967) (holding the Fourth Amendment protects the use of public pay phones); *see also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 35 (2004) (summarizing the thrust of *Katz* as a bright line test as to which communications are protected by the Constitution and which are not); *Katz v. United States*, OYEZ, https://www.oyez.org/cases/1967/35 [https://perma.cc/QWK8-MVE8] [hereinafter OYEZ] (showing *Katz* was a seven to one decision). Justice Thurgood Marshall did not participate in the arguments or ruling. OYEZ, *supra* note 31. *See generally* Johnathan Chait, *Will the Supreme Court Just Disappear?*, N.Y. MAG., (Feb. 21, 2016), http://nymag.com/daily/intelligencer/2016/02/will-the-supreme-court-just-disappear.html [https://perma.cc/YGG8-EGYW] (reporting Justice Antonin Scalia's vacant Supreme Court seat leaves many controversial cases in limbo, where even if the Court renders a decision, any controversial decision would result in a 4–4 stalemate). This result, in essence, negates the Supreme Court even rendering a decision at all. *Id.*

32 *See Katz*, 389 U.S. at 359 (summarizing the government's argument that wiretap surveillance involves no physical intrusion of the telephone booth, and thus, no constitutional concern). Responding to the fact that a telephone booth is a public area, the Court stated, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351.

33 *See id.* at 361 (Harlan, J., concurring) ("There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation

Despite the expectation of privacy advanced in *Katz*, exceptions to the Fourth Amendment, such as the third-party doctrine, allow warrantless government surveillance.[34] According to the third-party doctrine, the Fourth Amendment does not apply to information voluntarily disclosed to third parties if the third party in question has an independent, usually business, interest in receiving information from an individual.[35] In *Morrison v. National Australia Bank Limited*, the Supreme Court defined the territorial reach of third-party subpoenas and warrants.[36] In *Morrison*, the government sought documents controlled by National Australia Bank ("the Bank") under the authority of the Securities and Exchange Act.[37] The Bank moved to quash the subpoena because the Securities and Exchange Act ambiguously references extraterritorial application of its provisions.[38]

---

be one that society is prepared to recognize as 'reasonable.'"). Justice John Marshall Harlan noted that a telephone booth resembles a home for Fourth Amendment purposes, and that warrantless electronic surveillance may violate the Fourth Amendment. *Id. See also* Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125, 176–77 (2005) (applying the reasonable expectation of privacy advanced in *Katz* to Internet activity in the twenty-first century); Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 455 (2007) (examining Justice Harlan's concurrence from an originalist standpoint and describing when the government may justify an invasion of personal privacy); Dr. Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 569 (2013) (highlighting the second prong of the standard advanced by Justice Harlan and arguing society today believes email privacy is reasonable).

34 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 568–69 (2009) [hereinafter Kerr, *Third-Party*] (examining the origin of the third-party doctrine regarding undercover informants' use of concealed recording devices); Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. CIV. RTS. L.J. 255, 271 (2013) (summarizing arguments in favor of the third-party doctrine); *but see* Jace C. Gatewood, *It's Raining Katz and Jones: The Implications of* United States v. Jones*-A Case of Sound and Fury*, 33 PACE L. REV. 683, 712–13 (2013) (suggesting application of the third-party doctrine to electronic communications poses deep constitutional and policy concerns because a great deal of data is submitted unintentionally).

35 *See* Mulligan, *supra* note 15, at 1576–77 (discussing the basic principles behind the third-party doctrine as a means of obtaining an individual's business records voluntarily submitted to a third party, such as a bank); *see also* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third-Party Doctrine*, 96 IOWA L. REV. BULL. 39, 50 (2011) (suggesting courts recognize an exception to the third-party doctrine for online communications if the message is reasonably necessary to meaningfully participate in society).

36 *See* 561 U.S. 247, 269 (2010) (holding that the Securities and Exchange Commission may only regulate domestic transactions).

37 *See id.* at 250 (emphasizing the Bank was a foreign entity with no connection to the United States).

38 *See id.* at 268 (finding that based on the text and legislative history of a specific section of the Securities and Exchange Act, its provisions apply only to transactions occurring in the United States); Peta Spender & Michael Tarlowski, *Adventures on the Barbary Coast: Morrison and Enforcement in a Globalised Securities Market*, 35 MELB. U.L. REV. 280, 298 (2011) (critiquing

The Court denied the government's request for the documents and found that the "[t]he presumption against extraterritoriality prescribes when a statute gives no clear indication of an extraterritorial application, it has none."[39] The tradition of the third-party doctrine leaves uncertainty regarding what privacy assurances courts will extend to email and other data.[40]

Data is distinguishable from tangible objects in many ways.[41] User data can be hidden and the owner may be disguised using sophisticated codes from anywhere in the world.[42] The user can access emails without being anywhere near where that data is stored.[43] For example, unlike a post card, a single sent email generally exists in many locations at once.[44]

Morrison after balancing the importance of foreign and domestic matters between nations); Elizabeth A. Rowe & Daniel M. Mahfood, *Trade Secrets, Trade, and Extraterritoriality*, 66 ALA. L. REV. 63, 65 (2014) (approaching the challenges that corporations face when seeking judicial enforcement of court orders issued within the United States).

[39] *See Morrison*, 561 U.S. at 269 (finding the presumption against extraterritoriality necessary for resolving national and international disputes in an orderly manner). Courts are not to contrarily interpret statutes contemplated and passed by Congress. *Id. See also* S. Nathan Williams, *The Sometimes "Craven Watchdog": The Disparate Criminal-Civil Application of the Presumption against Extraterritoriality*, 63 DUKE L.J. 1381, 1398–99 (2014) (expanding on the presumption against extraterritoriality in civil and criminal contexts).

[40] *Compare* United States v. Maxwell, 45 M.J. 406, 418–19 (App. Armed Forces 1996) (holding that an individual enjoys Fourth Amendment protection of remotely stored America Online, Inc. ("AOL") emails and rejecting the required disclosure rationale), *with* Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001) (finding that defendant's emails and chat room activity did not have a reasonable expectation of privacy); *see also* Ryan Walsh, *Extraterritorial Confusion: The Complex Relationship Between Bowman and Morrison and a Revised Approach to Extraterritoriality*, 47 VAL. U. L. REV. 627, 642 (2013) [hereinafter Walsh, *Extraterritoriality*] (noticing a revival of the presumption against extraterritoriality and providing specific national security exceptions to protect the country in a complex global environment).

[41] *See* Sherry F. Colb, *What Is A Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 134 (2002) (discussing how public and private considerations factor into data's Fourth Amendment protection); David R. Johnson & David Post, *Law and Borders-the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1396–97 (1996) (examining the separation of subsidiary spheres or levels within the Internet).

[42] *See* Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 HARV. L. REV. 531, 551 (2005) [hereinafter Kerr, *Digital World*] (finding many investigators prefer to copy an individual's data via bitstream and review the copies rather than the originals).

[43] *See* Daskal, *supra* note 9, at 368 (describing the divisibility of data as both a convenience and a hazard for the individual user).

[44] *See* Schultheis, *supra* note 9, at 688 (stating the main enticement for cloud data storage is that it is accessible to the user anywhere Internet is available); *see also* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 344–45 (2002) (noting some states, California for example, regulate certain types of email transactions and tobacco advertisements); *but see* Kerr, *Digital World*, *supra* note 42, at 551 ("[A] search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer.").

Finally, law enforcement may search and seize data without physically traveling to a storage facility.[45] Scholars suggest updating the laws that govern third-party disclosure of personal electronic data to more realistically mirror the unique features of intangible data.[46]

Personal information transmitted via email, including bank and hospital records, traverses numerous third-party servers while being copied at each juncture.[47] Today, data transmitted while using Gmail or

---

[45] *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 200 (2d Cir. 2016) (stating the government attempted to compel disclosure of data located in Ireland); Jason Young Green, *Railing against Cyber Imperialism: Discussing the Issues Surrounding the Pending Appeal of* United States v. Microsoft Corp., 16 N.C. J.L. & TECH. ON. 172, 187–88 (2015) (discussing the hybrid nature of the SCA warrant initially granted in *Microsoft*); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 376 (2014) [hereinafter Kerr, *Next Generation*] (suggesting Congress enacted the Electronic Communication Privacy Act ("ECPA") in a time when data storage was expensive whereas today, ISPs may store the entirety of an individual's user data for a relatively low cost). Kerr claims this inversion led to mass storage of data which "renders [the] ECPA's structure exactly backwards for the operation of modern computer networks." Kerr, *Next Generation*, *supra* note 45, at 376.

[46] *See* Mulligan, *supra* note 15, at 1571 (summarizing the problems caused by the third-party doctrine within the SCA); *see also* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) [hereinafter Solove, *Codification*] (stating the third-party doctrine encompasses companies, like Amazon, that store troves of revealing user information). Solove further posits that courts are hesitant to stray from a narrow analysis as to whether particular law enforcement practices pose constitutional risks. *Id.* at 774. *See* Wei Chen Lin, *Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud, and Encryption*, 65 DEPAUL L. REV. 1093, 1127 (2016) (analyzing the arguments for and against strong encryption as a data privacy measure); *but see* Kerr, *Third-Party*, *supra* note 34, at 573 (arguing the third-party doctrine maintains the technological neutrality of the Fourth Amendment).

[47] *See* Simon M. Baker, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered its Protections Obsolete*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 75, 103–104 (2011) (predicting how recent court decisions treating opened emails will affect Facebook and MySpace messages as in remote storage); Eric R. Hinz, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 493 (2012) (offering an example of early problems with the term storage when a hospital wishes to keep a copy of some electronic data for back-up purposes, but does not consider that data in storage). While the individual may wish for this information to remain private, the third-party doctrine removes any expectation of privacy. *Id. See also* Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 SAINT THOMAS L. REV. 169, 240 (2012) [hereinafter Walsh, *Mosaic*] (suggesting Congress enacted the SCA at least in part to counteract increasing government collection of personal data). Today, because the government is capable of numerous and distinct forms of surveillance, the data from each of these forms may be aggregated into one singular account, much like a mosaic in the world of art. *Id.* at 173. If the government does collect a mosaic of information, the Fourth Amendment protects that information. *Id.*

Facebook is also generally subject to the third-party doctrine.[48] The sum of an individual's data usage across all of these services give the investigator a "mosaic" of private information.[49] Individuals consider their personal information as private, not just to other individuals, but also to the government.[50] Data's quirks, even in 1986, led Congress to create a basic framework of Fourth Amendment protections.[51]

B. Enactment of the SCA as Part of the ECPA

Initial widespread use of the Internet began with businesses using desktop or laptop computers connected to private servers.[52] Yet, outside the office, few people accessed the Internet for non-business reasons or even owned personal computers during this time.[53] In short, personal

---

[48] *See* Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1445 (2015) (discussing the common email and social media services used today that are subject to the third-party doctrine); Daniel Shickich, *What Your Tweet Doesn't Say: Twitter, Non-Content Data, and the Stored Communications Act*, 8 WASH. J.L. TECH. & ARTS 457, 461 (2013) (analyzing privacy expectations when the user completes a clickwrap consent form before utilizing Internet services).

[49] *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) ("In 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."); *see also* Walsh, *Mosaic*, *supra* note 47, at 173 (describing the government's surveillance capabilities when aggregating data across services).

[50] *See* Hinz, *supra* note 47, at 489 (introducing privacy concerns from the standpoint of an investigation involving the Detroit police department and mayor following the police shooting of Tamara Greene in 2003); Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 460 (2013) (suggesting data privacy laws should be narrowly tailored to fit specific circumstances and predicting reduced privacy expectations for data stored in the cloud).

[51] *See supra* Part II.B (examining the legislative response to slowly increasing Internet use during the time Congress contemplated the SCA).

[52] *See* Courtney M. Bowman, *A Way Forward after Warshak: Fourth Amendment Protections for E-Mail*, 27 BERKELEY TECH. L.J. 809, 825 (2012) (arguing that the SCA was crafted as a bill to protect a business convenience, not personal privacy considerations); Sasha Segall, *Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105, 1115 (2013) (stating that numerous ISPs today operate storage facilities outside of the United States); *see also* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 584 (2011) (examining early government use of bank and telephone company records); Mulligan, *supra* note 15, at 1560 (discussing that few individuals had home access to the Internet in the 1980s because personal computers were large and expensive). Those that did have access to personal computers had minimal options when seeking ISPs. Mulligan, *supra* note 15, at 1560; Kerr, *Global Internet*, *supra* note 24, at 287 (noting initial Internet use in the United States was primarily domestic).

[53] *See* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy under the Stored Communications Act*, 98 GEO. L.J. 1195, 1197 (2010) (revealing that an IBM mainframe cost $12 million in 1970); Schultheis, *supra* note 9, at 666–67 (reporting fourteen percent of Americans

Internet usage in 1986 pales in comparison to today.[54] Despite its minimal usage, individuals and civil rights groups quickly began to voice Internet privacy concerns.[55] Because the Fourth Amendment protects "people, not places," legislators were at odds in determining whether stored electronic communications should be afforded the same reasonable expectation of privacy as a telephone booth.[56] Particularly, legislators examined extending the government's reach beyond the United States's borders.[57]

---

used the Internet in 1995, while sixty-six percent of Americans used the Internet in 2005, and eighty-seven percent of Americans used the Internet in 2014).

54 *See* Terri A. Cutrera, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 141 (1991) (marking a sharp increase in hacking activity as computer and communications technologies progressed); Robert W. Kastenmeier et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 718 (1989) (enumerating available communications technologies, such as cordless telephones, paging devices, and miniature cameras). The government wished to protect these communications while providing certain exceptions for when the ISP may be subject to disclosure. *Id.* at 719. *See* Aaron Smith, *15% of American Adults Have Used Online Dating Sites or Mobile Dating Apps*, PEW RES. CTR. (Feb. 11, 2016), http://www.pewinternet.org/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/ [https://perma.cc/7Q3W-PYE7] (reporting that usage by eighteen to twenty-four year olds has increased nearly 300% since 2013). Usage of dating sites or mobile dating apps for fifty-five to sixty-four year olds has doubled. *Id.*

55 *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1274 (2004) [hereinafter Solove, *Surveillance Law*] (mentioning the government used COINTELPRO, an early surveillance program operated with minimal oversight, on Civil Rights activists who demanded, among other things, individual privacy); Mulligan, *supra* note 15, at 1561–62 (explaining that before the SCA, stored communications were not protected by any federal legislation).

56 *See* Katz v. United States, 389 U.S. 347, 352 (1967) (defining the scope of the Fourth Amendment in terms of telephone communications); S. Rep. No. 99-541, at 5 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555 ("Most importantly, the law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment."); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1609–10 (2003) [hereinafter Kerr, *Cybercrime*] (distinguishing the process of identifying property rights of tangible materials to assigning property rights to intangible data); *but see* Kerr, *User's Guide*, *supra* note 10, at 1209 (explaining email data is traditionally stored on the premises of the ISP and not within the home or physical control of the individual). Individual users may believe stored emails to be part of their virtual home, but those messages are stored on the premises of the ISP. Kerr, *User's Guide*, *supra* note 10, at 1209. *See also* Solove, *Surveillance Law*, *supra* note 55, at 1270–71 (noting the surveillance of telegraph communications as a guide when Congress contemplated applying the Fourth Amendment to online correspondence).

57 *See* H.R. Rep. 99–647, at 32–33 (1986) (denying extraterritorial application of the SCA to seize data located outside the territorial United States). The report reflects:

> By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example it . . . regulates only those "interceptions" conducted within the territorial United States. Similarly, the controls in [Section 2703]

Ultimately, Congress sought to ensure basic privacy rights of individuals using electronic communication by enacting the SCA as a subordinate title of the ECPA.[58]

Three main titles comprise the ECPA: the Wiretap Act, the Pen Register Statute, and the SCA.[59] The Wiretap Act oversees the collection of content data whereas the Pen Register Statute applies to non-content data.[60] The Wiretap Act and Pen Register Statute enable the government to intercept email content in real time.[61] Based on how the data is transmitted, § 2703 splits all stored communications data into two categories: electronic communication services ("ECS") and remote computing services ("RCS").[62] Section 2703(a) pertains to the disclosure of ECS data while § 2703(b) applies to RCS data.[63] An individual uses ECS

> regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States.

Id.

58 *See* Kerr, *Next Generation*, *supra* note 45, at 384 (positing in the 1980s, Congress focused on protecting content rather than non-content data). Unopened messages stored less than 180 days received the highest protection while non-content received minimal consideration. *Id.* at 384–85. *See also* Kerr, *Cybercrime*, *supra* note 56, at 1602–03 (offering early court cases involving government requests for individual user data primarily involved child pornography).

59 *See generally* Wiretap Act, 18 U.S.C. § 2511 (2012) (authorizing collection of content data in criminal investigations); Pen Register Statute, 18 U.S.C. § 3122 (2012) (permitting disclosure of non-content communications in relation to an "ongoing criminal investigation" conducted by a governmental agency); § 2703 (allowing compelled disclosure of stored communications data).

60 *See In re* Warrant to Search, 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014) (informing the subject and body of an email message comprises content data while the addressee, time sent, sender location, and other logistical information comprise non-content email data). Because the Wiretap Act authorizes real-time surveillance, a much more detailed warrant is required than under the SCA. *Id.* at 469. The distinction blurs between what statute a given search warrant, subpoena, or court order falls under when the government wishes to conduct multiple forms of surveillance. *Id.*

61 *See* Kerr, *Next Generation*, *supra* note 45, at 376 (stating the majority of privacy protections established in the ECPA were aimed at real-time surveillance). When Congress enacted the ECPA, the government primarily conducted surveillance in real-time and rarely seized stored information, while today the opposite is true. *Id.*

62 *See generally* § 2703(a) ("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 . . . ."); § 2703(b) ("A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . .").

63 *See* § 2703(a) (describing the 180-day time limit); § 2703(b) (allowing compelled disclosure of stored data); *see also* People v. Harris, 949 N.Y.S.2d 590, 596 (N.Y. Crim. Ct. 2012) (finding that Twitter is primarily an electronic communication service ("ECS") provider, and records associated with a Twitter account are subject to subpoena according to the SCA); *In re* United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) (categorizing stored emails as data under control of a remote computing service ("RCS") provider for the

when sending and receiving emails and uses RCS to store messages once they are opened.[64] The type of service provided and whether the data has been in storage for more than 180 days determines what mechanism the government must employ to compel disclosure under § 2703.[65]

Section 2703 erects a tapering system controlling the conditions under which ISPs must disclose data to the government.[66] First, the government may seek basic user and transactional information with an administrative subpoena authorized by § 2703(c).[67] Second, non-content records may be obtained by a court order found in § 2703(d).[68] To obtain this court order, the government must demonstrate "specific and articulable facts" showing there are "reasonable grounds to believe" that the information in question is "relevant and material to an ongoing criminal investigation" rather than probable cause.[69] Also according to § 2703(d), the government

---

purposes of determining the appropriate mechanism to employ under the SCA); Hinz, *supra* note 47, at 515 (mentioning many interfaces today combine ECS and RCS services, making classification of messages difficult). Hinz offers the example of two professors collaborating on a single document saved in Dropbox. Hinz, *supra* note 47, at 515. The professors each use a RCS to store the document and an ECS to make edits over the Internet. *Id.*

64 *See* Hinz, *supra* note 47, at 496 (establishing the process of sending and receiving an email involves electronic computing services while remote computing services store the message once the message is read and stored).

65 *See* Backer, *supra* note 18, at 390 (stating the greatest level of protection available is for electronic communications stored in an ECS for less than 180 days); *see also* Hinz, *supra* note 47, at 496 (explaining since the SCA only distinguishes between ECS and RCS providers despite numerous technological advances since 1986, courts must determine what type of service requires what level of privacy protection on a case by case basis). An ISP may offer both ECS and RCS services, so while during an exchange the ISP may stay the same, the legal requirements of that ISPs conduct in handling data change when the nature of the service switches from ECS to RCS. Hinz, *supra* note 47, at 496. For example, per the SCA, ISPs may not voluntarily disclose ECS data to other parties at any time; whereas, ISPs are prohibited from disclosing RCS data only if that ISP is not allowed to access the communication for reasons other than storage and processing. *Id.*

66 *See generally* § 2703 (creating three tiers of data available via disclosure under the SCA); *see also* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 207–08 (2d Cir. 2016) (summarizing the methods by which the government may compel disclosure of minimally distinct types of data under the SCA).

67 *See* § 2703(c)(1)(a) (requiring an ISP to disclose "a record or other information pertaining to a subscriber to or customer of such service . . . only when the governmental entity: obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . .").

68 *See* § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued . . . if the governmental entity offers specific and articulable facts showing that . . . the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.").

69 *See id.* (enumerating the specific and articulable facts standard); *see also* Kaitlin G. Klamann, *Show Me the Warrant: Protection of Stored Electronic Communications in New York State*, 41 FORDHAM URB. L.J. 1407, 1422 (2014) (explaining that the distinctions found in the

may seek some user content with a subpoena under § 2703(c)(2) or a § 2703(d) order provided the government gives notice to the ISP's customer.[70] Finally, the government may obtain "priority stored communications"—stored communications held by the ISP for less than 180 days and stored communications in storage for more than 180 days—the government must prove probable cause and obtain a search warrant authorized by § 2703(a), unless the government is seeking data older than 180 days and provides notice to the customer.[71]

Warrants authorized by § 2703(a) are subject to the F.R.C.P., while subpoenas and court orders found in §§ 2703(b) and 2703(c) are not.[72]

SCA turn on the type of service provider and the status of the data, i.e., whether an email has been opened); Backer, *supra* note 18, at 399 (criticizing the specific and articulable facts standard); Schultheis, *supra* note 9, at 669 (citing limited distinctions between the function of an SCA warrant and an ordinary subpoena).

[70] *See* § 2703(b)(1) (allowing disclosure with or without notice to the customer). The statute states:

> A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . without required notice to the subscriber or customer . . . or with prior notice from the governmental entity to the subscriber or customer if the governmental entity: uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena[.]

Id. See also § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued . . . if the governmental entity offers specific and articulable facts showing that . . . the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.").

[71] *See* § 2703(a) (providing the warrant provision of the SCA's disclosure capabilities). The statute states:

> 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.

Id. See § 2703(b)(1)(B)(i) ("A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . without required notice to the subscriber or customer . . . ."); *Microsoft Corp.*, 829 F.3d at 207 (summarizing binary relationship between content and non-content stored data).

[72] *See Microsoft Corp.*, 829 F.3d 197, at 222 (requiring the warrant to comply with the traditional notions of the Federal Rules of Criminal Procedure); § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued . . . if the governmental entity offers

Generally, warrants are subject to more geographic limitations than subpoenas and court orders.[73] In short, SCA subpoenas and court orders are usually served via fax on the ISP, thereby creating a legal duty upon the ISP to surrender the requested data to the government, eliminating the need for an agent to ever step foot on the premises of the storage facility.[74] The SCA, while generally applicable to all stored data, does not authorize extraterritorial application of any of its mechanisms that compel disclosure.[75] However, a plain text reading of the statute does not readily answer whether court orders issued under § 2703(d) are also subject to the Federal Rules, and therefore, a review of relevant case law is in order.[76]

C. Warshak *and* Microsoft

Before the Internet connected the world, Fourth Amendment questions primarily involved geographic considerations.[77] Cases involving the required disclosure of email data authorized by extraterritorial application of the SCA are remarkably scarce.[78] In 2010,

---

specific and articulable facts showing that . . . the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."); *see also* § 2703(b)(1)(B)(i) (allowing the government to "require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . without required notice to the subscriber or customer . . . or with prior notice from the governmental entity . . . .").

73 *See Microsoft Corp.*, 829 F.3d at 210 (following the presumption against extraterritoriality advanced in *Morrison*).

74 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 471 (declaring SCA orders function more like subpoenas than traditional search warrants).

75 *See generally* § 2703(a) ("A governmental entity may require the disclosure . . . of the contents . . . in electronic storage . . . ."); In re *Warrant to Search*, 15 F. Supp. 3d at 468 (finding that § 2703 applies to the communications services Microsoft provides).

76 *See* § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued . . . if the governmental entity offers specific and articulable facts showing that . . . the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."); *Microsoft Corp.*, 829 F.3d at 214 (stating ordinary subpoenas may require production of materials located abroad). Warrants and subpoenas are separate legal instruments. *Microsoft Corp.*, 829 F.3d at 214. The warrant in *Microsoft* cited § 2703(a), not § 2703(d), making it a SCA warrant, not a court order or subpoena. *Id.* at 200.

77 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 476 (reviewing case law utilizing territorial analyses); Andrew Tyler Ohlert, *Appealing to Reason-able Expectations of Privacy: Increasing Appellate Review under ECPA*, 66 HASTINGS L.J. 1731, 1746 (2015) (finding that generally very few cases examine the SCA or ECPA). Many forms of modern surveillance are conducted in secret and this threatens the legitimacy of judicial review. Ohlert, *supra* note 77, at 1746.

78 *See* State v. Rose, 330 P.3d 680, 688 (Or. App. 2014) (upholding a SCA court order to compel the ISP to surrender the email data located in California). In *Rose*, Oregon law enforcement officials sought to enforce a state-issued search warrant to seize email data located in California in relation to a child pornography investigation. *Id.* at 682. While the warrant was not issued under authority of the SCA, the court mentions the Act in relation to whether a state court may issue an order similar to a § 2703(d) court order. *Id.* at 684. Because

however, the Sixth Circuit Court of Appeals held in *United States v. Warshak*, that the government violated the Fourth Amendment by compelling an ISP to produce email data without first obtaining a warrant.[79] In *Warshak*, the government moved to present email data seized under the SCA as evidence in relation to a fraud investigation.[80] Warshak moved to quash the motion because the government seized the data without first satisfying the Fourth Amendment probable cause requirement.[81] The court likened an ISP to a post office or telephone company, and thus, the government was otherwise forbidden from unwarranted snooping on an individual.[82] *Warshak* held § 2703(d) was unconstitutional because it allows disclosure of email data without requiring probable cause.[83] Generally, the standard of proof that the government is required to show increases from reasonable suspicion to probable cause based on a general balancing test between law and order

---

an Oregon statute created a mechanism for the process of interstate warrants similar to the SCA, the court upheld the warrant and compelled the ISP to retrieve the data from California. *Id.* at 686. In upholding the warrant, the court noted that the warrant under Oregon law was sufficiently particular. *Id.* at 688. *See also* Mark Wilson, Comment, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U.L. REV. 261, 277 (2013) (demonstrating that electronic storage is an uncertain term).

79 *See* 631 F.3d 266, 288 (6th Cir. 2010) (holding the Fourth Amendment applies to email correspondence); *see also* Bowman, *supra* note 52, at 835 (arguing that the language of the SCA coupled with loose judicial interpretation thereof lead to unconstitutional application of the SCA).

80 *See Warshak*, 631 F.3d at 290–91 (describing the investigation and the compelled disclosure by the email provider NuVox).

81 *See id.* at 283–84 (summarizing Warshak's constitutional defense that email communications are private).

82 *See id.* at 286 (discussing the similarities between an ISP and a post office or telephone company and the constitutional protections thereof). While technically a third party, the court distinguished an ISP from a bank in *Miller* because a bank is an intended recipient, while an ISP is merely an intermediary. *Id.* at 288. *See also* Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 549, 555 (2013) (utilizing a formula for privacy invasions similar to the Learned Hand Balancing test involving negligence).

83 *See Warshak*, 631 F.3d at 290 (concluding that the SCA violates the Fourth Amendment, but electing not to reverse the lower court's conviction of Warshak due to harmless error).

and the individual's right to privacy.[84] This expectation of privacy found in *Warshak*, however, is only binding law within the Sixth Circuit.[85]

Microsoft catalyzed the debate of the government's territorial reach of stored data in criminal investigations and elevated the issue to the world stage.[86] In *Microsoft,* the Department of Justice ("DOJ") petitioned for and received a warrant authorized by § 2703(a) to obtain email data linked to an unnamed individual under the control of Microsoft in relation to an ongoing narcotics investigation in December 2013.[87] Microsoft moved to quash the warrant, claiming that the authority of the SCA does not extend

---

[84] *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that granting SCA warrants to collect cell site location information ("CSLI") based on the reasonable and articulable facts standard is not per se unconstitutional under the third-party doctrine); *In re* Application of U.S., 733 F. Supp. 2d 939, 943 (N.D. Ill. 2009) (requiring a showing of probable cause for a warrant to obtain CSLI); *In re* U.S. for Orders Authorizing Installation and Use, 416 F. Supp. 2d 390, 396–97 (D. Md. 2006) (holding that probable cause was required for pen register data because non-content data can amount to location tracking similar to GPS). The government requested pen register data that may be used to determine an individual's past location using cellular tower triangulation. In re *U.S. for Orders Authorizing Installation and Use*, 416 F. Supp. 2d at 392. The court then cryptically mused the hybrid authority of the SCA warrant is "at best murky and, at worst, illusory." *Id.* at 396. *See generally* Daniel Solove, *How Justice Scalia Defended Your Digital Privacy—and Also Held It Back*, VICE NEWS (Feb. 16, 2016), http://motherboard.vice.com/read/justice-scalia-digital-privacy-and-the-third-party-doctrine [https://perma.cc/2QZK-Q4M3] [hereinafter Solove, *Justice Scalia*] (positing as a constitutional originalist, Justice Scalia believed that GPS tracking constituted a search, while disclosure of third-party data did not).

[85] *See* Backer, *supra* note 18, at 392 (stating that Warshak appealed to the Sixth Circuit); *see also* Bowman, *supra* note 52, at 820 (summarizing constitutional considerations for not requiring probable cause to require disclosure of emails stored more than 180 days).

[86] Stempel, *supra* note 17 (hailing the *Microsoft* appeal as a "landmark" victory for privacy advocates).

[87] *See In re* Warrant to Search, 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014) (identifying the type of warrant in question as authorized by § 2703(a) of the SCA). The court likened this warrant to a subpoena and found the government may compel disclosure of the data located in Dublin. *Id.* at 472. *But see* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 230 (2d Cir. 2016) (Lynch, concurring) (noting on appeal that the nationality of the suspect—under investigation and tied to the relevant email account—was unknown). Further, those that are not U.S. citizens, or U.S. citizens that claim they reside outside of the United States, stand to gain the most from the majority ruling. *Id.* at 224. Since the government could never compel Microsoft to disclose data located abroad, those individuals received an "absolute" protection. *Id. See also* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 781 (2016) (discussing the interests of foreign governments if the tables were turned in a future Microsoft scenario). Woods argues that U.S. ISPs should be allowed to disclose data stored in the United States and linked to a non-U.S. citizen to a foreign government under specific conditions. *Id. But see* Cox, *supra* note 1 (noting that many suspect the individual at the center of the Microsoft dispute to be an operator of Silk Road, a black market available on the dark web).

beyond the United States's territorial borders.[88] The DOJ claimed that the function of the SCA warrant did not involve extraterritorial searches or seizures.[89] The United States District Court for the Southern District of New York upheld the warrant and ordered Microsoft to disclose the enumerated email data in August of 2014.[90] In July of 2016, the Second Circuit overturned the decision upholding extraterritorial application of the warrant.[91]

On appeal, *Microsoft* strictly followed the *Morrison* doctrine against extraterritoriality and invalidated the warrant.[92] In doing so, the court determined the "Act's privacy provisions were its impetus and focus" and that the needs of law enforcement were not the "primary motivator for the enactment."[93] Also, the court directed the government to adhere to the

---

88 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 470 (conveying Microsoft's argument that the presumption against extraterritoriality prohibits courts from applying the SCA outside of U.S. borders).

89 *See id.* at 470 (concluding the debate centers around whether a search takes place with SCA warrants).

90 *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624, at *8 (S.D.N.Y. 2014) (upholding the SCA warrant on appeal and providing minimal further analysis on the issues of probable cause or extraterritoriality); Sam Thielman, *Microsoft Case: DOJ Says It Can Demand Every Email from Any U.S.-Based Provider*, GUARDIAN (Sept. 9, 2015), http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant [https://perma.cc/RK3T-U6WN] [hereinafter Thielman, *Microsoft Case*] (acknowledging that the Department of Justice ("DOJ") contends the emails in question resemble business records subject to disclosure under the third-party doctrine).

91 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016) (finding that Congress did not endorse extraterritorial application of SCA warrants); Stempel, *supra* note 17 (detailing the reversal of the SCA warrant in *Microsoft*). Before the appellate decision, Microsoft warned that upholding the warrant could "spark a global 'free-for-all' that would . . . [prompt] law enforcement authorities elsewhere [to] seize emails belonging to Americans and stored in the United States." Stempel, *supra* note 17. *See also* Lindsay La Marca, Note, *I Got 99 Problems and a Warrant Is One: How Current Interpretations of the Stored Communications Act Offend International Comity*, 44 HOFSTRA L. REV. 971, 995 (2016) (arguing that courts should look to the physical location of the data in determining whether the government may compel disclosure); Alexander Dugas Battey Jr., *A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act*, 42 RUTGERS COMPUTER & TECH. L.J. 262, 292–93 (2016) (suggesting the warrant requirement found in the Law Enforcement Access to Data Stored Abroad ("LEADS") Act to be incorporated into the SCA).

92 *See Microsoft Corp.*, 829 F.3d 197, at 210 (following the two-pronged test in *Morrison* wherein the court first decides "whether the relevant statutory provisions contemplate extraterritorial application"). Second, if the court finds that the provision does not consider extraterritorial application, the court then decides if the challenged conduct qualifies as "extraterritorial." *Id.* If the conduct is extraterritorial, it is outside the bounds of the statute. *Id.*

93 *See id.* at 222 (concluding the focus of the SCA after reviewing its warrant provisions, other sections of the statute, and accompanying legislative history).

already-established mutual legal assistance treaty ("MLAT") processes in the interest of international comity.[94] Finally, and perhaps most remarkably, the Second Circuit acknowledged the intrusive third-party doctrine and derived from the legislative history of the SCA that Congress intended the Fourth Amendment to reign supreme.[95]

Much of the debate on *Microsoft* centers on specific language within the SCA.[96] Before its appeal, *Microsoft* captured the attention of ISPs, telecommunications companies, privacy advocates, and supporters of international law.[97] Compounded with the classified and controversial information leaked by National Security Agency ("NSA") analyst Edward Snowden in 2013, scholars and journalists alike cite growing concern for

---

[94] *See id.* at 221 (deferring to the international law enforcement framework of mutual legal assistance treaty ("MLAT") procedures); Daskal, *supra* note 9, at 395 (examining commonly suggested jurisdictional Fourth Amendment triggers such as national origin or crime alleged).

[95] *See Microsoft Corp.*, 829 F.3d 197, at 214 ("When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions."); *but see* Joseph Schrempp, In Re *Warrant to Search a Certain Email Account: A Victory for Privacy in the Face of a New Technological World*, 19 TUL. J. TECH. & INTELL. PROP. 223, 235 (2016) (analyzing the privacy victory in Microsoft as a possible tool criminals could use to evade law enforcement investigations in the future).

[96] *See In re Warrant to Search,* 15 F. Supp. 3d 466, 474 (S.D.N.Y. 2014) (countering ambiguity within the text of 18 U.S.C. § 2703(a) with the need to facilitate law enforcement activities). Many email service providers do not verify the identity of an individual creating an account. *Id.* at 474.

[97] *See* Valsamis Mitsilegas, *Surveillance and Digital Privacy in the Transatlantic 'War on Terror": The Case for a Global Privacy Regime,* 47 COLUM. HUM. RIGHTS L. REV. 1, 44 (2016) (stating Microsoft offered to store Europeans' data in Germany in November of 2015). Microsoft designed this protocol to keep Europeans' data out of the U.S. government's reach in the wake of the Southern District of New York's opinion in *Microsoft*. *Id. See also* Steven R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law*, 43 CONN. L. REV. 709, 712 (2011) (examining the rise of server farms within the context of Pirate Bay wishing to avoid territorial laws); John Markoff, *Microsoft Plumbs Ocean's Depths to Test Underwater Data Center*, N.Y. TIMES (Jan. 31, 2016), http://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html [https://perma.cc/K2V8-4U5M] (reporting that Microsoft is testing an innovative underwater storage center off the coast of California that uses oceanic current to power and cool blocks of storage equipment); *but see In re* Search Warrant No. 16–960–M–01 to Google, No. 16-1061-M, 2017 WL 471564, at *11 (E.D. Pa. Feb. 3, 2017) (deviating from the holding in *Microsoft* and finding that because the investigative conduct relevant to the SCA occurs within the United States, no principles of extraterritoriality are implicated). The court also declined to follow *Microsoft* in order to not "run afoul of principles of comity and also presents a commonsense interpretation of the SCA which will not lead to absurd results." *Id.* Elsevier, Inc. v. Grossman, No. 12 CIV 5121 (KPF), 2016 WL 7077109, at *9 (S.D.N.Y. Aug. 4, 2016) (following the second prong of the two-prong test advanced in *Morrison* and utilized by *Microsoft* in deciding whether the Racketeer Influenced and Corrupt Organizations ("RICO") investigation at issue involved extraterritorial implications).

data privacy and more generally, individual liberty.[98] As a result, individuals, civil rights groups, and the states themselves are watching the federal government's actions closely with respect to surveillance practices involving domestic and international implications.[99]

---

[98] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/PP53-ASJU] (revealing widespread and covert collection of cellular telephone data by the National Security Agency ("NSA") on behalf of the United States government); Dan Froomkin, *Edward Snowden is on Twitter: @Snowden*, INTERCEPT (Sept. 29, 2015), https://theintercept.com/2015/09/29/edward-snowden-twitter-snowden/ [https://perma.cc/98LG-QXQ6] [hereinafter Froomkin, *@Snowden*] (announcing former NSA analyst Edward Snowden created a Twitter account to more directly address nefarious surveillance practices by, among others, the U.S. government); Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/6HQX-ZX24] (publishing an open letter available to the general public on February 16, 2016 in response to the government's request for Apple to create new code to unlock an iPhone used by one of the San Bernardino shooters). The letter warns:

> The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

Cook, *supra* note 98. *But see* Katie Benner, *U.S. Says It Has Unlocked iPhone without Apple*, N.Y. TIMES (Mar. 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0 [https://perma.cc/F8K6-TK7S] (alluding to other ongoing cases involving the government seeking data stored on locked iPhones that suggest the issue is likely to materialize again); Clark D. Cunningham, *Apple and the American Revolution: Remembering Why We Have the Fourth Amendment*, 126 YALE L.J. F. 216, 225 (2016) (detailing the amount of data requested by the government in *Microsoft* and connecting email searches to phone searches).

[99] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 50 U.S.C. § 1861(b)(2)(B) (2012) [hereinafter PATRIOT Act] (prescribing to obtain a warrant to seize foreign tangible things the government must produce "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized [foreign intelligence and international terrorism] investigation . . . ."); Riley v. California, 134 S. Ct. 2473, 2486 (2014) (stating that the locking function on modern smartphones is a strong security feature). The Supreme Court found that, incident to an arrest, the police may not search the contents of an individual's cell phone without first obtaining a warrant. *Riley*, 134 S. Ct. at 2494. *See also* Elizabeth Atkins, *Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?*, 10 WASH. J.L. TECH. & ARTS 51, 76–77 (2014) (discussing the reduced standard of proof under the PATRIOT Act); Brett Weinstein, *Legal Responses and Countermeasures to National Security Letters*, 47 WASH. U. J.L. & POL'Y 217, 222 (2015) (discussing the negative public response to National Security Letters that function similar to SCA warrants); Dan Froomkin, *USA Freedom Act: Small Step for Post-Snowden Reform, Giant Leap for Congress*, INTERCEPT (June 2, 2015), https://theintercept.com/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/

D. New Legislation on the Block: the CalECPA

Recently, individual states, such as California, have addressed matters regarding electronic communications privacy.[100] The main goal of California's legislation is to ensure that law enforcement must obtain a warrant based on probable cause before obtaining electronic communication information or electronic device information.[101] California enacted the CalECPA in response to data privacy concerns posed in *Microsoft,* and the bill contains both strengths and weaknesses.[102]

[https://perma.cc/G4HF-MPSG] (reporting the revision of the controversial PATRIOT Act ends fourteen years of bulk collection of cell phone records while reauthorizing other controversial provisions allowing the collection of business records). These amendments accomplish "absolutely nothing to restrain the vast majority of the intrusive surveillance revealed by Snowden." Froomkin, *supra* note 99.

100 *See* 725 ILL. COMP. STAT. ANN. 168/10 (2016) (requiring a court order based on probable cause for law enforcement to obtain cell phone location information on an individual during a criminal investigation); IND. CODE § 35-33-5-11(a) (2016) (prohibiting seizure of individual user data for surveillance without a warrant); MD. CTS. & JUD. PROC. CODE § 10-408(a)(1)(iv) (2015) (requiring a court order based on probable cause for law enforcement to obtain location information based on cell phones or other devices on an individual during a criminal investigation); MINN. STAT. § 626A.42(2) (2015) (prohibiting the use of cell phone location information in a criminal investigation without a warrant based on probable cause); MONT. CODE § 46-5-110 (2015) (providing that a government entity must obtain a search warrant before obtaining location information of an electronic device, and providing a civil penalty for wrongful invasions); TENN. CODE § 39-13-610(c) (2016) (prohibiting a governmental entity or law enforcement agency from obtaining the location information of an electronic device without a search warrant except under certain circumstances); *see also* Randall T. Shepard, *The Maturing Nature of State Constitution Jurisprudence*, 30 VAL. U. L. REV. 421, 424 (1996) (discussing imbalances of rights between the state and federal levels); Sen. Mark Leno & Sen. Joel Anderson, *California Electronic Communications Privacy Act, (CalECPA) – SB 178,* ACLU OF N. CAL. (Oct. 20, 2015), https://www.aclunc.org/our-work/legislation/calecpa [https://perma.cc/V7CE-UENG] (introducing the CalECPA as revolutionary for communications privacy in California).

101 *See New CA Poll: Voters Concerned about Digital Privacy, Support Efforts to Increase Protections from Warrantless Searches*, ACLU OF N. CAL. (Sept. 2, 2015), https://aclunc.org/news/new-ca-poll-voters-concerned-about-digital-privacy-support-efforts-increase-protections [https://perma.cc/KT69-GAUX] [hereinafter *ACLU Poll*] (presenting polling data that indicates public desire for increased electronic communications privacy, that companies like Google and Microsoft receive many government requests for data each year, and scholarship raising concerns that granting such requests under the outdated SCA threatens constitutional trends seen in SCA case law); Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (October 8, 2015), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [https://perma.cc/MW3V-D83H] (highlighting the potential that the CalECPA has to bolster privacy expectations).

102 *See infra* Part III.C (examining the merits of CalECPA within the context of *Microsoft*).

Numerous interest groups collaborated to make the CalECPA a reality.[103] Individuals expressed a desire for increased privacy rights.[104] Law enforcement officials wanted to provide essential emergency services without violating the Constitution.[105] Technology corporations did not want to lose business when customers fled to encrypted or foreign competitors.[106] The language of the statute provides some guidance in the wake of the *Microsoft* debate.[107]

The CalECPA contains numerous specific definitions that more accurately reflect the current landscape of available methods of electronic communications.[108] Also, CalECPA section 1546.1(d)(2) requires law enforcement to prove probable cause before obtaining electronic communications information without assigning differing requisite

---

[103] *See Landmark, supra* note 19 (interpreting the California legislature's swift action as a strong desire for data privacy assurances); *ACLU Poll*, *supra* note 101 (reporting AT&T received over 64,000 government demands for customer data in 2014); *see also* Magid, *supra* note 19 (referring to the interests of law enforcement officials as well as individual families in protecting children from online abuse).

[104] *See ACLU Poll*, *supra* note 101 (laying out results of a poll offered to the public regarding data privacy). Before the CalECPA's enactment, the ACLU conducted a statewide poll in California that indicated a public desire for increased electronic privacy protections. *Id.* First, eighty-two percent of Californians responded that the police should have a warrant before searching digital information. *Id.* Second, seventy-nine percent supported a warrant requirement for tracking cell phone activity. *Id.* Third, seventy-seven percent believed text messages deserve the warrant requirement as well. *Id.*

[105] *See id.* (mentioning law enforcement has incentive to adopt bright-line definitions regarding data seizure); *see also* Colleen Curry, *U.S. Cops Aren't Getting Warrants to Spy on People's Cellphones for Petty Crimes*, VICE NEWS (Aug. 25, 2015), https://news.vice.com/article/us-cops-arent-getting-warrants-to-spy-on-peoples-cellphones-for-petty-crimes?utm_source=vicenewsfb [https://perma.cc/6965-WASP] (finding that police use a device known as a "stingray" that mimics a cell tower to intercept an individual's data without his knowledge). However, a stingray also collects other individuals' cell phone data indiscriminately. Curry, *supra* note 105. Further, there is question in numerous jurisdictions as to whether the police are obtaining warrants before using stingrays. *Id.*

[106] *See* Markoff, *supra* note 97 (introducing Microsoft's plans to store customer data in state-of-the-art underwater data storage facilities off the coast of California to increase customer privacy); *ACLU Poll*, *supra* note 101 (noting citizens' interest in privacy regarding their text messages and cell phones).

[107] *See supra* Part II.D (reviewing language in the CalECPA that assists in resolving the extraterritoriality and standard of proof concerns exhibited in *Microsoft*).

[108] *See* CAL. PENAL CODE § 1546(c) (2016) (defining electronic communication as: "the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system"); § 1546(d) (defining electronic communication information as: "any information about an electronic communication . . . including[] . . . the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication . . ."); § 1546(e) (defining electronic communication service as: "a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information").

standards of proof based on the 180-day distinction seen in the SCA.[109] Instead, all warrants seeking electronic communication data require probable cause consistent with the Fourth Amendment, regardless of time in storage.[110] This measure eliminates concerns over the time limit imposed in the SCA that scholars claim is arbitrary.[111] Further the CalECPA generally prohibits required disclosure, subject to limited exceptions and also generally requires notice.[112] However, § 1546.1(d)(3) more generally limits the territorial reach of the CalECPA in a manner similar to § 2703(a) of the SCA.[113]

---

[109] *See* 18 U.S.C. § 2703(a) (2012) ("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."); CAL. PENAL CODE § 1546.1(a)(1) (2016) ("Except as provided in this section, a government entity shall not do any of the following: [c]ompel the production of or access to electronic communication information from a service provider."); § 1546.1(d)(2) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.").

[110] *Compare* U.S. Const. amend. IV (mandating that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"), *with* § 1546.1(d)(1) ("The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought."); *see also* Kerr, *User's Guide supra* note 10, at 1234 (advancing further privacy protections to RCS and ECS data in storage for more than 180 days).

[111] *See* Backer, *supra* note 18, at 396 (suggesting that all email is subject to the reasonable expectation of privacy in *Katz*); Hinz, *supra* note 47, at 521 (summarizing a recent proposal by Senator Patrick Leahy to eliminate the 180-day distinction within the SCA and require a warrant for compelled disclosure of any ECS content no matter the time in storage).

[112] *See* § 1546.1(c)(5) ("[i]f the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information . . . ."); § 1546.1(c)(6) ("[i]f the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device . . . ."); § 1546.2(a) ("Except as otherwise provided in this section, any government entity that executes a warrant[] . . . shall serve upon[] . . . the identified targets of the warrant or emergency access, a notice that informs the recipient that information about the recipient has been compelled or obtained . . . .").

[113] *Compare* 18 U.S.C. § 2703(a) (2012) ("A governmental entity may require the disclosure . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . ."), *with* § 1546.1(d)(3) ("The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants."); *see also* CAL. PENAL CODE § 1546.1(b)(4) (2016) (providing the government may compel production of or access to electronic information from an ISP "[p]ursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access

One alternative to adopting the language of the CalECPA in resolving concerns over *Microsoft* that is important to consider is a recent amendment to Rule 41 of the F.R.C.P.[114] Rule 41(b)(6)(a) allows a district judge to authorize remote access of electronic storage media located within or outside that district in situations where technological means have been used to conceal the location of the storage media.[115] Criticism of the SCA, individual state data privacy legislation, and an amendment to the F.R.C.P. indicate a problem exists with data privacy.[116]

III. ANALYSIS

Recent discussion following *Microsoft* leaves a key issue regarding data privacy unresolved.[117] The reversing opinion only addressed the territorial reach of "warrants" authorized by SCA § 2703(a) but not other available court orders described in § 2703(d).[118] This distinction is

---

to the information via the subpoena is not otherwise prohibited by state or federal law"); *see also* Bryan R. Kelly, #*privacyprotection: How the United States Can Get Its Head out of the Sand and into the Clouds to Secure Fourth Amendment Protections for Cloud Journalists*, 55 Washburn L.J. 669, 697 (2016) (suggesting Congress model its updated SCA after the newly-enacted CalECPA).

114 *See* FED. R. CRIM. P. 41(b)(6) (2016) (allowing extraterritorial disclosure of data by ISPs to the government). The amendment adds:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (a) the district where the media or information is located has been concealed through technological means; or (b) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Id. *See also* Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 YALE J. L. & TECH. 26, 30 (2016) (advancing the goal of amending Rule 41 is to remove unnecessary obstacles to effective law enforcement investigations involving digital crimes). However, critics of Proposed Rule 41 believe amending this rule would remove transparency from the government's investigation. *Id*. at 43.

115 *See* FED. R. CRIM. P. 41(b)(6) ("A magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district . . . .").

116 *See infra* Part III.A (exploring dissonance between the Fourth Amendment in terms of SCA disclosure).

117 *See* Green, *supra* note 45, at 187–88 (summarizing the parties' positions in the lower court opinion in *Microsoft*).

118 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 220 (2d Cir. 2016) (holding Congress intended the SCA warrant to entail domestic limitations when enacting the SCA); Shickich,

important because warrants authorized by § 2703(a) require the government to prove probable cause and are subject to the geographic limitations of the F.R.C.P., whereas court orders prescribed in § 2703(d) are available through the specific and articulable facts standard, and not constrained by the physical boundaries of the F.R.C.P.[119] While warrants seeking email data less than 180 days old are now deservedly limited geographically, non-content data should be considered in the analysis as well.[120] Individual states, like California, are enacting legislation to remedy these concerns, but state-based legislation does not address communications privacy on a federal level.[121]

First, Part III.A examines the SCA under emerging paradigms of the Fourth Amendment.[122] Next, Part III.B analyzes current interests omitted from the *Microsoft* decision.[123] Part III.C then assesses the CalECPA and its detailed language as a possible solution to those interests impinged on by *Microsoft*.[124] Finally, Part III.D offers a solution to both the standard of proof and extraterritorial application dilemmas following *Microsoft* by proposing an amendment to § 2703(d).[125]

A. Revisiting the SCA and the Fourth Amendment in the Age of Data

Email data, data stored in the cloud, social media records, and information transmitted from wearable health technology is subject to

---

supra note 48, at 462 (observing that § 2703 governs compelled disclosure of content and non-content data).

119 *Compare* 18 U.S.C. § 2703(a) (2012) ("A governmental entity may require the disclosure . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . ."), *with* § 2703(d) ("A court order . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that . . . the contents . . . are relevant and material to an ongoing criminal investigation."); *see also In re* Warrant to Search, 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014) (admitting that § 2703(a) ambiguously refers to the Federal Rules of Criminal Procedure ("F.R.C.P."). Two interpretations are possible: first, § 2703(a) could be interpreted to incorporate the geographic limitations included in F.R.C.P. 41; and second, Congress intended some procedural aspects of § 2703(a) to apply to investigations, while other "more substantive rules are derived from other sources." In re *Warrant to Search*, 15 F. Supp. 3d at 470.

120 *See Microsoft Corp.*, 829 F.3d at 222 (holding Congress did not intend for SCA warrants to apply extraterritorially).

121 *See infra* Part III.C (concluding that protections created by the CalECPA do not override the SCA in federal investigations).

122 *See infra* Part III.A (exploring current problems with SCA disclosure regarding the Fourth Amendment).

123 *See infra* Part III.B (discussing the unresolved questions left from *Microsoft*).

124 *See infra* Part III.C (examining the CalECPA's strengths and weaknesses).

125 *See infra* Part III.D (proposing amendment to § 2703(d)).

required disclosure according to a statute contemplated in the 1980s.[126] The standard of proof of anything, "relevant and material to an ongoing criminal investigation" is a lower threshold for the government to meet when seeking older, stored email content compared with probable cause, which is the standard when seeking access to correspondence sent through the ordinary mail.[127] Ambiguity within the text of the Act further compounds privacy concerns.[128] While individuals enjoy more defined privacy expectations regarding their email content following *Microsoft*, older emails and non-content data remain there for the taking.[129]

If the requirement of probable cause is ambiguous within the text of the statute, further difficulties manifest when courts are forced to arbitrarily assign standards of proof to the limited technological distinctions within the SCA.[130] Section 2703 especially lumps all Internet activity into two categories, ECS and RCS.[131] With § 2703(a), the

---

126 *See* Daskal, *supra* note 9, at 366 (stating that records of FaceTime and Google Chats, as well as non-content information like recipient logs, are subject to the provisions of the SCA); Langley, *supra* note 9, at 1644 (summarizing how products, such as Fitbit, monitor and store data related to the user's respiratory rate, skin temperature, and heart rate); *see also* Schultheis, *supra* note 9, at 683 (suggesting that data stored in the cloud is at increased risk following interpretations of the SCA as seen in *Microsoft*).

127 *See* 18 U.S.C. § 2703(d) (2012) ("A court order . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that . . . the contents . . . are relevant and material to an ongoing criminal investigation."); *see also* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (finding that email subscribers enjoy a reasonable expectation of privacy regarding their email content).

128 *See* § 2703(a) ("A governmental entity may require the disclosure . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . ."); *see also In re* Warrant to Search, 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014) (admitting that the text of the SCA is ambiguous as to whether the ordinary physical boundaries of the F.R.C.P. apply to the warrant provision in § 2703(a)); Backer, *supra* note 18, at 380 (lamenting ambiguity within the SCA led the government to seek vast amounts of user data without proving probable cause).

129 *Compare Warshak*, 631 F.3d at 288 (prescribing Fourth Amendment protections to email correspondence despite the lower standard of proof in the SCA), *with* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016) (finding Congress did not intend for the SCA to apply extraterritorially for warrants but not subpoenas or court orders on appeal); *see also* Backer, *supra* note 18, at 398 (expressing desire that the Supreme Court afford Fourth Amendment protections to email correspondence).

130 *See Compare* United States v. Maxwell, 45 M.J. 406, 417 (App. Armed Forces 1996) (finding an individual receives Fourth Amendment protection of remotely stored AOL emails), *with Warshak*, 631 F.3d at 288 (applying Fourth Amendment protections to email correspondence despite the reduced standard of proof in the SCA); *see also* Green, *supra* note 45, at 190 (advancing cloud technology as an example of a confusing concept to regulate with current legislation).

131 *See* Hinz, *supra* note 47, at 515 (illustrating how the framework of the SCA fails to consider online activity that fits both ECS and RCS categories).

government may obtain "contents of a wire or electronic communication," which applies to virtually all of the services offered online.[132] Nevertheless, because the SCA contains limited definitions of different kinds of ISPs, many services today do not easily fit within the ECS or RCS classification.[133] This framework shifts the burden onto courts to determine what privacy considerations a unique Internet service deserves.[134] The credibility of the process by which courts determine the proper standard of proof erodes if the governing statute lacks sufficient definitions of the services affected.[135] *Microsoft* was an example of this attrition.[136]

Ultimately, *Microsoft* laid to rest much of the confusion observed when the term "warrant" found in § 2703(a) is conflated with a court order or subpoena available in § 2703(d), specifically regarding their geographic limitations.[137] However, this decision only addressed the privacy protection afforded to one common form of electronic activity and heaved a glut of other common forms into the shadows.[138] As a result, the geographic reach of court orders authorized by § 2703(d) remains unfettered.[139]

---

132 *See* § 2703(a) (defining the broad scope of the government's authority).

133 *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (expressing concern over the difficulty in applying the SCA to the various forms of communications technologies).

134 *See id.* (identifying that CSLI falls within § 2703(d) and that the reduced standard of proof is not per se unconstitutional). However, the court heavily analyzed what standard of proof should be applied pursuant to the SCA. *Id.* at 610. *See also In re* U.S. for Orders Authorizing Installation and Use, 416 F. Supp. 2d 390, 397 (D. Md. 2006) (noting the statute's lack of clear definitions regarding the disclosure of CSLI).

135 *See* Baker, *supra* note 47, at 110 (stating courts have difficulty in applying the SCA, which led to a quizzical body of jurisprudence).

136 *See supra* Part II.C (analyzing the rationale and privacy implications of *Microsoft* in the Southern District Court of New York). In effect, *Microsoft* removed the probable cause requirement set forth in *Warshak*. *Supra* Part II.C.

137 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016) (determining that Congress unequivocally intended for geographic limitations enumerated in F.R.C.P. 41 to apply to SCA warrants); Green, *supra* note 45, at 192 (predicting all ECPA warrants in the future may functionally resemble subpoenas).

138 *See Microsoft Corp.*, 829 F.3d at 220–22 (analyzing the issue of geographic limitations only within the context of § 2703(a) warrants).

139 *See id.* at 216 (reinforcing the concept that subpoenas may be applied extraterritorially by stating foreign entities are not absolutely insulated from U.S. grand jury subpoenas solely because of their geographic location).

B. The Microsoft *Reversal Only Partially Addresses Data Privacy*

Two issues loom in the aftermath of *Microsoft*.[140] First, the SCA does not require probable cause to compel an ISP to disclose email content data that is in RCS storage for more than 180 days.[141] Second, though the Second Circuit applied the geographic bounds found in the F.R.C.P. to § 2703(a), the court failed to address whether these same limits apply to other court orders authorized in § 2703(d).[142] Assuming the same facts in Microsoft except replacing the email content data the government sought with non-content data, similar international considerations would be triggered if a U.S. agency infringed on the sovereign authority of another nation by obtaining that data.[143]

In *Microsoft*, the lower court relied heavily on the language of § 2703(d) where a SCA warrant functions more like a subpoena, rather than a search warrant, and required a lower standard of proof.[144] Neither *Warshak* nor *Microsoft* directly addressed the sufficiency of the 180-day limitation as a determinative factor when conducting Fourth Amendment analyses.[145] Further, scholars suggest the 180-day distinction no longer advances the original purport of the SCA.[146]

Broad application of the third-party doctrine to vastly distinct forms of personal data threatens the Fourth Amendment rights of United States

---

140 *See infra* Part III.B (summarizing the standard of proof and extraterritoriality issues following *Microsoft*).

141 *See* 18 U.S.C. § 2703(a) (2012) (authorizing compelled disclosure "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" using a court order in § 2703(d)); § 2703(d) ("[a] court order . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that . . . the contents . . . are relevant and material to an ongoing criminal investigation.").

142 *See Microsoft Corp*., 829 F.3d at 208 (applying the F.R.C.P. only to SCA § 2703(a)).

143 *See id.* at 221 (deliberating upon previously established law enforcement procedures between the United States and Ireland by way of the MLAT).

144 *See In re* Warrant to Search, 15 F. Supp. 3d 466, 468–70 (S.D.N.Y. 2014) (discussing various standards of proof available under § 2703); Hinz, *supra* note 47, at 521 (summarizing a recent suggestion by Senator Patrick Leahy to eliminate the 180-day distinction within the SCA and require a warrant for all data).

145 *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (acknowledging that email correspondence today may contain information concerning an individual's private life); In re *Warrant to Search*, 15 F. Supp. 3d at 477 (rejecting Fourth Amendment protections for email communications on the basis of the third-party doctrine).

146 *See* Backer, *supra* note 18, at 399 (arguing the SCA is outdated and the privacy considerations of numerous Americans are at risk); Daskal, *supra* note 9, at 378–79 (concluding geographic location no longer limits investigations involving data); Hinz *supra* note 47, at 518 (summarizing unsuccessful proposed legislation to remove the 180-day time limitation found within the SCA).

citizens.[147] In *Katz*, the Court stated that communications conducted in public do not automatically lose Fourth Amendment protections.[148] Email correspondence today regularly occurs both publicly and privately, and users still consider data relating to their messages private.[149] Yet, without further statutory protection in the SCA, individuals will continue to submit private information to third-party services like Twitter under the misconception that their data is somehow protected.[150] Though the Second Circuit availed priority stored communications data sought by SCA warrants with Fourth Amendment considerations, non-priority stored communications sought with SCA court orders and subpoenas remains unprotected.[151]

Email data today is sharply distinguishable from both the banking records that spawned the third-party doctrine and email data common in 1986 when Congress enacted the SCA.[152] Banking records reveal strictly

---

147 *See* Cover, *supra* note 48, at 1473 (positing many corporations act as avatars for their users and individuals have a privacy expectation despite the existence of the third-party doctrine).

148 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (providing that individuals may express a subjective desire to keep certain communications or materials private, even while in public areas); *see also* Baker, *supra* note 47, at 459 (applying the concept of the term public to easily accessible social media accounts like Twitter or Facebook); *but see In re* Search Warrant No. 16–960–M–01 to Google, No. 16-960-M, 2017 WL 471564, at *11 (E.D. Pa. Feb. 3, 2017) (holding that processing SCA warrants to obtain potentially foreign-stored data controlled by Google does not involve extraterritorial government conduct). The Court emphasized "[e]lectronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory interest in the user data." In re *Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *9. *See also* Elsevier, Inc. v. Grossman, No. 12 CIV 5121 (KPF), 2016 WL 7077109, at *9 (S.D.N.Y. Aug. 4, 2016) (analyzing the possible extraterritorial implications of a RICO investigation after *Microsoft*).

149 *See* Riley v. California, 134 S. Ct. 2473, 2494 (2014) (finding that data poses no immediate threat to an arresting officer, and thus, its seizure must only be accessed pursuant to a search warrant); Mulligan, *supra* note 15, at 1585–86 (analyzing an individual's subjective expectation of privacy with respect to the Fourth Amendment).

150 *See* Cover, *supra* note 48, at 1450 (positing the voluntary nature of Internet communications threaten to diminish privacy expectations pursuant to the Fourth Amendment); *see also* Froomkin, *@Snowden*, *supra* note 98 (predicting Twitter will face pressure from the U.S. government to disclose data concerning tweets made by Edward Snowden from @Snowden).

151 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 214 (2d Cir. 2016) ("When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions."). Here, the court discussed only warrants and not subpoenas or court orders. *Id.*

152 *See* Hinz *supra* note 47, at 492–93 (noting hospitals faced high costs to store medical records and some chose to send records electronically to third-party storage services);

financial information, while email content today may contain anything from an Amazon receipt to sensitive health information.[153] In the past, businesses primarily used email for internal communication on private servers, distinct from other email servers used by other businesses.[154] Today, businesses, organizations, and individuals alike all utilize publicly available email and other services for convenient communication on a daily basis.[155] A conglomeration of all of the data an individual transmits renders a unique account of his or her life.[156] Courts reviewing the SCA have yet to fully recognize this distinction.[157]

SCA orders and subpoenas, available under the significantly reduced specific and articulable facts standard, establish an exception to the Fourth Amendment.[158] Courts recognize this exception without considering the concept of intrusion discussed in *Katz*.[159] By requiring the ISP to surrender information related to an ongoing criminal investigation, the government

---

Kastenmeier, *supra* note 54, at 734 (stating cell phone tracking is more difficult than that of traditional mobile phones).

153 *See* Cover, *supra* note 48, at 1449 (describing the ways technology companies today gather and utilize user data). Amazon recommends books based on an individual's shopping history. *Id.* Readers of the online *Washington Post* receive ads tailored from their Amazon history as well. *Id.* Online shopping history can reveal intimate personal information, for example that an individual is pregnant. *Id. See also* Langley, *supra* note 9, at 1642 (advancing that Fitbits monitor, among other things, respiration, heart rate, and hydration level). These devices transmit information everywhere they go but surprisingly are not regulated by the Health Insurance Portability and Accountability Act ("HIPAA") or the Food and Drug Administration ("FDA"). *Id.* at 1648.

154 *See* Mulligan, *supra* note 15, at 1559–60 (describing the limited nature of early business Internet usage).

155 *See* Robison, *supra* note 53, at 1202 (examining cloud technology and its role in reducing a user's physical location as a barrier to accessing and manipulating data).

156 *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (musing that the term "account" truly conveys the illustrative nature of the sum of a user's data).

157 *See* Greenwald, *supra* note 98 (summarizing widespread domestic and international concern following the disclosure of NSA collection of mass cell phone records by Edward Snowden); *cf.* Cook, *supra* note 98 (rebuking the government's request for Apple to create code capable of bypassing older iPhone encryption technology on the grounds that this would lead to future requests for code capable of bypassing new iPhone technology, thus compromising the privacy considerations of millions of individuals worldwide). Privacy legislation, such as the SCA, may become totally obsolete if the government may access content on mobile devices without the aid of the manufacturer. Cook, *supra* note 98.

158 *See* Shickich, *supra* note 48, at 463–64 (explaining SCA orders do not require probable cause but allow the government to compel disclosure of non-content data by ISPs).

159 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *In re* Warrant to Search, 15 F. Supp. 3d 466, 468 (S.D.N.Y. 2014) (allowing compelled disclosure of email non-content data based on a showing of specific and articulable facts rather than probable cause).

avoids having to conduct an intrusive search.[160] Instead, the ISP obtains the data and delivers it to the government.[161] However, an intrusion still occurs regardless of who obtains the data.[162] The hybrid function of the § 2703(d) court order is to blame for this form of intrusion, and the evidence obtained on this basis threatens basic constitutional rights of millions of Internet users.[163]

Widespread use of the SCA to obtain stored communications data without corresponding Fourth Amendment scruples enables the government to obtain a detailed portrait of an individual's private life.[164] When aggregated, electronic communications data form a mosaic of an individual's life and allows the government to look in with much more detail than an ordinary wiretap or pen-register.[165] The government is able to take this data, and through computing technology, paint very accurate portraits of individuals under investigation.[166] Allowing this type of information gathering on such a low standard of proof threatens the Fourth Amendment protections of liberty itself.[167] Congress must recognize this chasm, act swiftly to correct the outdated SCA, and

---

160 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 471–72 (accepting the government's contention that the SCA warrant functions more like a subpoena and does not involve a search).

161 *See* Klamann, *supra* note 69, at 1421 (stating the task of obtaining the data is assigned to the ISP, not the government).

162 *See Search*, BLACK'S LAW DICTIONARY, *supra* note 25, at 672 (defining a search as: "[a]n examination of a person's body, property, or other area that the person would reasonably be expected to consider as private, conducted by a law enforcement officer for the purpose of finding evidence of a crime"); *Seizure*, BLACK'S LAW DICTIONARY, *supra* note 25, at 678 (elucidating seizure as: "[t]he act or instance of taking possession of a person or property by legal right or process; esp. . . . a confiscation or arrest that may interfere with a person's reasonable expectation of privacy"); Morrison, *supra* note 9, at 267 (offering that the Federal Bureau of Investigations ("FBI") may ask ISPs to search for illegal content on websites).

163 *See* Backer, *supra* note 18, at 398 (underlining the need for updated legislation to avoid privacy violations when the government obtains mass amounts of communications data linked to an individual without a warrant); Foley, *supra* note 33, 468 (addressing the issue of whether or not casual online searches should be afforded constitutional privacy protections based on originalist interpretation).

164 *See* Mulligan, *supra* note 15, at 1596 (finding the SCA poses constitutional questions to data in remote storage); *see also* Atkins, *supra* note 99, at 75 (summarizing recent privacy concerns following reporting that the United States conducts broad dragnet-style surveillance over its citizens without their knowledge under the PATRIOT Act).

165 *See* Walsh, *Mosaic*, *supra* note 47, at 223 (positing that because an individual's movements can be tracked with current technology, there should be some limit to the government's ability to do so).

166 *See id*. at 173 (summarizing recognition of mosaic theory by the Supreme Court).

167 *See id.* at 239 (explaining non-content data such as CSLI and email account log information can be used to track an individual's physical movements).

rebalance the liberty interests of individuals with the needs of law enforcement.[168]

In general, courts may not construe extraterritorial application within an act absent express language or clear legislative intent thereof.[169] However, the lower court in *Microsoft* interpreted one passage of legislative history expressly prohibiting extraterritorial application as an express endorsement.[170] The House Report reflects the SCA applies only to data transactions taking place within the territorial United States.[171] Further, when Congress enacted the SCA, extraterritorial searches would have been inconceivable because most email activity at the time occurred domestically within private servers, primarily for business purposes.[172] Thus, the rationale utilized by the Southern District of New York in applying SCA warrants extraterritorially lacked congressional approval and violated the presumption against territoriality.[173]

The legislative history surrounding the 1986 Act indicates Congress did not intend for any provision involving compelled disclosure in the

---

168 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 233 (2d Cir. 2016) (Lynch, J., concurring) (commending Congress on previously adept privacy legislation and urging legislators to "take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs[]" and amend the SCA); *see also* Marca, *supra* note 91, at 995 (positing the location of the data as a key point in the government disclosure analysis); Battey Jr., *supra* note 91, at 292–93 (suggesting Congress look to the already relevant LEADS Act for guidance in adding a warrant requirement to the outdated SCA).

169 *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 249 (2010) (prohibiting extraterritorial application of statutes lacking either express language or Congressional assent thereof); *but see* Blackmer v. United States, 284 U.S. 421, 443 (1932) (holding the government may, in relation to a criminal trial, compel the return of a U.S. citizen that maintained minimum contacts with the United States); *see also* Schultheis, *supra* note 9, at 675 (stating the text of the SCA does not reference extraterritorial application).

170 *See In re* Warrant to Search, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) (upholding the SCA warrant to compel Microsoft to produce data located in Ireland); *Morrison*, 561 U.S. at 249 (mandating when neither a federal statute nor its legislative history indicates intent for extraterritorial application, it has none).

171 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 473 (acknowledging the House Report while accepting the government's position that in the instant case, the function of the SCA warrant does not involve extraterritorial principles); H.R. Rep. 99-647, at 32–33 (1986) (indicating "the controls in [§ 2703] regarding access to stored wire and electronic communications are intended to apply *only to access within the territorial United States*") (emphasis added).

172 *See* Mulligan, *supra* note 15, at 1563 (stating in the 1980s, even if businesses stored communications remotely, those servers were domestic).

173 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 477 (allowing the DOJ to compel Microsoft to return data stored in Ireland); Schultheis, *supra* note 9, at 680 (summarizing Ireland's concern over the United States unilaterally seizing emails stored within its borders); *but see* Kerr, *Third-Party*, *supra* note 34, at 566 (defending application of the third-party doctrine in that it focuses on data neutrality rather than the individual's origin in a more orderly fashion).

SCA to apply extraterritorially.[174] However, the lower court in *Microsoft* ignored the House Report in favor of case law supporting the position that since it is the ISP that obtains the data, no principles of extraterritoriality are affected.[175] There, *Microsoft* acknowledged the presumption against extraterritoriality found in *Morrison,* yet chose to distinguish that case from the current situation based on the hybrid function of the SCA warrant.[176] In fact, the magistrate judge conceded that the language of § 2703(a) ambiguously references the requirements of the F.R.C.P. without addressing the issue of extraterritoriality.[177] Distinguishable from *Blackmer*, the warrant in *Microsoft* was aimed at a third-party ISP, not an individual.[178] Many larger ISPs operate globally and maintain some form of minimum contacts with the United States.[179] Because many of these ISPs retain non-content data domestically, the government could easily obtain non-priority stored communications by securing the § 2703(d) order in the district within which the company stores the data.[180] Currently, § 2703(d) orders do not require probable cause and can be used to obtain a wide variety of non-priority data.[181] Then, the government can analyze that data and utilize it to particularize future orders, subpoenas, or warrants.[182] Thus, § 2703(d) remains a trap door for government

---

174 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 478 (holding the SCA may be applied to obtain data stored outside U.S. borders); *see also* H.R. Rep. 99-647, at 32–33 (1986) (determining the term "interstate or foreign commerce" excludes interceptions that occur outside of the United States).

175 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 479 (concluding the government's reach established in *Blackmer* was sufficient to override the House Report's express prohibition on extraterritorial application).

176 *See* 18 U.S.C. § 2703(a) (2012) (authorizing compelled disclosure of stored communications data); In re *Warrant to Search*, 15 F. Supp. 3d at 471–72 (dismissing the issue of extraterritorial application in favor of the framework of the SCA).

177 *See* In re *Warrant to Search*, 15 F. Supp. 3d at 470 (admitting that the language of the statute is ambiguous regarding the physical limitations of the F.R.C.P.). The F.R.C.P., if applicable to § 2703(d), require subpoenas and court orders to be executed domestically. *Id*.

178 *See* Blackmer v. United States, 284 U.S. 421, 433 (1932) (stating Blackmer chose to travel to France and remained there even after being served a subpoena under a long-arm statute); In re *Warrant to Search*, 15 F. Supp. 3d at 476 (noting Microsoft is a third-party ISP subject to required disclosure in § 2703).

179 *See* Cover, *supra* note 48, at 1478 (highlighting the global nature of U.S.-based companies like Apple and Google); Markoff, *supra* note 97 (advancing Microsoft is testing innovative underwater storage centers outside U.S. jurisdiction). Microsoft's reported aim is to explore and implement environmentally friendly storage methods. Markoff, *supra* note 97.

180 *See* Cover, *supra* note 48, at 1460 (describing how non-content data may be disclosed without a warrant); Shickich, *supra* note 48, at 469 (finding that non-content data enjoys little Fourth Amendment protection under the SCA).

181 *See* Shickich, *supra* note 48, at 462–63 (enumerating customer name, address, records of session durations, and length and type of service used as examples of non-content data).

182 *See* Mulligan, *supra* note 15, at 1583 (stating that personal data reveals much more about an individual than ordinary business records such as physical location).

investigations.[183] Likely a result, courts in the future will have little guidance as to the privacy expectations and procedures of non-priority stored communications.[184]

Individuals and ISPs alike have an interest in a definitive statutory resolution regarding privacy expectations of non-priority data and extraterritorial application of the SCA.[185] With the privacy protections of § 2703(d) left unresolved, domestic and foreign entities that do business with United States citizens are still subject to similar orders in surrendering evidence in the company's custody, possession, or control.[186] By compelling corporations to procure the materials themselves, courts may avoid extraterritoriality concerns, but they do not avoid possible international implications.[187] The same standard to obtain bank records now seemingly applies to non-priority data in the wake of *Microsoft*.[188] As a result, domestic ISPs stand to lose substantial future business due to privacy concerns of their customers.[189] Additionally, by seizing non-priority stored communications located abroad through SCA warrants, the United States government stands to lose credibility within the international community.[190] Discord between existing doctrines and the *Microsoft* decision leaves future courts at peril in granting SCA warrants seeking data stored outside of the United States, and some states are

---

183 *See* Shickich, *supra* note 48, at 462–63 (conveying that non-content records may be disclosed under the reduced standard of proof found in § 2703(d)).

184 *See id.* at 464 (establishing the general trend that courts view non-content data as less deserving of privacy protection than content data).

185 *See* Baker, *supra* note 47, at 110–11 (arguing for the heavy reform or outright repeal of the SCA due to evidence of inadequacy in application across a wide range of courts); Mitsilegas, *supra* note 97, at 44 (outlining one response taken by Microsoft to keep Europeans' data safe from U.S.-based intelligence efforts).

186 *See* Green, *supra* note 45, at 199 (stating Apple, Google, and Facebook have begun encrypting their users' data); Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 249 (2010) (endorsing the presumption against extraterritoriality when a statute contains only domestic considerations).

187 *See* Green, *supra* note 45, at 199 (suggesting that a notice requirement may prove helpful in resolving international complications); Schultheis, *supra* note 9, at 682 (stating nations are to work together in investigating and prosecuting crime)*; see also* Walsh, *Extraterritoriality*, *supra* note 40, at 640 (arguing that the government has an interest in pursuing SEC violations abroad but must also follow the Constitution and the presumption against extraterritoriality in its pursuits).

188 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 207–08 (2d Cir. 2016) (analyzing extraterritorial application of the SCA only within the context of § 2703(a)).

189 *See* Swanson, *supra* note 97, at 712 (noting Google filed for a patent for a water-based data center in 2007); *but see* Schultheis, *supra* note 9, at 669 (stating the lower court in *Microsoft* ignored geographic boundaries altogether by focusing on the function of the SCA warrant).

190 *See* Schultheis, *supra* note 9, at 683 (discussing possible negative international responses to the use of SCA warrants like in *Microsoft*).

experimenting with their own privacy legislation to avoid state-level instances of the federal *Microsoft* scenario.[191]

C. *CalECPA Resolves* Microsoft*'s Deficiencies*

Congress met growing concern for government accountability and individual privacy following the Snowden leaks with little legislative action.[192] Further uncertainty involving the standard of proof and extraterritoriality limitations that normally accompany search warrants could compound international tensions.[193] This Part discusses the CalECPA with regard to its potential to solve the questionable standard of proof and extraterritorial application of the SCA evident in *Microsoft*.[194]

While other states approached the issue of digital privacy with a probable cause requirement, the CalECPA is the most comprehensive bill of its kind.[195] By eliminating the 180-day distinction found in the SCA, the CalECPA requires each warrant to be granted upon a showing of probable cause.[196] This heightened standard of proof may resolve the

---

191 *See infra* Part III.C (examining the strengths and weaknesses of the CalECPA compared to the SCA); Berman, *supra* note 44, at 321 (describing numerous concerns following the Southern District of New York's ratification of the warrant in *Microsoft*).

192 *See* Kerr, *User's Guide*, *supra* note 10, at 1233–34 (analyzing rationales for raising the standard of proof required to obtain user data). Kerr suggests raising privacy protections for content stored for more than 180 days. *Id.* at 1234. *See also* Froomkin, *@Snowden*, *supra* note 99 (describing the amendment to the PATRIOT Act as a minimal win for privacy advocates).

193 *See Microsoft Corp.*, 829 F.3d at 221 (acknowledging delicate international considerations in denying extraterritorial application of the warrant authorized by § 2703(a)); Daskal, *supra* note 9, at 378 (arguing SCA warrants should be subject to the same territorial limitations as ordinary search warrants governed by the F.R.C.P.).

194 *See infra* Part III.C (analyzing the potential of the CalECPA to resolve lingering privacy concerns following *Microsoft*).

195 *See* 725 ILL. COMP. STAT. 168/10 (2016) (requiring a court order based on probable cause to obtain CSLI); IND. CODE § 35-33-5-9 (2016) (prohibiting disclosure of data and use of unmanned aerial vehicles for surveillance without proving probable cause); MD. CTS. & JUD. PROC. CODE § 10-408 (2015) (requiring a court order based on probable cause for law enforcement to obtain location information based on cell phones or other devices on an individual during a criminal investigation); MINN. STAT. § 626A.42 (2016) (prohibiting the use of cell phone location information in a criminal investigation without a warrant based on probable cause); MONT. CODE § 46-5-110 (2015) (mandating a government entity must obtain a search warrant before obtaining location information of an electronic device); TENN. CODE § 39-13-610 (2016) (forbidding a governmental entity or law enforcement agency from obtaining the location information of an electronic device without a search warrant).

196 *Compare* 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 . . . ."), *with* CAL. PENAL CODE § 1546.1(d)(2) (2016) ("A court shall issue such an order upon a finding that there is probable cause to believe that the

inconsistencies seen in previous cases analyzing the SCA.[197] Further, *Warshak* established Fourth Amendment protections for email communications.[198] While *Warshak* is controlling law only within the Sixth Circuit, the CalECPA bolsters privacy expectations of email communications by requiring probable cause for all warrants seeking disclosure of electronic communications information from an ISP on a state level.[199] The required standard of proof became an issue in *Microsoft* because there, extraterritorial application of the warrant only involved email data in storage for less than 180 days.[200] The CalECPA contains no such time distinction and probable cause is required for the government to obtain electronic communications data.[201] With exact language, the CalECPA addresses the probable cause and extraterritorial application issues seen in *Microsoft*.[202]

CalECPA section 1546.1(d)(3) prohibits extraterritorial application of government surveillance powers by requiring warrants issued under the CalECPA to comply with the general constraints of search warrants.[203]

---

information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.").

197 *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (finding that granting an SCA warrant to obtain CSLI based on the specific and articulable facts standard is not per se unconstitutional under the third-party doctrine); *In re* Application of U.S., 733 F. Supp. 2d 939, 943 (N.D. Ill. 2009) (mandating probable cause for a warrant to obtain CSLI).

198 *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding the Fourth Amendment applies to email correspondence); Bowman, *supra* note 52, at 828 (describing *Warshak* as an expansion of the Fourth Amendment for email communications).

199 *See* CAL. PENAL CODE § 1546.1(d)(1) ("The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought."); § 1546.1(d)(2) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law."); *see also* Backer, *supra* note 18, at 396 (suggesting email communications are private and therefore must be protected by a probable cause requirement consistent with the Fourth Amendment); Shepard, *supra* note 100, at 424 (identifying inadequacies between the federal and state constitutions).

200 *See In re* Warrant to Search, 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014) (applying the 180-day distinction seen in the SCA to the email data requested by the government).

201 *See* CAL. PENAL CODE § 1546.1(d)(2) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.").

202 *See* § 1546.1(d)(3) ("The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants.").

203 *Compare* 18 U.S.C. § 2703(a) (2012) ("A governmental entity may require the disclosure . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."), *with* CAL. PENAL CODE § 1546.1(d)(3) ("The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants.");

CalECPA Section 1546.1(a)(1) establishes a presumption against compelled disclosure of electronic communications information, but allows the government to compel an ISP to turn over data under limited circumstances.[204] The exceptions provided under Section 1546.1(c) limit the government's ability to access the data itself or compel the ISP to surrender it instead.[205] However, similar to the SCA, the CalECPA does not contemplate the geographic reach of its subpoenas capable of accessing non-content data, such as sender and recipient information and time logs.[206] Courts outside of the Second Circuit may, like the lower court in *Microsoft*, find no extraterritorial concerns, and continue to grant SCA warrants, subpoenas, and court orders seeking content and non-content data stored abroad.[207] Conversely, if courts interpret *Microsoft* and the

---

s*ee also* FED. R. CRIM. P. 41(b)(1) ("A magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district.").

[204] *Compare* 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"), *with* CAL. PENAL CODE § 1546.1(a)(1) ("Except as provided in this section, a government entity shall not do any of the following: [c]ompel the production of or access to electronic communication information from a service provider."). Compelled disclosure under § 2703(a) does not require an ongoing criminal investigation, while the CalECPA does. 18 U.S.C. § 2703(a); CAL. PENAL CODE § 1546.1(a)(1). *But see* 18 U.S.C. § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued . . . if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.").

[205] *See* CAL. PENAL CODE § 1546.1(c)(6) ("If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information."); § 1546.1(c)(7) ("If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device."); *see also* Magid, *supra* note 19 (reporting the CalECPA restricts the government's ability to compel disclosure of user data consistent with the Fourth Amendment by requiring probable cause).

[206] *See* CAL. PENAL CODE § 1546.1(b)(4) (providing the government may compel production of or access to electronic information from an ISP "[p]ursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law"); *see also* Shickich, *supra* note 48, at 461–62 (reviewing the non-content data such as search terms, cookies, and IP addresses in Twitter's record retention consent clickwrap form).

[207] *See* 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that has been in electronic storage . . . ."); CAL. PENAL CODE § 1546.1(a)(1) ("Except as provided in this section, a government entity shall not do any of the following: [c]ompel the production of or access to electronic communication information from a service provider."); *but see In re* Warrant to Search, 15 F. Supp. 3d 466, 471 (S.D.N.Y. 2014) (likening SCA warrants to subpoenas in that government agents do not physically travel to where the data is stored).

provisions of the CalECPA to prohibit extraterritorial application, government requests for data would be subject to the geographic limitations found within F.R.C.P. 41.[208]

Warshak, *Microsoft,* and the newly enacted CalECPA all show promise to reinforce the privacy interests of U.S. citizens.[209] Absent a showing of probable cause, CalECPA generally prohibits required disclosure of relevant materials to the government during an investigation.[210] Further, the government would only be able to require disclosure by the ISP under limited circumstances and not just because a certain email account is under investigation.[211] Finally, ISPs are not prohibited from providing notice to the individual linked to the email account, except in certain circumstances.[212] Because the CalECPA offers improvements that resolve both issues seen in *Microsoft*, Congress should revise the SCA with similar language in mind.[213]

---

[208] *Compare* In re *Warrant to Search*, 15 F. Supp. 3d at 476 (finding the execution of the SCA warrant does not extend the government's reach beyond United States's borders), *with* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 214 (2d Cir. 2016) ("When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions."); *see also* FED. R. CRIM. P. 41(b)(1) ("A magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district.").

[209] *See* Backer, *supra* note 18, at 397 (urging the Supreme Court to resolve the dispute following *Microsoft*); Shickich, *supra* note 48 at 469 (stating courts treat non-content data as existing within public space).

[210] *See* CAL. PENAL CODE § 1546.1(d)(2) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law."); *see also* Green, *supra* note 45, at 392–93 (offering the government may employ SCA warrants with corresponding gag orders forbidding the ISP from providing notice of the search to the individual associated with the stored data).

[211] *Compare* 18 U.S.C. § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued . . . if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."), *with* CAL. PENAL CODE § 1546.1(a)(1) ("Except as provided in this section, a government entity shall not do any of the following: [c]ompel the production of or access to electronic communication information from a service provider.").

[212] *See* CAL. PENAL CODE § 1546.2(a) ("Except as otherwise provided in this section, any government entity that executes a warrant[] . . . shall serve upon[] . . . the identified targets of the warrant or emergency access, a notice that informs the recipient that information about the recipient has been compelled or obtained . . . .").

[213] See *infra* Part III.D (proposing amendment to 18 U.S.C. § 2703(d)).

D. A Proposed Solution to the Extraterritorial SCA Warrant

Establishing a general probable cause standard to compel disclosure of content and non-content data would ensure that Americans freely communicate with one another without fear of unwarranted government surveillance.[214] Because the CalECPA does not expressly address extraterritorial seizure of stored communications data, language from the F.R.C.P. would suffice in supplementing the outdated SCA.[215] Including these provisions would cure the extraterritoriality and standard of proof woes seen in *Microsoft*, and thus, Congress should amend § 2703(d) to mirror the more robust provisions of the CalECPA.[216]

1. Amendment to SCA § 2703(d)

Scholars reviewing required disclosure of content and non-content under the SCA recommend raising the minimum standard of proof to probable cause.[217] Further, scholars disagree with the extraterritorial application of a seemingly domestic statute.[218] A controlling statute with a stricter standard of proof may have changed the course earlier on in *Microsoft*.[219]

The proposed text would appear as follows:

---

[214] *See* Backer, *supra* note 18, at 397 (describing limited privacy protections available to email correspondence under the SCA); Langley, *supra* note 9, at 1658 (recommending that personal health data be incorporated into the definition of contents within the SCA due to the sensitive nature of personal health information).

[215] *Compare* CAL. PENAL CODE § 1546.1(d)(3) ("The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants."), *with* FED. R. CRIM. P. 41(b)(1) ("A magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district."); *see also* Shickich, *supra* note 48, at 464 (describing circumstances under which Twitter user's non-content data may be disclosed to law enforcement without a warrant).

[216] *See infra* Part III.D (proposing an amendment to § 2703(d) of the SCA).

[217] *See* Backer, *supra* note 18, at 397 (predicting the Supreme Court will take the SCA standard of proof issue on directly); Schultheis, *supra* note 9, at 1453 (calling for a probable cause requirement to compel disclosure of personal data from an ISP under the SCA following the controversial leaks made by Edward Snowden).

[218] *See* Backer, *supra* note 18, at 397 (suggesting that email users enjoy a reasonable expectation of privacy); Schultheis, *supra* note 9, at 682 (claiming extraterritorial processing of SCA warrants threatens the cloud computing industry on a global scale).

[219] *See In re* Warrant to Search, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) (finding the structure of the SCA sufficient to justify extraterritorial application); Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016) (holding that the SCA does not obligate Microsoft to disclose email content data located in Ireland).

> d) Requirements for court order. A court order for disclosure *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)*, under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only ~~if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation~~ *upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law* . . . In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.[220]

2. Commentary

The proposed amendment to the SCA recalibrates the relationship between the government's interest in prosecuting crime and the Fourth Amendment privacy expectations of individuals.[221] Requiring a showing of probable cause eliminates the ambiguous authority presented between

---

[220] The proposed amendment above is the work of the author. The author wishes to add text shown in italics, and remove existing text shown with strikethrough. *See* 18 U.S.C. § 2703(a) (describing the technical limitations of SCA warrants); § 2703(d) (allowing required disclosure based on specific and articulable facts); CAL. PENAL CODE § 1546.1(d)(2) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law."); FED. R. CRIM. P. 41(b)(1) ("A magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or *property located within the district*.") (emphasis added); Kerr, *User's Guide*, *supra* note 10 (suggesting Congress amend the SCA); Woods, *supra* note 87, at 781 (arguing that Congress must adjust the jurisdictional reach of the ECPA and accommodate criminal or counterterrorism investigations for foreign governments).

[221] *See supra* Part III.B (analyzing apparent weaknesses within the SCA regarding the standard of proof and extraterritorial application).

the SCA and the F.R.C.P. in *Microsoft*.[222] The proposed amendment also includes language from the F.R.C.P. limiting the geographic reach court orders and subpoenas issued under § 2703(d) while providing the possibility for emergency exceptions.[223] A requirement that the data in question be stored within the issuing district along with an increased burden of proof ensures the government may not exceed its constitutional reach.[224] These measures will have limited effects, however, because the SCA is not the only federal statute currently authorizing government surveillance of electronic communications with a standard of proof lower than probable cause.[225] Further, the CalECPA does not allow the government to obtain information for criminal investigations using hybrid search warrants.[226] Because the CalECPA is currently untested in the courts, it remains unclear whether its provisions will solve the issues evident in *Microsoft*.[227] State solutions such as the CalECPA would limit state power, but not federal power due to the lingering SCA.[228]

The CalECPA, subject to limited exceptions, requires the government to show probable cause in exchange for any warrant seeking to access

---

222 *See supra* Part III.C (discussing ambiguity within 18 U.S.C. § 2703(a) as to whether the geographic limitations of the F.R.C.P. apply to § 2703(a) and arguing a clearer definition would aid courts in reviewing SCA cases).

223 *See* FED. R. CRIM. P. 41(b)(1) ("A magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district."). F.R.C.P. 41 also includes exceptions to its territorial limit. *Id.* For example, facing threat of imminent bodily harm to an individual, the law enforcement may exceed its territorial authority. *Id. See also* Walsh, *Extraterritoriality*, *supra* note 40, at 642–43 (providing specific national security exceptions allowing courts to violate the presumption against extraterritoriality).

224 *See* Backer, *supra* note 18, at 399 (arguing the SCA must be revisited by Congress due to the problematic application of its provisions as seen in *Microsoft*).

225 *See* USA PATRIOT Act, 50 U.S.C. § 1861(b)(2)(B) (2012) (stating to obtain a warrant to seize foreign tangible things the government must produce "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation"); Atkins, *supra* note 99, at 81 (arguing that the standard of proof found in the PATRIOT Act must be raised to probable cause); Froomkin, *@Snowden*, *supra* note 98 (lamenting that Congress made little substantive change to the majority of the controversial and intrusive nature of the PATRIOT Act).

226 *See* CAL. PENAL CODE § 1546.1(d)(2) (2016) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.").

227 *See In re* Warrant to Search, 15 F. Supp. 3d 466, 476–77 (S.D.N.Y. 2014) (applying little available case law relevant to extraterritorial application of the SCA).

228 *See* CAL. PENAL CODE § 1546.1(d)(2) ("A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or *federal* law . . . .") (emphasis added); Zetter, *supra* note 101 (providing that five states have similar protections for data content and nine have warrant protections for GPS data); Kelly, *supra* note 113, at 697 (musing the potential benefit of modeling an amendment to the SCA after the CalECPA).

electronic information, including stored information.[229] Regarding notice, CalECPA warrants require notice to the individual as a default, subject to certain exceptions.[230] Current disagreement among courts in granting SCA warrants for various types of information often boils down to which authority the judge prefers.[231] Further, *Microsoft* only expressly resolved the issue of extraterritorial application as to SCA warrants, and not court orders or subpoenas.[232] If future trial courts grant SCA warrants for email data without the government showing probable cause, the burden then shifts on the appellate court to invalidate that warrant.[233] Of the proposed textual amendments to the SCA, there is little scholarly analysis of the appropriate standard of proof for non-content data.[234] Adding twenty-first century language to the SCA will more concretely alert courts as to the reach of their court orders and subpoenas.[235]

Scholars propose alternatives relying on today's often-catastrophic legislative process to amend the federal SCA as displayed in F.R.C.P. 41(b)(6).[236] While the government has a definite interest in gaining tools to combat tech-savvy criminals, the language of F.R.C.P. 41(b)(6) is both

---

229 *See* CAL. PENAL CODE § 1546.1(a)(1) ("Except as provided in this section, a government entity shall not do any of the following: [c]ompel the production of or access to electronic communication information from a service provider.").

230 *See* § 1546.2(a) ("Except as otherwise provided in this section, any government entity that executes a warrant[] . . . shall serve upon[] . . . the identified targets of the warrant or emergency access, a notice that informs the recipient that information about the recipient has been compelled or obtained . . . .").

231 *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (granting an SCA warrant to collect cell site information based on the specific and articulable facts threshold is not per se unconstitutional under the third-party doctrine); *In re* Application of U.S., 733 F. Supp. 2d 939, 943 (N.D. Ill. 2009) (mandating a showing of probable cause for a warrant to obtain CSLI); *In re* U.S. for Orders Authorizing Installation and Use, 416 F. Supp. 2d 390, 397 (D. Md. 2006) (holding probable cause was required for CSLI data).

232 *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 221 (2d Cir. 2016) (recalibrating the issue of geographic limitations within the context of § 2703(a)).

233 *See id.* at 222 (reversing the lower court decision to uphold the SCA warrant).

234 *See* Kerr, *User's Guide*, *supra* note 10, at 1235–36 (proposing amended text to 18 U.S.C. § 2703(d) to resolve confusion with the ECS and RCS distinction before the standard of proof and extraterritoriality debate seen in *Microsoft*). Kerr also suggests Congress further enhance privacy protections to data in storage for more than 180 days. *Id.* at 1234.

235 *See* Shickich, *supra* note 48, at 464 (stating that according to the current SCA and case law, judges may compel disclosure of non-content data from Twitter without obtaining a warrant).

236 *See* FED. R. CRIM. P. 41(b)(6) (requiring that the government has "authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district"); *see also* Backer, *supra* note 18, at 397 (urging the Supreme Court to avail email correspondence of Fourth Amendment protection); Kerr, *User's Guide*, *supra* note 10, at 1615 (advancing amendment to the SCA to cure ambiguities between the ECS and RCS distinction).

overly broad and vague.[237] The phrase "electronic storage media" can be construed to mean anything from a motion picture to the information stored and transmitted via wearable health technology.[238] Further, the rule does not denote whether "outside" includes foreign territories or just U.S. districts separate from the district issuing the warrant.[239] Finally, while the proposed amendment would help in a situation where the government knows that the individual is using technological means to conceal the data's location, granting a SCA warrant would still be based on the "specific and articulable" facts standard of reasonable suspicion contained in § 2703(d).[240] While this proposed rule awaits approval, United States courts will continue to review SCA warrants under the evolving *Microsoft* paradigm.[241] However, because § 2703(a) references the F.R.C.P., this recent amendment should, in the interest in added individual privacy, be revised.[242] Instead, amending § 2703(d) of the SCA to include an increased standard of proof and limit extraterritorial application would comprehensively resolve the *Microsoft* conundrum in one fell swoop.[243]

Others believe the Supreme Court, as in *Katz*, should set the standard of proof for requiring disclosure of email data based on probable cause

---

237 *See* FED. R. CRIM. P. 41(b)(6) (providing the government has the "authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district").

238 *See* Langley, *supra* note 9, at 1659 (summarizing data privacy expectations for wearables as the same for any other stored electronic communications); Shickich, *supra* note 48, at 464 (observing that non-content data is readily subject to disclosure under the specific and articulable facts standard of § 2703(d)).

239 *See* FED. R. CRIM. P. 41(b)(6) (adopting the government has "authority to . . . seize or copy electronically stored information located *within or outside that district*") (emphasis added).

240 *See* 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 . . . 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* . . . .") (emphasis added); CAL. PENAL CODE § 1546.1(d)(2) (2016) ("[a] court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or *federal* law.") (emphasis added); FED. R. CRIM. P. 41(b)(6) (suggesting the government has "authority to . . . seize or copy electronically stored information located *within or outside that district*") (emphasis added).

241 *See* Schultheis, *supra* note 9, at 689 (concluding concerns will not subside until Congress updates data privacy legislation to match technology's growing infrastructure).

242 *See* 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . .").

243 *See supra* Part III.B (examining the two issues posed in *Microsoft* regarding the appropriate standard of proof and extraterritorial application of SCA warrants).

and avoid Congress altogether.[244] While a decision from the Supreme Court would resolve the issue, this theory assumes that the Supreme Court is ready and willing to offer blanket Fourth Amendment protections to a relatively new form of potentially anonymous communication.[245] Also, this theory requires a Court capable of handing down a definitive answer to a controversial matter.[246] A sweeping solution from the Court, while possible due to the vacant seat on the Court left by Justice Antonin Scalia, presupposes the Court granting certiorari to a case involving email privacy and the SCA.[247] Because it is possible the Court may also choose to deny Fourth Amendment protections to email communications or defer to Congress in enacting appropriate legislation, amending the SCA places control of the future of email privacy rightfully with the legislative branch.[248]

Taken together, perhaps the strongest reason to amend the SCA is the undeniable reality that email usage today vastly differs from email usage in the 1980s and requires commensurate legal protection.[249] Content is not limited to business communications as it now offers an intimate view of an individual's life.[250] Emails can be sent from devices other than computers from almost anywhere in the world.[251] Paradoxically,

---

244 *See* Katz v. United States, 389 U.S. 347, 359 (1967) (holding that communications conducted in a public telephone booth deserve a reasonable expectation of privacy from government surveillance); Backer, *supra* note 18, at 396 (arguing Congress has been reluctant to update the SCA despite rapidly advancing technology, and thus, the Supreme Court should tackle the issue instead).

245 *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (mentioning email and other Internet communications often contain the most intimate information that the individual wishes to keep private); Weinstein, *supra* note 99, at 249 (stating one way to avoid law enforcement surveillance on the Internet is to use anonymization software, such as Tor, that makes the user's identity unknown to both the ISP and the government).

246 *See* Chait, *supra* note 31 (noting eight justices currently preside over the Court).

247 *See* Bowman, *supra* note 52, at 809 (noting *Warshak* was a 6th Circuit decision); Solove, *Justice Scalia*, *supra* note 84 (arguing Justice Scalia notoriously believed searches of materials provided to third parties do not violate the Fourth Amendment). Justice Scalia's absence means the Court may finally reign in the third-party doctrine and mandate Fourth Amendment protections to email communications. *Id*. *See also* OYEZ, *supra* note 31 (conveying the Court decided *Katz* in a seven to one decision, with Justice Black dissenting and Justice Marshall abstaining). The reasonable expectation of privacy advanced in *Katz* did not require a five-four ruling. *Id*.

248 *See* Backer, *supra* note 18, at 401 (urging the Supreme Court to scale back the government's ability to seize data without proving probable cause).

249 *See* Schultheis, *supra* note 9, at 689 (concluding that concerns will not subside until laws are updated to match our growing infrastructure).

250 *See* Langley, *supra* note 9, at 1658 (analyzing data privacy expectations for fitness technology); Shah, *supra* note 9, at 540 (opining data submitted in relation to Facebook and WhatsApp communications are subject to disclosure under the SCA).

251 *See* Daskal, *supra* note 9, at 366 (explaining the mobile nature of email and other Internet communications).

individuals today use the Internet regularly to share intimate information globally with little to no regard for the government's near-Orwellian surveillance capabilities.[252] Amending the SCA would attack the problem at the source while leaving a choice amongst the states to do the same.[253] For each of these considerations, it is imperative to equate our daily email correspondence to the parchment papers to which the Fourth Amendment refers.[254]

IV. CONCLUSION

In the din of modern existence, privacy stands to be one, if not the most important, fundamental liberty in the twenty first century deserving of a rigorous defense. Almost fifty years after *Katz*, communications technology connects U.S. citizens on an ongoing basis. Since the name Snowden became widely known, many scholars and individuals believe that the Fourth Amendment nears obsolescence as the surveillance powers of the United States government expand. Those left in peril are ordinary U.S. citizens who rely on email communication for business or personal reasons. To quell growing concerns over digital privacy, Congress should amend the outdated structure of the SCA. Otherwise, unchecked government surveillance power will induce the once vital liberties afforded by the Fourth Amendment to wither away.

Returning to Frank's situation, the government may only require disclosure of Microsoft's domestic data after proving probable cause, as the language of the Fourth Amendment and the F.R.C.P. intend. With greater privacy protections, U.S. citizens may freely and legally associate online without unnecessary fear of government surveillance. ISPs may too reap the benefits of the digital age, so long as they maintain an acceptable balance between consumer protection and compliance with legitimate law enforcement requests. While no legislation is perfect, organic growth of case law surrounding the CalECPA should assist in bringing communications privacy to the full attention of the legislature, the High Court, and the American public. Well-reasoned and frequently

---

252 *See* Atkins, *supra* note 99, at 86 (examining the government's wide surveillance powers under the PATRIOT Act); Curry, *supra* note 105 (inquiring whether certain police forces are obtaining warrants based on probable cause before using Stingray technology); Greenwald, *supra* note 98 (revealing information provided by NSA analyst Edward Snowden in 2013 that the United States government conducts mass dragnet-style surveillance on cell phone data with the cooperation of numerous cell service providers without first seeking particularized search warrants).

253 *See supra* Part III.B (summarizing constitutional privacy concerns that email users face following *Microsoft*).

254 *See* U.S. CONST. amend IV (guaranteeing "[t]he right of the people to be secure in their persons, houses, papers, and effects").

tended legislation, like the CalECPA, may prove to be the loam in which the roots of the Fourth Amendment receive new life.

Brian Tuinenga[*]

[*] J.D. Candidate, Valparaiso University Law School (2017); B.A., Philosophy and Political Science, Augustana College (2011). The author wishes to thank Professor Robert Knowles for his guidance and expertise, as well as the editors of the *Valparaiso University Law Review* for their tireless efforts in revising and improving this Note. Finally, the author wishes to thank his family, especially his parents, for their unending inspiration and support.