Catholic University Journal of Law and Technology

Volume 24 | Issue 1 Article 8

December 2015

Implications for the Future of Global Data Security and Privacy: The Territorial Application of the Stored Communications Act and the Microsoft Case

Russell Hsiao
Catholic University of America, Columbus School of Law

IMPLICATIONS FOR THE FUTURE OF GLOBAL DATA SECURITY AND PRIVACY: THE TERRITORIAL APPLICATION OF THE STORED COMMUNICATIONS ACT AND THE MICROSOFT CASE

Russell Hsiao*

It is the year 2020. The Chinese government has demanded that Google, the owner and operator of Gmail, a web-based e-mail service, turn over to local law enforcement authorities the metadata and contents in e-mail accounts of two individuals. The two targets of this demand are both Chinese citizens and well-known human rights activists.[1] One person received a human rights award in the West for her courageous struggle for democracy in the Xinjiang Uyghur Autonomous Region, and the other is her lawyer. Beijing claims both have broken domestic law by allegedly conducting "unlawful" protests in front of a central government office. The pair is ostensibly challenging the government's heavy-handed tactics in China's restive western region. The Ministry of Public Security abides by domestic laws and protocols, which grants them the legal authority to acquire all records from the e-mail accounts for further criminal investigation.[2] Upon receiving the Chinese government's request, Google's

* J.D. Candidate 2016, The Catholic University of America's Columbus School of Law; B.A. International Studies with University Honors, 2005, American University. The author would like to thank Professor Chris Savage for serving as the expert reader and members of the journal's editorial board for reviewing earlier drafts. He may be reached at 22hsiao@cua.law.edu.

[1] Assume for the purpose of this intellectual exercise that the awards were conferred by the U.S. Government; a recognition meant to highlight the differences in values between the two governments and how such differences could affect our judgment. Furthermore, also consider, or assume for the matter of this exercise), that there were news reports that some Uyghur may be receiving training in neighboring Pakistan with known terrorist groups and could be plotting violent attacks against the Chinese government. *See, e.g.*, Michael Wines, *China Says Region's Attackers Trained in Pakistan*, N.Y. TIMES, Aug. 2, 2011, at A3.

[2] In late 2014, the Chinese government announced a Draft Counterterror Law requiring companies to keep servers and user data within China, supply law enforcement authorities

response team quickly tracks the location of the data, and determines that the accounts' metadata—or non-content information—is stored in computer servers in China. This practice is consistent with Beijing's data localization and retention rules, however, the content of the e-mails—the content of the communications—are stored in servers in the United States.

Across the Pacific, in a similar fashion U.S. law enforcement lawfully acquires a warrant from a judge to search and demand the production of e-mails of an American citizen with suspected ties to a murderous drug cartel. The metadata, or e-mail header information (*i.e.,* "From:," "To:", "CC:," and Timestamp fields of the e-mails),[3] of the subject's e-mails are stored in servers located within the United States. However, as a result of the company's data routing and server architecture, a complex, and confidential system proprietary to the company, Google's databases are spread throughout the United States and worldwide.[4] In the case of the drug suspect the contents of the e-mails, such as the subject line and body, are stored in servers physically located in Russia.[5]

How should Google respond to the requests of the Chinese and American governments? Is Google legally obligated to turn over the foreign-stored data to the local authorities? Should Google be legally obligated to turn over the foreign-stored data in response to a unilateral demand by a government?

The latter hypothetical scenario parallels an actual case now before the Second Circuit Court of Appeals. In *Microsoft v. United States*, prosecutors at the Department of Justice ("DOJ") sought and obtained a warrant in 2013 for the information contained in a Microsoft Outlook account.[6] The requested infor-

---

with communications records and censor terrorism-related Internet content. A second draft of the law was released in late February 2015 (*See, e.g.*, Reuters, *China Draft Counterterror Law Strikes Fear in Foreign Tech Firms*, RE/CODE (Feb. 27, 2015), http://recode.net/2015/02/27/china-draft-counterterror-law-strikes-fear-in-foreign-tech-firms/?utm_source=newsletter&utm_medium=e-mail&utm_campaign=rc_e-mail_daily&utm_content=china-draft-counterterror-law-strikes-fear-in-foreign-tech-firms.

[3] *Reading full e-mail headers*, GOOGLE.COM, https://support.google.com/mail/answer/29436?hl=en (last visited Mar. 8, 2015).

[4] James C. Corbett, et al., *Spanner: Google's Globally-Distributed Database*, GOOGLE, INC., http://static.googleusercontent.com/media/research.google.com/en//archive/spanner-osdi2012.pdf (last visited Sept. 20, 2015).

[5] *See generally* United States v. Gorshkov, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (finding the Fourth Amendment does not apply to FBI agents' "extraterritorial access to computers in Russia and their copying of data contained thereon.").

[6] Kathleen Porter, *Microsoft Versus the Federal Government: Round Three*, ROBINSON & COLE (Apr. 9, 2015), http://www.dataprivacyandsecurityinsider.com/2015/04/microsoft-versus-the-federal-government-round-three/; *see also In re* A Warrant to search a Certain E-mail Account Controlled & Maintained by Microsoft Corp. (*In re* Microsoft), 15 F.Supp.3d 466 (S.D.N.Y. 2014).

mation was stored in computer servers based in Dublin, Ireland.[7] Microsoft challenged the legality of the warrant,[8] arguing that since it was issued by the court under the Stored Communications Act ("SCA"), it can only apply to data stored within the United States.[9] The District Court, however, sustained the warrant authorizing the search and held Microsoft in contempt for then failing to produce the data.[10] Microsoft appealed the District Court's ruling before the Second Circuit Court of Appeals, which heard the case on September 9, 2015.[11] As of this publication, a decision has not been reached.[12]

A handful of articles have addressed the issues surrounding whether the SCA, as written, applies to data stored outside the United States. From one perspective, the dispute revolves around the proper interpretation of the SCA's meaning and how extraterritoriality principles apply to that statute.[13] However, the practical implications of the dispute extend well beyond statutory interpretation.[14] The practical issues include the policy implications of an extraterritorial application of the SCA on relations between the United States and other countries, and on the business models and profitability of major U.S. corporate entities such as Microsoft, Google, and Amazon.[15]

---

7 *In re* Microsoft, 15 F.Supp.3d 466.

8 *Id.*

9 *Id.*

10 *Id.*

11 Sam Thielman, Microsoft case: DOJ says it can demand every email from any US-based provider, THE GUARDIAN (Sept. 9, 2015, 4:06 PM), http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant.

12 *See* Porter, *supra* note 6.

13 *Compare* Orin S. Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?*, WASH. POST: THE VOLOKH CONSPIRACY (July 7, 2014) [hereinafter Kerr, *Legal Protections*], https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/25/more-on-privacy-rights-in-e-mail-stored-outside-u-s/ (stating that the SCA is generally thought to apply only inside the United States) *with* Jennifer Daskal, *The Microsoft Warrant Case: A Response to Orin Kerr*, JUST SEC. (Sept. 3, 2015, 3:28 PM), https://www.justsecurity.org/25801/microsoft-warrant-case-response-orin-kerr/ (determining that both parties and two judges have agreed that this case is about whether the SCA applies outside of the United States); *see also Privacy Law – Stored Communications Act – District Court Holds that SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign Servers* – In re *Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 128 HARV. L. REV. 1019, 1023-26 (2015); *see also* Andrew Fields, *Lowering the Temperature on the Microsoft-Ireland Case,* LAWFARE (Sept. 11, 2015, 10:10 AM), https://www.lawfareblog.com/lowering-temperature-microsoft-ireland-case (implying that if Microsoft loses it will not change the meaning of the SCA or be a blow to internet privacy and state sovereignty)

14 Thielman, *supra* note 11.

15 Jennifer Daskal, *Case To Watch : Microsoft v. US on the Extraterritorial Reach of the Electronic Communications Privacy Act*, JUST SEC. (Mar. 6, 2015, 1:13 PM), https://www.justsecurity.org/20780/case-watch-microsoft-v-united-states-extraterritorial-reach-electronic-communications-privacy-act.

In light of these considerations, some commentators have described the decision by the DOJ to attempt to obtain the e-mail content by means of an American court-issued warrant, as opposed to the utilization of diplomatic channels through a "Mutual Legal Assistance Treaty" ("MLAT"), as a "policy choice."[16] The assertion that warrant usage is a "policy decision"—with the implication that the choice is not strictly a legal one to be resolved by the courts—foreshadows the challenges facing the U.S. and other nations in dealing with this issue. Indeed, the issues relevant to this case also touches on how governments will reconcile differing norms and values between legal systems, competing foreign policy goals, and economic interests.[17] To date, the international policy implications of data globalization—the unfettered flow of knowledge in the form of data-packets crossing borders on the Internet—remain unsettled.[18]

Against the backdrop of increased tensions between governments over cyber-conflicts in cyberspace, such as cyber-espionage[19] and government surveillance,[20] the issues of data nationalism[21] and territorial jurisdiction over activities in cyberspace are causing more international friction than ever.[22] Some

---

16 Jonah F. Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. J. (Jan. 28, 2015, 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ (explaining "DOJ made a policy choice to seek a warrant rather than using the MLAT process, based in large part on concerns about the efficacy of the MLAT system and the potential for a drawn-out waiting period").

17 *See In re* A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F.Supp. 3d 466, 467 (S.D.N.Y. 2014) (stating Microsoft contends that the United States does not have the authority to issue a warrant which requires extraterritorial search and seizure); *see also* Jonah F. Hill, *supra* note 16 (noting that Microsoft would rather the request for data to go through MLAT, otherwise having to comply with multiple requests and in multiple jurisdictions would be unduly burdensome).

18 There is no set definition of data globalization. The author uses it to describe the idea of "unfettered knowledge flow" by analogy to globalization in trade, which generally means the removal of trade barriers.

19 The estimated annual cost of cybercrime and economic espionage to the world economy ranges from $445 billion to $1 trillion. *See* Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and espionage costs $445 billion annually*, WASH. POST (June 9, 2014), http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

20 Glenn Greenwald et al., *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, THE GUARDIAN, (June 11, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. In 2013, former federal government contractor Edward Snowden leaked a trove of classified materials revealing extensive government surveillance programs covering both American and non-American communications. *Id.*

21 DANIEL CASTRO, THE INFO. TECH. & INNOVATION FOUND., THE FALSE PROMISE OF DATA NATIONALISM 10 (2013).

22 For instance, China's Internet czar Lu Wei, director of the State Internet Information Office, has repeatedly called on the United States to respect China's cyber sovereignty. *See,*

governments have already enacted or are considering new data security and privacy measures, such as data localization laws that require data collecting Internet companies to store the collected data on servers physically located within the country.[23] For instance, Russia enacted a new law effective as of September 1, 2015, requiring Internet companies to locate their computer servers that contain personal information on Russian citizens within the country's borders.[24] Developments such as this led some legal scholars, such as Columbia Law Professor Tim Wu[25] to predict the "Balkanization" of the Internet[26]—the fragmentation of the Internet into separate, nationalized segments.[27] Actions such as those of the U.S. government in the *Microsoft* case, claiming the right to directly gain access to data not physically stored within its territory, may inadvertently encourage this trend.

These concerns do not mean a government lacks legitimate interests or should be foreclosed from obtaining digital evidence that may be stored outside the jurisdiction of its courts or otherwise outside the government's territorial control. Efficient acquisition of data is increasingly critical for criminal investigations that transcend national borders, and in some cases national security, as more data goes online and is only obtainable by digital means.[28] However, the efficiency of MLAT arrangements is questionable, even in cases between friendly nations with shared values such as democracy and human rights, as is the case of *Microsoft* between the United States and Ireland. Factor in the reality that some of the United States' largest trading partners do not

---

e.g., Lu Wei, *Cyber Sovereignty Must Rule Global Internet*, HUFF. POST (Feb. 14, 2015, 5:59 AM), http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html.

[23] For a detailed discussion about the challenges of data nationalism, *see* Castro, *supra* note 21.

[24] *Deadline for Compliance with Russian Localization Law Set for September 1, 2015,* PRIV. & INFO. SEC. L. BLOG (Jan. 2, 2015), https://www.huntonprivacyblog.com/2015/01/articles /deadline-for-compliance-with-russian-localization-law-set-for-september-1-2015/.

[25] Professor Tim Wu is the author of *The Master Switch*: *The Rise and Fall of Information Empires*. The book offers a detailed account about the characters involved in the rise and fall of information empires, from the telephone, to the radio and television, and the Internet, within the United States. *See generally* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 168-75 (2010).

[26] Bob Davis, *Rise of Nationalism Frays Global Ties*, WALL ST. J., Apr. 28, 2008, at A16 (statement of Tim Wu, law professor at Columbia University) ("'We're facing a step-by-step Balkanization of the global Internet…It's becoming a series of national networks.'").

[27] *See generally* Robert Pringle, *Balkanization*, ENCYC. BRIT., http://www.britannica.com/EBchecked/topic/50323/Balkanization (last visited Sept. 22, 2015).

[28] NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-86, GUIDE TO INTEGRATING FORENSIC TECHNIQUES INTO INCIDENT RESPONSE, at ES-1, 3-2 (2006), http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

share similar values and may even be considered competitors in the political and military arenas, a warrant issued by a U.S. judge, sworn to uphold strict legal standards, to obtain data residing in a foreign nation—even if that entails recovering data from overseas—may be the best among worst options. To be sure, the courts' eventual resolution of the dispute in *Microsoft v. United States,* will have policy implications that go well beyond the narrow legal issue that the case presents on the surface.

This Note discusses the legal and policy implications of *Microsoft v. United States*. Part I provides technical background on how electronic mail, or e-mail, works. Part II presents an overview of the relevant provisions of the SCA and the different legal instruments, including warrants, subpoenas, and court orders, available to law enforcement under the statute. Part III reviews the procedural history of the *Microsoft* case, as well as the legal and policy positions taken by the government and Microsoft. Part IV weighs the parties' arguments, analyzes the efficacy of the available legal instruments, presents the lower court's ruling, and ultimately offers a new framework for handling digital evidence in the case of cross-border data transfers and law enforcement cooperation.

As the Internet continues to expand, evolve, and connect more people online, the cross-border data transfers that make it possible are increasingly important with respect to economic activity, social and military communications, and law enforcement purposes. This Note argues that the resolution of the *Microsoft* case will have profound implications for the evolution of the Internet in general and particularly, the use of e-mail, sparking a robust conversation about the concept of sovereignty in cyberspace, and whether it exists in this new paradigm.[29]

I. ELECTRONIC COMMUNICATIONS AND THE INTERNET

A thorough legal analysis of stored electronic communications is enhanced by a background discussion about the evolution of electronic communications and the nature of the Internet.[30] Like the Internet itself, e-mail was born in the Pentagon-sponsored Advanced Research Projects Agency Network program—more commonly known as "ARPANET." The ARPANET is a linked network of computers in government sponsored research labs hosted at universities and

---

[29] Mark Scott, *Ireland Lends Support to Microsoft in Email Privacy Case*, N.Y. TIMES (Dec. 24, 2014, 5:44 AM), http://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case.

[30] For an overview of the history the Internet, *see generally* WU, *supra* note 25.

firms throughout the United States.[31] The inception of e-mail is described by some Internet historians as a "found art" or a "lucky accident;" [32] the first program for sending electronic messages within a specific computer, via a time-sharing system, was invented in the early 1960s.[33] This early system permitted researchers using a time-sharing-enabled computer to send short electronic messages to one another that only the addressed recipient could read.[34]

The first electronic-mail delivery system between two computers was programmed in 1972 by engineer Ray Tomlinson at the technology firm, Bolt Beranek and Newman.[35] Prior to Tomlinson's simple but ingenious program, electronic messages could only be sent and received within a single time-sharing-enabled computer.[36] Tomlinson's program built on an existing file transfer protocol ("FTP") that he worked on called "CPYNET," which allowed a computer user to transfer computer files to another computer within the network.[37] The same year, an APRANET programmer at MIT, Abhay Bhushan, included Tomlinson's e-mail program into ARPANET's FTP.[38] Historians of the Internet proclaimed that "[e]-mail was to the ARPANET what the Louisiana Purchase was to the young United States."[39] Indeed, ARPANET took Tomlinson's idea of transferring mail messages via FTP and expanded it one-hundred-fold.

A. The Meteoric Rise of E-mail

Today, e-mail is the most ubiquitous professional and personal means of communications.[40] Obviously, this was not always the case. In early 1976, four

---

31 *See* KATIE HAFNER AND MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 187 (1996).

32 *See id*. at 189 ("The ARPANET's creators didn't have a grand vision for the invention of an earth-circling message-handling system.").

33 Due to its high costs and limited capacity, "time-sharing" was a groundbreaking 'hack' of early computers that permitted multiple researchers to share the processing capacity of a single computer system. *See id.* at 190.

34 BARRY M. LEINER, ET AL., INTERNET SOC'Y, BRIEF HISTORY OF THE INTERNET 2-3 (2012), http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf.

35 HAFNER & LYON, *supra* note 31, at 191 ("The first electronic-mail delivery engaging two machines was done one day in 1972 by a quiet engineer, Ray Tomlinson at BBN.").

36 *Id.* at 190.

37 *See* J. POSTEL & J. REYNOLDS, INTERNET ENG'G TASK FORCE, RFC 959, File Transfer Protocol (FTP) 1 (1985), https://www.ietf.org/rfc/rfc959.txt (noting that the objectives of FTP include: the promotion of the sharing of files [computer programs and/or data] and the encouragement of indirect or implicit [via programs] use of remote computers); *see also* HAFNER & LYON, *supra* note 31, at 191.

38 *Id.* at 191-192.

39 HAFNER & LYON, *supra* note 31, at 189.

40 *The First E-mail Message of Ray Tomlinson*, HIST. OF COMP., http://history-computer.com/Internet/Maturing/Tomlinson.html (last visited Apr. 4, 2015).

years after CPYNET,[41] ARPANET hosted 98 sites and was processing approximately 9,800 e-mails per day.[42] Meanwhile, the United States Postal Service ("USPS") was handling 50 billion items of first-class mail a year,[43] which translates roughly to about 137 million items per day—more than a thousand times the rate of e-mail messages. Twenty years later, in 1996, individual sites were capable of processing 150,000 e-mail messages every day.[44] In 2013, nearly another 20 years later, roughly 183 billion e-mails were sent each day.[45]

The USPS recognized the challenges from e-mail to traditional mail correspondences from the very beginning. "We are being bypassed technologically," lamented an assistant U.S. Postmaster General at the beginning of 1976—referencing the emergence of e-mails.[46] Government studies published during that time recommended adding e-mail to the services of the Post Office.[47] However, government regulators ultimately decided to adopt a free market approach and to refrain from creating any significant government role in providing e-mail services.[48]

Early on, the Advanced Research Projects Agency ("ARPA") management—the predecessor of the Defense Advanced Research Projects Agency ("DARPA")—recognized the surprising success and future importance, of e-mail.[49] An internal report from the late 1970s sent by the Information Processing Techniques Office ("IPTO") to ARPA management stated,

> The largest single surprise of the ARPANET program has been the incredible popularity and success of network mail. There is little doubt that the techniques of network mail developed in connection with the ARPANET program are going to sweep the country and drastically change the techniques used for intercommunication in the public and private sectors.[50]

---

41 *Id.*

42 HAFNER & LYON, *supra* note 31, at 211 ("MIT was a typical site, and by extrapolation, if one machine processed about a hundred pieces of e-mail a day, multiplied by a factor of 98 or so (the number of hosts then on the Net).").

43 *Id.* ("…electronic mail didn't yet appear to pose a threat to the U.S. postal system [that] … handled more than 50 billion pieces of first-class mail a year.").

44 *Id.*

45 JUSTIN LEVENSTEIN, THE RADICATI GRP., INC., EMAIL STATISTICS REPORT: 2013-2017 – EXECUTIVE SUMMARY (Sara Radicati ed., 2013), http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf; *see also* Marshall Brain & Tim Crosby, *How E-mail Works*, HOWSTUFFWORKS, http://computer.howstuffworks.com/e-mail-messaging/e-mail6.htm (last visited Mar. 8, 2015) (stating that a market research firm found that more then 183 billion emails were being sent in a day).

46 HAFNER & LYON, *supra* note 31, at 212.

47 *Id.*

48 *Id.* at 213.

49 *Id.* at 214.

50 *Id.*

The managers at IPTO were correct in their prediction about the disruptive effects of e-mail.

B. How E-mail Works

Initially, different computer programs and operating systems handled e-mail differently.[51] This led to compatibility issues for network operators.[52] If a reader's mail handling program is incompatible with the sender's program, messages might be unreadable, or simply dropped.[53] Indeed, "[w]hen one mail handler couldn't parse [e-mail] headers sent by others, it was as if a postal clerk in Keosha, Wisconsin, were being asked to deliver letters addressed in Sanskrit and Arabic."[54] The technical challenges grew exponentially as the number of mail programs ballooned and the number of connected nodes on the Internet grew.[55] A common standard to permit different programs to handle electronic messages was sorely lacking but clearly critical for the efficient functioning and viability of the nascent electronic messaging system.[56]

1. POP3, IMAP, and STMP

Today, there are several different Internet standards for delivering and retrieving e-mails. Three of the most popular are POP3, IMAP, and SMTP, which exist at the application layer of Internet protocols.[57]

The Post Office Protocol ("POP3") is used by local e-mail clients running on individual computers to retrieve e-mail from a remote server over an Internet connection.[58] IMAP, or "Internet Message Access Protocol," is a more advanced Internet protocol that permits users to access e-mails on multiple devices.[59] IMAP accomplishes this by commanding that the data representing the e-mail messages remain on the remote e-mail server.[60] This stored data can be accessed by and downloaded by multiple devices, such as a work computer, a

---

51 *Id.* at 199.
52 HAFNER & LYON, *supra* note 31, at 200.
53 *Id.* at 199.
54 *Id.* at 198.
55 *Id.*
56 *Id.* at 197 ("imagine a local post office somewhere … making up its own rules for addressing, packaging, stamping, and starting mail … invent its won set of ZIP codes …").
57 There are four layers in Internet protocols: application, transport, Internet, and link. *See, e.g.,* Henrik Frystyk, *The Internet Protocol Stack*, WORLD WIDE WEB CONSORT. (July 1, 1994), http://www.w3.org/People/Frystyk/thesis/TcpIp.html.
58 Brain & Crosby, *supra* note 45.
59 *Id.*
60 *Id.*

home computer, and a smartphone.[61] IMAP also enables the user to organize e-mail into folders;[62] the folder structure is maintained on the server as well.[63] With IMAP, when a user searches for an e-mail, the search is commanded by the user's device with the data containing the message is located on the assigned server, not the user's local device.[64]

Most if not all modern e-mail clients and servers support POP3 and IMAP, which are the two most prevalent Internet standard protocols for e-mail retrieval.[65] Many webmail service providers such as Gmail, Outlook, and Yahoo! Mail either use IMAP or POP3 to allow e-mails to be downloaded to a local device.[66] Unless specified by the user to the e-mail client to do otherwise, the POP3 server will generally delete the messages from the server.[67]

Simple Mail Transfer Protocol ("SMTP") is the most widely used Internet protocol for delivering e-mail client-side, on a local machine mail applications.[68] These applications typically use SMTP for sending outbound messages to a mail server for relaying.[69] For receiving messages, client applications typically either use the POP3 or IMAP protocols discussed above.[70] Moreover, there are proprietary Internet Protocol ("IP") systems—such as Microsoft Exchange[71]—and webmail systems, like Hotmail, Gmail, or Yahoo! Mail, which use their own non-standard protocols to access e-mail accounts on their own mail servers as an alternative to POP3.[72] However, all webmail systems, use SMTP when sending or receiving e-mail from outside their own systems.[73]

For the purpose of this Note, it will be instructive to briefly describe what happens when someone sends an e-mail message. When someone clicks "send" on an e-mail, the sender's e-mail client connects to the SMTP mail server that the user has associated with the e-mail account.[74] The e-mail client exchanges data with the SMTP server, transmitting the addresses of the sender and recipient, the body of the message, and other information.[75] The SMTP

---

61 *Id.*
62 *Id.*
63 *Id.*
64 Brain & Crosby, *supra* note 45.
65 *Id.*
66 *Id.*
67 *Id.*
68 Electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages. *See id.*
69 *Id.*
70 Brain & Crosby, *supra* note 45.
71 *Id.*
72 *Id.*
73 *See id.*
74 *Id.* (explaining what happens when a client sends an e-mail).
75 *Id.*

server takes the "to" address, such as johndoe@example.com, and breaks it into two parts—the recipient's unique identifier (e.g., the "name") to the left of the "@" symbol and the domain name to the right of the symbol.[76] If the recipient is in the same domain as the sender, the e-mail delivery server would simply hand the message to its retrieval server—the POP3 or IMAP systems as detailed earlier.[77] If the recipient is at another domain, then the SMTP server will relay the data representing the e-mail message to that domain.[78] To accomplish this, the delivery server sends a signal to a Domain Name Server ("DNS") to obtain the IP address of the receiver server for the recipient's e-mail domain.[79] The DNS replies with one or more IP addresses for the SMTP server associated with the recipient's domain.[80] The sender's e-mail delivery server then connects with the recipient's retrieval server for the recipient's e-mail domain, and transfers the message to the recipient server.[81] The recipient server, if it recognizes the recipient's domain name, then transfers the message to the recipient e-mail domain's POP3 server, which puts the message in the appropriate mailbox.[82]

II. THE STORED COMMUNICATIONS ACT

E-mail communications are subject to certain privacy protections under United States law.[83] The Stored Communications Act ("SCA") governs the privacy rights of individuals and legal obligations of electronic communications service providers, such as Microsoft's Outlook e-mail service, with respect to disclosure of information regarding stored communications, including both the content of e-mails and associated addressing and account information.[84] The SCA was passed as part of the Electronic Communications Privacy Act ("ECPA") of 1986 and is codified at 18 U.S.C. §§ 2701-2712.[85]

---

76 Brain & Crosby, *supra* note 45.

77 *Id.*

78 *Id.*

79 *See How does email work? A simple (illustrated) explanation,* VISION DESIGN GRP. (Feb. 24, 2010), https://www.visiondesign.com/how-does-email-work-a-simple-illustrated-explanation (explaining the process of sending outgoing emails).

80 Brain & Crosby, *supra* note 45.

81 *Id.*

82 *Id.*

83 CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2012), http://fas.org/sgp/crs/misc/R41733.pdf.

84 *See* Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012); *see also* 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, 1208 (2004) [hereinafter Kerr, *User's Guide*] (stating the SCA was enacted as a part of the Electronic Communications Privacy Act).

85 For a comprehensive overview of the Electronic Communications Privacy Act, *see*

The SCA establishes three different ways that the government can obtain information from a service provider: a subpoena, court order, and/or warrant.[86] The instrument that the government uses matters because "[t]he instrument law enforcement agents utilize dictates both the showing that must be made to obtain it and the type of records that must be disclosed in response."[87] A subpoena requires the least in the way of a government showing of need for the information, but only provides access to basic account information and related material, not the content of e-mails.[88] A warrant requires the most robust showing but, if approved by a court, permits the government to fully access e-mail content.[89] The court order procedure requires an intermediate showing by the government but provides less data than available under a warrant.[90] This statutory structure is designed to protect the privacy of Internet users.[91]

Indeed, the SCA created "a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."[92] As George Washington University Law Professor Orin Kerr aptly described: "The SCA acts as both a shield and a sword. On one hand, it has a provision forbidding providers to divulge communications unless an exception applies…on the other hand, one of the exceptions is a provision requiring providers to comply with the appropriate legal process."[93] In other words, "[a]s the Fourth Amendment does not protect information that individuals have voluntarily turned over to a third party…the SCA was passed to provide privacy protections that would otherwise be absent."[94] On the other hand, the SCA provides the government with three direct legal instruments to compel a provider to disclose certain personal records if it is necessary for criminal investigation.[95] The *Microsoft* case deals with the disclosure of e-mail content, and the use of each of the statutory means to obtain the content of an e-mail is outlined below.[96]

Doyle, *supra* note 83, at 7-34.

86 18 U.S.C. § 2703(b).

87 *In re* Microsoft, 15 F.Supp.3d at 468.

88 *See* RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 5 (2015), https://www.fas.org/sgp/crs/misc/R44036.pdf.

89 *Id.*

90 Kerr, *User's Guide*, *supra* note 84, at 1219.

91 *See* S. REP. NO. 99-541, at 3-5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3357-59 (describing the legislative history of the Electronic Communications Privacy Act).

92 Kerr, *User's Guide*, *supra* note 84, at 1212.

93 Kerr, *Legal Protections, supra* note 13.

94 Privacy Law – Stored Communications Act – District Court Holds that SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign Servers, *supra* note 13.

95 18 U.S.C. § 2703(b).

96 Privacy Law – Stored Communications Act – District Court Holds that SCA Warrant

A. ADMINISTRATIVE SUBPOENA

Under 18 U.S.C. § 2703(b)(1)(B)(i), the contents of wire or electronic communications in a remote computing service[97] ("RCS") that have been in storage for *more than six months* (180 days) may be obtained by the government "with prior notice from the governmental entity to the subscriber or customer if the governmental entity—(i) uses an *administrative subpoena* authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena."[98] Because obtaining e-mail content by means of a subpoena requires "prior notice" to the subscriber,[99] this will often not be an effective technique in the case of an ongoing criminal investigation of the sort at issue in *Microsoft.*

B. COURT ORDER

Under 18 U.S.C. § 2703(d), the content of wire or electronic communications in a remote computing service and records concerning electronic communication service or remote computing service may be obtained by the government via a court order, "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"[100]

Obligates U.S. Provider to Produce Emails Stored on Foreign Servers, *supra* note 13.

97 18 U.S.C. § 2703(b)(1)(B)(i); 18 U.S.C. § 2711(2) ("[T]he term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.").

98 18 U.S.C. § 2703(b)(1)(B)(i). The content of e-mails less than six months old can only be obtained by means of a warrant. 18 U.S.C. § 2703(a). One circuit has concluded that in the normal course users have a reasonable expectation of privacy with respect to the content of their e-mails generally, which means that under the Fourth Amendment (not, literally, under the SCA), a warrant is required for the government to obtain access to any e-mails. *See* United States v. Warshak*,* 631 F.3d 266 (6th Cir. 2010). The statute's distinction between older and newer e-mails likely reflects Congress's understanding of e-mail technology as it existed in 1986. *See* Brief for Appellants, United States of America v. Steven Warshak, Harriet Warshak, and Tci Media, Inc., 631 F.3d 266 (6th Cir. 2010) (No. 08-3997); As discussed below, in *Microsoft,* the Government obtained a warrant, so the distinction is irrelevant in that context.

99 18 U.S.C. § 2703(b)(1)(B)(i)-(ii).

100 Moreover, "[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." 18 U.S.C. § 2703(d).

C. WARRANT

Under 18 U.S.C. § 2703(a), the government may compel the production of content within an electronic communication in electronic storage, but only if it is pursuant to a warrant.[101] Specifically:

> 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.[102]

The warrant provision within the SCA under 2703(a) also attaches the disclosure of stored contents of electronic communication covered by an administrative subpoena:

> 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.[103]

III. *MICROSOFT CORPORATION V. UNITED STATES*

On December 4, 2013, Magistrate Judge Francis of the U.S. District Court for the Southern District of New York issued a search warrant for a specified e-mail account maintained by Microsoft that was the subject of a criminal investigation.[104] The warrant authorized, among other things, production of the "contents of all e-mails stored in the account, including copies of e-mails sent from the account."[105]

Microsoft's Global Criminal Compliance ("GCC") team, which is responsible for responding to search warrant requests for stored electronic information, complied with the warrant insofar as it called for the production of non-content information from the target account stored on servers within the United States.[106] However, Microsoft determined that the account itself, along with the content of the e-mails, was hosted and stored in servers located within data centers in Ireland.[107] Consequently, Microsoft moved to quash the search warrant, on the grounds that the warrant was invalid to the extent that it the required the retrieval of records from a server located outside the territory of the

---

101 *Id.* § 2703(a).
102 *Id.*
103 *Id.*
104 *In re* Microsoft, 15 F.Supp.3d at 467-68.
105 *Id.* at 468.
106 *Id.*
107 *Id.*

United States.[108] According to Microsoft, that requirement amounted to an impermissible "extraterritorial" application of the warrant.[109]

On April 25, 2014, Magistrate Judge Francis denied Microsoft's motion.[110] Judge Francis ruled that "[e]ven when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law."[111] On July 31, 2014, the District Court affirmed the Magistrate's decision, but stayed enforcement of the ruling pending appeal.[112] The Government then moved to lift the stay, which the District Court granted on August 29, 2014.[113] Microsoft still refused to comply with the warrant, and was subsequently held in contempt by the District Court.[114] The case was appealed to the Second Circuit, which heard this case on September 9, 2015; the court's ruling has not yet been announced.[115]

Like other American internet companies providing commercial e-mail services, Microsoft stores customers' e-mail messages in data centers, which are physical facilities containing clusters of networked computer servers that may be used for remote storage, processing, or electronic transmission of data.[116] Major commercial entities such as Microsoft maintain data centers both around the United States and abroad.[117] Where a customer's e-mail data is stored often, but not always, depends on which data center is closest to the user; this business practice is undertaken in order to reduce network "latency," which refers to the lag time between when a user requests information from the network and the time it is received.[118] The greater the transmission distance between the

---

[108] *Id.*

[109] *Id.* at 467.

[110] *Id.* at 468; *see* Joseph Ax, *U.S. Judge Rules Search Warrants Extend to Overseas E-mail Accounts*, REUTERS (Apr. 25, 2014, 6:41 PM), http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425.

[111] *In re* Microsoft, 15 F.Supp.3d at 477 (provides explanation about the 'presumption against extraterritorial application of American law').

[112] Order Affirming the Decision of Magistrate Judge, *In re* Microsoft, 15 F.Supp.3d 466 (S.D.N.Y. Aug. 11, 2014) (No. 80).

[113] Memorandum and Order Granting the Government's Motion to Lift the Stay of Execution, *In re* Microsoft, 15 F.Supp.3d 466 (S.D.N.Y. Aug. 29, 2014) (No. 90).

[114] Stipulation Regarding Contempt Order, *In re* Microsoft, 15 F.Supp.3d 466 (S.D.N.Y. Sept. 8, 2014) (No. 92).

[115] Amended Notice of Appeal, *In re* Microsoft, 15 F.Supp.3d 466 (S.D.N.Y. Aug. 29, 2014) (No. 95).

[116] Margaret Rouse, *data center definition*, WHATIS.COM, http://whatis.techtarget.com/definition/datacenterdefintion (last visited Mar. 8, 2015) ("A data center (sometimes spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.").

[117] *In re* Microsoft, 15 F.Supp.3d at 467.

[118] *Id.*; *see also* Brief of Computer and Data Science Experts as Amici Curiae Supporting Appellant at 15, Microsoft Corp. vs. United States, No. 14-2985-cv (2d Cir. Dec. 15, 2014).

customer and the data center, the more latency will occur when delivering the requested data.[119] Overall, latency is affected by the data's travel distance, the transmission medium,[120] and the number of switching points along the way, called "router hops".[121] In the case of Microsoft, the "country code" that a user enters when setting up an account may prompt the company to migrate the account's information to a data center in or near the specified country.[122] Other factors may also affect where the company chooses to store the account data. When an account is migrated to a server abroad, most of the "content" and some of the "non-content" information are subsequently deleted from the U.S. based servers.[123]

The dispute in the *Microsoft* case does not involve any claim that the government failed to justify the issuance of the warrant *per se*.[124] The dispute also does not involve any claim that it would be technically difficult for Microsoft, in the United States, to retrieve the data called for by the warrant from the distant server in Ireland.[125] Instead, the legal and policy disputes relate to whether the SCA can or should properly be read to permit the issuance of warrants that

---

> While network latency is often measured in fractions of a second, these seemingly infinitesimal delays have dramatic effects. One study found, for example, 'that a half-second delay causes a 20 percent drop in traffic on Google, and a one tenth of a second delay can lower Amazon's sales by 1 percent.

Id.

[119] *In re* Microsoft, 15 F.Supp.3d at 467.

[120] *Latency*, WHATIS.COM, http://whatis.techtarget.com/definition/latency (last visited Mar. 8, 2015) (e.g., fiber optics versus copper wires or coaxial cable).

[121] *Id. See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? 54 (2008).

> "Bandwidth limitations illustrate an important but poorly understood fact: the efficacy of Internet communications depends on the real-space location of both data and the underlying Internet hardware through which the data travel (routers and exchange points, and the fiber-optic cables, phone lines, cable lines, and microwave and satellites transmitters and receptors that interconnect them."

Id.

[122] *In re* Microsoft, 15 F.Supp.3d at 467 (For example, if a user enters "China" in the country code at registration, Microsoft may then migrate the account to a server located closest to the user in mainland China, or perhaps in the case of Google, Hong Kong.)

[123] *Id.*

> The non-content information that remains in the United States when an account is migrated abroad falls into three categories. First, certain non-content information is retained in a data warehouse in the United States for testing and quality control purposes. (A.B. Decl., ¶ 10). Second, Microsoft retains "address book" information relating to certain web-based e-mail accounts in an "address book clearing house." (A.B. Decl., ¶ 10). Finally, certain basic non-content information about all accounts, such as the user's name and country, is maintained in a database in the United States. (A.N. Decl., ¶ 10).

Id.

[124] *Id.* at 466.

[125] *Id.* at 467-70.

require the retrieval of information from servers located on foreign soil and the production of that information in the United States; and the practical effects that production would have on U.S. foreign relations.[126]

A. Microsoft's Arguments

Microsoft argued that under 18 U.S.C. § 2703(a), the government may require the disclosure of the content of electronic communications "only pursuant to a warrant issued *using the procedures described in the Federal Rules of Criminal Procedure*."[127] The rule in question, Rule 41, limits the geographical areas that may be covered by a search warrant.[128] Federal courts do not have the authority to issue warrants for the search and seizure of property outside the territorial limits of the United States and therefore, Microsoft argued, the warrant in question was invalid to the extent that it required production of data from computer servers in Ireland.[129] More broadly, Microsoft argued that under well-established Supreme Court precedent, statutes are presumed *not* to have any extraterritorial effect unless Congress clearly indicates that extraterritorial effect is intended.[130] According to Microsoft's appellate brief, "[t]he 'cluster of ideas' that attends the term 'warrant' includes the understanding that ordinarily 'United States district judges possess no extraterritorial jurisdiction'—no jurisdiction even beyond their own *districts*—and thus may not issue warrants for searches and seizures abroad."[131] Microsoft argued that it would be inconsistent with that precedent to interpret the SCA as authorizing extraterritorial warrants in any case.[132] Microsoft emphasized the Irish government and other international entities had already raised objections to a United States court purporting to authorize search and seizure of data stored in Ireland.[133] These governments, clearly unsettled by the U.S. government's perceived overreach, are under-

---

126 *Id.* at 469-77.

127 *Id.* at 470.

128 *See* Lily Hay Newman, *Google Says Proposed DoJ Warrant Tweaks Are "Monumental" Fourth Amendment Violation*, SLATE.COM (Feb. 19, 2015, 12:10 PM), http://www.slate.com/blogs/future_tense/2015/02/19/google_says_proposed_doj_rule_41_revision_is_monumental_fourth_amendment.html (remarking that the Department of Justice is taking steps to revise FRCP 41 and that "[t]he DoJ wants judges to be able to issue warrants even if the source of a botnet or other anonymous action is unknown"); Memorandum from David Bitkower to the Honorable Reena Raggi 2 (Dec. 22, 2014) (on file with the U.S. Department of Justice Criminal Division).

129 *In re* Microsoft, 15 F.Supp.3d at 470.

130 *Id.* at 466-70.

131 Weinberg v. United States, 126 F.2d 1004, 1006 (2d Cir. 1942).

132 Brief for Appellant at 22, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 8, 2014).

133 Reply Brief for Appellant at 15, Microsoft Corp. v. United States, No. 14-298d-cv (2d Cir. Apr. 8, 2015).

standably pushing back with data protection measures.[134]

1. Amicus Brief supporting Microsoft

In an *amicus brief* supporting Microsoft, Verizon Communications Inc., Cisco Systems, Inc., Hewlett-Packard Co., Ebay Inc., Salesforce.com, Inc., and Infor argued that the scope of the District Court's ruling was excessive.[135] These entities argued that permitting the United States government to obtain unilateral access to customers' stored communications overseas could harm American businesses.[136] In this line of reasoning, if it became known that the United States government could access information stored overseas, customers in foreign nations would be reluctant to entrust their data to any U.S.-based company.[137] This problem, these tech entities argue, "affects not only the e-mail service at issue in the case, but a host of other communication services, data storage providers, and technology companies."[138] Second, "[i]t will expose American businesses to legal jeopardy in other countries and damage American businesses economically."[139] Third, "[i]t will upset our international agreements and undermine international cooperation. And it will spur retaliation by foreign governments, which will threaten the privacy of Americans and non-Americans alike."[140] Many of these corporations do business internationally and are therefore subject to the laws of foreign nations, thus, they are understandably concerned about the impact that an unfavorable ruling in the Microsoft case could potentially have on their ability to compete with foreign competitors. Furthermore, an unfavorable ruling could attenuate their justifications for resisting foreign governments request for similar data in the past.

B. Government's Arguments

1. Possibly Ambiguous Statutory Language

The Government argued that the SCA is at worst ambiguous on the question of the statute's territorial application, and at best susceptible to a favorable in-

---

134 *Id.*
135 Brief of Verizon Commc'ns Inc., et al. as Amici Curiae Supporting Appellant at 4, Microsoft Corp. vs. United States, No. 14-2985-cv (2d Cir. Dec. 15, 2014).
136 *Id.* at 6.
137 *Id.* at 10-11.
138 *Id.* at 4.
139 *Id.*
140 *Id.*

terpretation for territoriality.[141] The pertinent portion of the SCA 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 … by a court of competent jurisdiction.[142]

"Using the procedures described," in the above excerpt, could have two very different meanings. Microsoft argued that this phrase incorporates all aspects of the Federal Rules of Criminal Procedures into section 2703(a), including the territorial limits on the scope of search warrants under Rule 41.[143] The Government, in contrast, argued only the procedural aspects of Rule 41 was applicable, and that the substantive rules governing the territorial scope of warrants are derived from other legal sources.[144] Indeed, given the unique characteristics of electronic mail, to copy all the features of the search warrants covering physical evidence— limitations on territoriality included—onto electronic communications and other digital evidence would render the instrument impracticable.[145] Both interpretations are plausible.

2. No Extraterritoriality

On the issue of the extraterritoriality, however, the Government's argument is more persuasive. Directly contrary to Microsoft and the *amici,* the Government argues that the SCA "does not implicate principles of extraterritoriality."[146] Microsoft argued that the presumption against territorial application invalidates the warrant because warrants are limited to territories under U.S. jurisdiction.[147] Indeed, "[w]hen a statute gives no clear indication of an extraterritorial application, it has none…and reflect[s] the 'presumption that United States law governs domestically but does not rule the world.'" [148] The Government, in contrast, claims that it is asking Microsoft, a corporation headquar-

---

[141] *In re* Microsoft, 15 F.Supp.3d at 470-72.

[142] 18 U.S.C. § 2703(a).

[143] Brief for Appellant at 23, Microsoft Corp., No. 14-2985-cv (2nd Cir. Mar. 9, 2015).

[144] *See In re* United States, 665 F.Supp.2d 1210, 1219 (D.Or. 2009) ('Issued' may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as a shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41.").

[145] *See* Brief for the United States of America at 25, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Mar. 9, 2015) (citing United States v. Berkos 543 F.3d 392, 398 (7th Cir. 2008)).

[146] *In re* Microsoft, 15 F.Supp.3d at 472.

[147] Brief for Appellant at 34-35, Microsoft Corp., No. 14-2985-cv (2nd Cir. Mar. 9, 2015).

[148] Kiobel v. Royal Dutch Petroleum Co., 569 U.S. ___, 133 S.Ct. 1659, 1664 (2013) (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010)).

tered in the United States, to issue certain commands from its computers, in the United States, in response to a United States subpoena.[149] From this perspective, the Government argues, the fact United States computers will retrieve information from servers that happen to be located overseas is legally irrelevant.

IV. ANALYSIS

Defining the territory that is under United States jurisdiction is a key element of this case.[150] Territorial jurisdiction may refer to jurisdiction over cases arising in or involving persons residing within a defined territory.[151] Territory is typically demarcated by physical boundaries.[152] However, territory can encompass areas over which a government, one of its courts, or one of its subdivisions has jurisdiction.[153] If a court does not have jurisdiction over the events or persons within it, then the court will not be able to bind someone to an obligation or adjudicate their rights.[154] Territorial jurisdiction can be waived, even unintentionally, by a defendant.[155] In the case before the Second Circuit, if territorial jurisdiction is defined by the location of the communications provider, then the Government's act would be territorial since it is obtaining the data from Microsoft, a company operating in the United States, with its corporate headquarter in Washington State.[156] On the other hand, if the territorial jurisdiction is defined by where the communication is stored, then the Government's actions would be extraterritorial, as could also be the case in *Microsoft*, with the data being stored in Ireland.

A. District Court's Ruling

1. Statutory Ambiguity

The District Court, agreeing with the Government's position, pointed out

---

149 Brief for the United States of America at 4, Microsoft Corp, No. 14-2985-cv (2nd Cir. Mar. 9, 2015).

150 *See generally In re* Microsoft, 15 F.Supp.3d at 470-77.

151 Jurisdiction, BLACK'S LAW DICTIONARY (10th ed. 2014).

152 *Id.*

153 *Id.*

154 *Territorial Jurisdiction Law & Legal Definition*, U.S. LEGAL, http://definitions.uslegal.com/t/territorial-jurisdiction/ (last visited Sept. 13, 2015).

155 *Id.*

156 *Microsoft Worldwide Sites*, MICROSOFT, https://www.microsoft.com/worldwide/phone/contact.aspx?country=United%20States (last visited Nov. 15, 2015).

that the SCA's language was ambiguous, and thus "a court must search beneath the surface of text that is ambiguous…."[157] The Court explained, "when construing the meaning of a statute, this Court will 'look not only to the particular statutory language, but also the design of the statute as a whole and to its object and policy."[158] The District Court noted that using the Federal Rules of Criminal Procedure could plausibly be understood as meaning either that the entire rule is incorporated, or that only the procedural aspects of the warrant process from Rule 41 is incorporated, with more substantive rules derived from other sources.[159] The District Court concluded that in light of this ambiguity, the Court must look at the "'statutory structure, relevant legislative history, [and] congressional purposes.'"[160]

2. Unique SCA Structure of Hybrid Warrant-Subpoena

In order to avoid the strict territorial limits on conventional warrants, the Government argued that an SCA warrant is "not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena."[161] In a seminal case repeatedly cited by the government to demonstrate the authority of the court to compel disclosure of records located abroad with a subpoena, the Second Circuit held that "[i]t is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has *in personam* jurisdiction of the person in possession or control of the material."[162] The court reasoned that like a conventional search warrant, an SCA warrant is issued by a neutral magistrate upon a showing of probable cause.[163] In contrast to a conventional warrant, however, an SCA warrant is executed like a subpoena:[164] "a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information."[165] That is, compelling an entity under the court's jurisdiction

---

157 *In re* Microsoft, 15 F.Supp.3d at 470.

158 Brief for the United States at 48, Microsoft Corp., No. 14-2985-cv (2d Cir. Mar. 9, 2015) (citing Johnson v. United States, 123 F.3d 700, 702 (2nd Cir. 1997)).

159 *See In re* Microsoft, 15 F.Supp.3d at 470.

160 *Id.* at 471.

161 *Id.* at 471-74 ("if an SCA Warrant were treated like a conventional search warrant, it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty ("MLAT")).

162 Brief for the United States of America at 14, Microsoft Corp. v. United States, No. 14-2985 (2d Cir. Dec. 8, 2014) (citing United States v. First Nat. City Bank, 396 F.2d 897, 900-01 (2d Cir. 1968)).

163 *In re* Microsoft, 15 F.Supp.3d at 471.

164 *Id.*

165 *Id.* at 472 (citing Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983) ("Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location.")).

to produce information under its control—even if located overseas—is a legally accepted practice in response to a subpoena. As noted earlier, a "subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information."[166] A SCA warrant is executed like a subpoena as it "does not involve government agents entering the premises of the [service provider] to search its servers and seize the e-mail account in question,"[167] but rather, requires the recipient to produce the information in its control.

On the issue of control, Microsoft argues that the sender of the e-mail remains in legal "constructive possession" and therefore, under *United States v. Guterma*, a subpoena would not be able to compel a "third-party naked possessor to produce and deliver them."[168] In *Guterma*, the Court quashed a subpoena that sought to compel a company to produce the personal papers of its chairman.[169] Where the company chairman's personal papers were stored in a safe within the office and not governed by any specific terms of use, all users of Microsoft web e-mail services have to first agree to be bound by the company's terms of services, which basically confers possession of the e-mails to Microsoft so that the e-mails can become part of Microsoft's files and records.[170] According to the Government, "the terms of service currently applicable to Microsoft's free email service do not suggest a mere caretaker or trust relationship. Rather, they assert Microsoft's right to access or use the contents of its customers' e-mails."[171] The District Court accepted this argument.[172]

---

166 *Id.*

167 *Id.* at 471-72.

168 Brief for Appellant at 46-47, Microsoft Corp., No. 14-298-cv5 (2d Cir. Dec. 8, 2014) (citing United States v. Guterma, 272 F.2d 344, 346 (2d Cir. 1959)).

169 *Id.* at 47.

170 The *amici curiae* of media organizations raise an interesting concern about the hybrid approach: "In particular, the court's formulation of a "hybrid" subpoena-warrant combination … muddies the protections of the Privacy Protection Act, 42 U.S.C. § 2000aa, and the recently revised DOJ policies, codified at 28 C.F.R. § 50.10." Brief of Media Orgs. as Amici Curiae Supporting Appellant, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 15, 2014).

171 Brief for the United States at 41-42, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8, 2014).

> When you transmit or upload Content [i.e., the text of e-mails] to the Services, you're giving Microsoft the worldwide right, without charge, to use Content as necessary: to provide the Services to you, to protect you, and to improve Microsoft products and services" and "To ensure that users comply with Microsoft's "Code of Conduct," Microsoft uses "automated technologies" to review the content of e-mails, and separately, when "investigating" possible violations, "Microsoft or its agents will review Content in order to resolve the issue."

Id.

172 *In re* Microsoft, 15 F.Supp.3d at 477.

Lastly, Microsoft argues that "*Marc Rich* sits in uneasy tension with the presumption against extraterritoriality; it should not be extended to grant the Government the extraordinary power it seeks here."[173] That said, as Microsoft is a United States entity, on this reasoning, the information should be produced even though it is located in Ireland.[174]

Even so, e-mails are oftentimes mistakenly characterized as private to the privacy advocates' chagrin.[175] Part of the problem when dealing with e-mail privacy is that many people generally have a misguided idea about how e-mail actually works.[176] This misconception is fueled by reference to the most common analogy, which is that an e-mail is akin to a traditional letter that we would put in an envelope and seal. The act of sealing the letter in an envelope demonstrates an expectation of privacy that it would only be opened and read by the recipient.[177] In reality, an e-mail operates more like a post-card.[178] No one can reasonably expect the content of a postcard to remain private, since its contents are in plain sight from the time it leaves the hands of the addressor. Yet, by simple analogy, we assume an expectation of privacy in the e-mails that we send. If people really want to keep their e-mails private, then users should encrypt them. Doing so would make the e-mail more akin to a traditional letter, since the encryption would, metaphysically speaking, serve as the envelope and represent the user's expectation of privacy.[179]

3. Legislative History

The District Court also analyzed the SCA's legislative history. The court agreed with the Government's views that legislative history is not clear and

---

[173] Brief for Appellant at 17, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8 2014).

[174] *See generally In re* Microsoft, 15 F.Supp.3d at 477.

[175] Kara Brandeisky, *5 Things You Didn't Know About Using Personal Email at Work*, TIME (Mar. 3, 2015), http://time.com/money/3729939/work-personal-email-hillary-clinton-byod/.

[176] Erik Kangas, *The Case for Email Security*, LUXSCI FYI BLOG, https://luxsci.com/blog/the-case-for-email-security.html (last visited Mar. 31 2015).

[177] Law enforcement has legal recourse to open letters, so Congress should not limit law enforcement's ability to similarly open e-mails. *See, e.g.*, U.S. v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001)).

[178] Andy Yen, *Think your e-mail's private? Think again*, TEDGlobal (Oct. 2014) (transcript available at http://www.ted.com/talks/andy_yen_think_your_email_s_private_think_again/transcript?language=en).

[179] For a brief discussion on the on-going debate about the trade-off between privacy through encryption and national security, *see, e.g.*, Ellen Nakashima & Barton Gellman, *As encryption spreads, U.S. grapples with clash between privacy, security*, WASH. POST, (Apr. 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

could be read to support either party.[180] However, a U.S. Senate report cited by the court, in discussing the nature of networked computers, acknowledged that "businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services."[181] This appears to reflect Congressional intent that the statute would cover information that would, at the very least, be transmitted and processed by computers located remotely and off site.

A U.S. House of Representatives report was clearer about the territorial demarcation of the law. The report states: "the controls in Section 201 of the Act [which became the SCA] regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States."[182] Despite this seemingly clear language, the District Court asserted that the statement was "ambiguous."[183] The District Court found that the case law relied upon by the Committee in reaching its conclusion on territoriality was flawed, because the case cited to addressed only the individual rights created by ECPA and not the territorial reach of the government's authority.[184]

Even if Congress wrongly understood the cases cited in the legislative history, its intent in passing the law would be defined by what it actually understood, wrongly or not. More plausibly, the District Court noted that the Committee's use of the word "access" did not clearly delineate whether it applied to "access to the location where the electronic data was stored or access to the location of the ISP in possession of the data."[185] As additional support for the claim that the relevant location is the location of the ISP, not the location of the server holding the data, the court cited the 2001 "USA PATRIOT Act," passed in the aftermath of the terrorist attack against the United States on September 11, 2001.[186]

Section 108 of the USA PATRIOT Act amended the law "to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located."[187] The amendment seems to indicate that Congress foresaw the

---

180 *In re* Microsoft, 15 F.Supp.3d at 472-74.
181 S. REP. NO. 99-541, at 3 (1986).
182 H.R. REP. NO. 99-647, at 32-33 (1986).
183 *In re* Microsoft, 15 F.Supp.3d at 473 (citing H.R. REP. NO. 99-647, at 32-33 (1986)).
184 *Id.* at 470.
185 *Id.* at 473.
186 *Id.* at 473-474 (citing H.R. REP. NO. 107–236(I), at 58 (2001)).
187 *Id.* at 474 (citing H.R. REP. NO. 107–236(I), at 58 (2001)); *see* Kerr, *Legal Protections, supra* note 13 ("From 1986 until 2001, the required under [under 2703(a)] was called 'a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant … [t]he change apparently reflects an attempt to clarify that the order is not a traditional Rule 41 search warrant, but rather merely a hybrid order issued using the procedures of Rule 41.").

SCA Warrant's utility as being qualitatively different from a conventional warrant. The counter argument would be that the PATRIOT Act expanded the scope of a given court's warrants to include the entire United States, but did not purport to authorize extraterritorial application.[188] But as even Microsoft recognized in its brief, "Congress did this because 'the cross-jurisdictional nature of the Internet' led to 'investigative delays' as officers sought warrants in other districts."[189] Indeed, it would be a glaring legislative oversight if, after the devastating attacks on the U.S. homeland caused by foreign-based terrorists, Congress will limit the necessary expansion of investigative capabilities that could stem such attacks in ways that Microsoft suggest.

In light of the ambiguities with the law, the Court made a balancing decision that weighed heavily on the practical considerations that it considered to tilt the scale in favor of the government's position. Nonetheless, this raises questions as to whether this approach really is as practical as the Government makes it out to be.

B. Mutual Legal Assistance Treaties

One tangential aspect of the dispute in *Microsoft* is the availability and efficacy of alternative means for the government to get access to data stored overseas. In *Microsoft,* there is no dispute that the company could technically and entirely, from within the United States, retrieve the requested information from Ireland.[190] Webs of bilateral and multilateral agreements make up a system to facilitate criminal investigations and prosecutions in the nations that are parties to them.[191] MLATs are the backbone of global cooperation among law enforcement agencies in cases that involve, but are not limited to, "locating and extraditing individuals, freezing assets, requesting searches and seizures, and taking testimony."[192] Here, the Government argued, and the District Court accepted, the claim that MLATs are often inefficient and slow.[193] On appeal, Microsoft vigorously disputes this view, noting that as it is relevant to this particular case, the United States and Ireland have established procedures for han-

---

188 Brief for Appellant at 23, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8, 2014) ("As discussed below [at 25-26], Congress changed this language in 2001, but only to make warrants effective '*Nation*wide,' not *world*wide.").

189 H.R. REP. NO. 107-236, at 57 (2001).

190 *Id*.

191 For instance, in the case of counter-narcotics, *see 2012 INCSR: Treaties and Agreements,* U.S. DEP'T OF STATE (Mar. 7, 2012), http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

192 Hill, *supra* note 16.

193 *Id.* ("The President's Review Group on Intelligence and Communication Technologies … estimates that it takes an average of ten months for DOJ to process MLAT requests, and can take years.").

dling international requests for information on an expedited basis.[194]

As the world "flattens"[195] digitally in the twenty-first century with ascent of the information revolution, more data is moving online—including that of criminals and their victims; the MLAT system has been slow in keeping pace with the rapid changes of data globalization.[196] Indeed, the DOJ estimates that over the past decade the "number of [MLATs] requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs has increased by nearly 60 percent, and the number of requests for computer records has increased ten-fold."[197] In light of this growth in reliance on MLAT requests, much must be done to address the issues of jurisdiction over cross-border data transfers, privacy, and legitimate law enforcement needs for evidence.[198] In this regard, Congress attempted to streamline MLAT in 2009 by making it easier for DOJ to obtain evidence on behalf of foreign counterparts.[199] As early as 2014, the Obama Administration was considering new legislative proposals to further expedite the MLAT process.[200]

Herein lies a key policy aspect of the problem raised by *Microsoft* concerning the Government's unilateral acquisition of foreign-stored data. MLATs typically include provisions that require the requesting party to agree not to bypass the MLAT by unilaterally obtaining evidence in the territory of the state where the evidence is located, and instead to only obtain such evidence in compliance with the law of that state.[201] As relevant to *Microsoft,* the United States has an MLAT with Ireland, and Irish Law requires authorizations from an Irish District Court Judge to obtain the content of e-mails from an electronic

---

194 Brief for Appellant at 58, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8, 2014).

195 THOMAS FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY 8 (2005) (defining "flat" as "connected": the lowering of trade and political barriers and the exponential technical advances of the digital revolution have made it possible to do business, or almost anything else, instantaneously with billions of other people across the planet).

196 Hill, *supra* note 16.

197 U.S. DEP'T OF JUSTICE, FISCAL YEAR 2015 BUDGET REQUEST: MUTUAL LEGAL ASSISTANCE TREATY PROCESS REFORM 1 (2015), http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

198 Hill, *supra* note 16 ("For example, MLATs frequently do not specify what constitutes "protected data" or under what conditions "content" differs from "metadata" for the purposes of information sharing.").

199 *Liberty and Security in a Changing World*, PRESIDENT'S REV. GRP. ON INTELL. & COMMC'NS TECH. 158 (Dec. 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

200 Press Release, U.S. Dep't of Justice, Off. of the Attorney Gen., Attorney General Holder Announces President Obama's Budget Proposes $173 Million for Criminal Justice Reform (Mar. 4, 2014) (on file with author).

201 Brief of Verizon Commc'n, Inc. et al. as Amici Curiae Supporting Appellant at 15, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

communications provider.[202]

Some commentators have described MLATs as an expression of state sovereignty.[203] Yet, there great ambiguity regarding state sovereignty within cyberspace—if it even practicable to think in terms of traditional sovereignty in cyberspace. The Internet is a distributed network[204] of networks that is transnational in scope, with servers and routers that store, process, and switch information located essentially anywhere in the world.[205] Although a government must have the right to legitimately regulate activities that have a substantial effect within its territory, the cross-border nature of the Internet necessarily involves legal regimes that extend beyond the national law of a country. Indeed, "international law has traditionally allowed countries nearly unlimited power to make law territorially subject only to some specific prohibitions, like the human rights norms against genocide and torture."[206] Moreover, "[t]he power to regulate extraterritoriality, while broad, is not unlimited: a state may make law governing 'conduct outside its territory that has or is intended to have substantial effect within its territory...'"[207] Given its multinational roots, it is reasonable that the appropriate legal framework to use in Internet governance would include elements of international law.[208] However, an absolutist approach to state sovereignty in cyberspace is untenable for the preservation of the Internet as we know it.

C. Conceptual Solutions

According to Microsoft, "[e]lectronic letters do not become the caretaker's records any more than physical letters do."[209] Rather, an e-mail provider is a mere "*intermediary* that makes e-mail communication possible," and "not the intended recipient of the e-mails"; it is the "functional equivalent of a post of-

---

202 *Id.* at 16.

203 *Id.* at 15-16.

204 HAFNER & LYON, *supra* note 31, at 244.

205 However, as the District Court noted in its decision, network engineering phenomenon such as "network latency" can limit the geographic distance between the server where the user's data is stored and the location of the end user since the quality of the service would decrease the farther the user is from the server. But whether this is an insurmountable challenge remains to be seen.

206 RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 401(1)(c) (AM. LAW INST. 1987); *see also* JAMES GRIMMELMANN, INTERNET LAW: CASES & PROBLEMS 78 (4th ed. 2014) (ebook).

207 RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 401(1)(c).

208 Henry H. Perritt, *The Internet is Changing the Public International Legal System*, 88 KY. L. J. 885, 885-86 (1999).

209 Brief for Appellant at 44, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8, 2014) (citing United States v. Warshak, 631 F.3d 266, 286-88 (6th Cir. 2010)).

fice." [210] The reasoning behind this analogy rests on the possessory interests of the e-mail sender, rather than the e-mail provider, in the 'electronic letter' even after the e-mail is sent.[211] The problem with this analogy as an argument in support of Microsoft's position is that even if a letter does not become the caretaker's record, the contents of a safe deposit box or of a letter inside a FedEx envelope would both nevertheless have to be disclosed if the Government obtained a warrant based on probable cause.[212] The statute's intent could not be to create a safe harbor for digital evidence that may be illegal and to prevent law enforcement from reaching the evidence, no matter the stakes.

Additionally, the technology of "packet switching," the process used by computers to break apart and transmit data over the Internet, makes the transmission of e-mails fundamentally different from letters.[213] In the former, an e-mail would first need to be disassembled and turned into "datagrams,"[214] which would be roughly analogous to unsealing the letter, and sending the letter and envelope separately, and have it reassembled when it reaches its recipient.[215] Thus, the expectation of privacy that one would have in a letter sent through the post office versus e-mail is incongruous. In any case, this distinction highlights an ambiguity that the law has not directly addressed.

One possible conceptual and technical approach to resolving the quagmire that e-mail providers are in, by having to serve as an intermediary, is "disintermediation."[216] In the context of e-mails, this is a process by which the e-mail service providers would be effectively removed from the relationship between the government seeking information and the actual targets of the government's inquiry within the nation-state.[217] Perhaps, e-mail providers ought to encrypt all data stored, processed, and transmitted. While this process could have been an easy solution in the late 1990s, just as the Internet was taking off, it is harder

---

[210] *Id.*

[211] *Id.* at 44-45.

[212] *Id.*

[213] Chris Woodford, *The Internet*, EXPLAINTHATSTUFF (Nov. 19, 2014), http://www.explainthatstuff.com/internet.html.

[214] *See* HAFNER & LYON, *supra* note 31, at 236 ("TCP would be responsible for breaking up messages into datagrams, reassembling them at the other end, detecting errors, resending anything that got lost, and putting packets back in the right order. The Internet Protocol, or IP, would be responsible for routing individual datagrams.").

[215] It is important to note here that "disassembly" is distinct from "sharding" or "partition", which are techniques for splitting large sets of data across several computers. *See* Brief for Computer and Data Science Experts as Amici Curiae Supporting Appellant at 17-19, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

[216] *See Disintermediation*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/disintermediation (last visited Nov. 15, 2015). Disintermediation is defined as "the elimination of an intermediary in a transaction between the two parties." *Id.*

[217] *Id.*

now that the "Internet has made the network itself the intermediary for much conduct that we might have thought had no intermediary at all prior to the Internet."[218] For this solution to work, international standards would have to be developed for e-mail encryption.

Another possible, but radical approach is a total exit solution in which the targets, or Internet users, also leave the jurisdiction of the nation-state, or in common parlance, go "off the grid" by using private, non-commercial, servers.[219] Consequently, the data would not be subject to any country's sovereign jurisdiction.[220]

The current approach taken by some governments to access digital evidence is a process that could be called "source-adhesion." This is a process by which the local intermediary would be required to maintain its records or at least copies of them—including e-mails, in its home country—which would only be accessible by the government upon clearly stipulated and accountable methods to minimize the use of such data.[221] However, with current technologies, this technique would result in greater costs to technology companies, and could cause an increase in network latency and significant inefficiencies in the global Internet network.[222]

A defining feature of the new digital age is data permanence. The growing importance of data collection and big data for various legitimate and less legitimate social, economic, and military purposes, however, is also giving rise to data nationalism.[223] Thus the MLAT system must be updated to provide recourse to the ongoing trend of data centralization and a consolidation of the Internet's network hardware behind territorial boundaries.[224]

As the District Court and other legal commentators have suggested, the MLAT system could be improved in many ways.[225] Yet, the highly discretionary language found in existing MLATs—even between friendly nations such as the United States and Great Britain, which effectively gives the country holding the data an unrestricted ability to deny requests for assistance—creates

---

218 GOLDSMITH & WU, *supra* note 121, at 70.

219 GOLDSMITH & WU, *supra* note 121, at 71.

220 GOLDSMITH & WU, *supra* note 121, at 71.

221 *See generally* 18 U.S.C. § 2703 (2012).

222 *See* Brief for Computer and Data Science Experts as Amici Curiae Supporting Appellant at 16-17, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

223 CASTRO, *supra* note 21, at 1 (arguing that data owners should use "contracts or laws to limit voluntary data disclosures so that data stored abroad receives the same level of protection as data stored domestically").

224 *See* Hill, *supra* note 16

225 *Id.* ("If [MLAT is] left unreformed, or reformed poorly, law enforcement and jurisdictional battles among and between governments and technology firms couple place yet another strain on the already stressed global Internet system.").

a disincentive to use MLATs as a means to acquire digital evidence.[226] Furthermore, if the hybrid subpoena-warrant theory is denied, criminals could evade SCA warrants by simply giving false information and by using techniques to obscure routing with e-mail providers to induce those providers to place the e-mails in an offshore server.[227]

A similar argument was advanced in the Australian libel case of *Dow Jones & Co. v. Gutnick*: "Dow Jones submitted that it was preferable that the publisher of material on the World Wide Web be able to govern its conduct according only to the law of the place where it maintained its web servers, unless that place was merely adventitious or opportunistic."[228] The Australian court disagreed and found, within the context of an action for libel, liability would be determined where the libelous speech was felt. [229] In *Microsoft,* the United States was seeking information about a crime that affected the United States. Therefore, its ability to obtain the required information should not be based on "adventitious or opportunistic" factors affecting where the data are located.[230] That said, if U.S. law enforcement asserts the authority to obtain the content of customers' data stored outside its territorial jurisdiction, foreign governments will be more likely to assert the same authority to obtain data of Americans citizens who come into contact with foreign law.

To put these matters into perspective, the former head of the National Security Agency and of the U.S. Cyber Command, General Keith Alexander, has called the breach of American secrets via cyber espionage "the greatest transfer

---

226 *See* Eric S. Rein & Bethany N. Schols, *Creative New Mechanisms for Banks to Recover Stolen Collateral*, 122 BANKING L. J. 725, 727 (2005).

227 China's government provides us with another radical alternative in that it is forcing its internet-using citizens to register with their real names for the purpose of virtual identification. *See, e.g.*, Josh Chin, *China Is Requiring People to Register Real Names for Some Internet Services*, WALL ST. J. (Feb. 4 2015, 5:43 PM), http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-Internet-users-1423033973 ("The new regulations, to be enforced starting March 1, ban nine categories of usernames, including anything that harms national security, involves national secrets, incites ethnic discrimination or hatred, or harms national unity. Names that promote pornography, gambling, violence, terror, superstition and rumors are also banned, according to the statement.").

228 *See* JAMES GRIMMELMANN, INTERNET LAW: CASES & PROBLEMS 79-85 (4th ed. 2014) (ebook) (citing Dow Jones & Co. v Gutnick [2002] HCA 56 (Austl.)).

229 Dow Jones & Co. v Gutnick [2002] HCA 56 (Austl.), *reprinted in* JAMES GRIMMELMANN, INTERNET LAW: CASES & PROBLEMS 79-85 (4th ed. 2014) (ebook).

230 Another legal argument being advanced by media organizations in opposition to the District Court's decision is that "if upheld, [the decision] will undermine procedural and substantive protections for material that is protected by the First Amendment. Even if the subscriber today is not a reporter – although we do not know for sure – the next subscriber may be." Although the extension of the legal argument presented by Microsoft is reasonable, it does not concern the present case. Thus, it is not directly addressed in this Note. *See* Brief of Media Orgs. as Amici Curiae Supporting Appellant at 2, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

of wealth in history."[231] Whether the United States Government will be able to effectively deal with these types of problems through bilateral diplomacy is questionable. Instead, an efficient system for retrieving information from overseas is needed to assist law enforcement in this effort.[232]

The Internet may have been "borderless" and capable of respecting anonymity at its inception.[233] Indeed in the 1990s, the web was epitomized by its "instant and universal communication, geographic anonymity, and decentralized routing," but these egalitarian principles gave way to criminals using it to hide their tracks online and for "computer users to get illegal information from computers outside the nation."[234] The Internet has consequently transformed into something else. A famous 2000 case revealed that the old conception of the borderless Internet was inaccurate; Yahoo! was confronted by claims from the French legal system that its auction of Nazi memorabilia violated French Law.[235] Yahoo! originally claimed that its servers were not located in France and that it could not tell where the requests to view the items were coming from. [236] In fact, however, the case revealed that "Yahoo!'s servers … were actually located on a website in Stockholm. Yahoo! had placed a constantly updated 'mirror' copy of its U.S. site in Sweden to speed access to the site in Europe."[237] Additionally, it was realized at that time that it is indeed possible in most cases to determine where a user was physically located.[238] A solution to the problem, as discussed in *Microsoft* may be to mandate the use of geographical identification on the Internet.[239] This would allow service providers to store data according to the location of the user.[240] The more this practice is imple-

---

231 John Seabrook, *Network Insecurity*, THE NEW YORKER, May 20, 2013, http://www.newyorker.com/magazine/2013/05/20/network-insecurity.

232 *See generally* Exec. Order No. 13,694, 80 Fed. Reg. 18077, 18077 (Apr. 2, 2015) (imposing economic sanctions on companies that directly benefitted from cyber-hackers).

233 *See generally The Role of Standards in the Growth of Global Economic Commerce: Hearing before the Subcomm. on Sci., Tech., and Space of the S. Comm. on Commerce, Sci., and Transp.*, 106th Cong. 18 (1999) (statement of Andrew B. Whinston, Director, Ctr. for Res. in Elec. Commerce).

234 Jack Goldsmith & Timothy Wu, *Digital Borders*, LEGAL AFFAIRS, Jan.-Feb. 2006 [hereinafter Goldsmith & Wu, *Digital Borders*], http://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp.

235 *See* Yahoo! Inc. v. La Ligue Contre Le Racisme Et, L'antisemitisme, 145 F.Supp.2d 1168, 1171-72 (N.D. Cal. 2001).

236 *Id.*

237 Goldsmith & Wu, *Digital Borders*, *supra* note 234.

238 *See* Dan Jerker B. Svantesson, *"Imagine there's no countries . . ."-Geo-identification, the law and the not so borderless internet*, EPUBLICATIONS@BOND, Feb. 2007, at 1-2, http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1131&context=law_pubs; *see also* Goldsmith & Wu, *Digital Borders, supra* note 234.

239 *See generally* Svantesson, *supra* note 238, at 4.

240 Goldsmith & Wu, *Digital Borders, supra* note 234

IP addresses (like "192.168.0.55") don't readily reveal a computer user's physical

mented, the fewer problems of the sort presented here will arise.

1. A New Matrix

Legal scholars and commentators have attempted to propose the optimal mix of legal instruments for data recovery in piecemeal. For Law Professor Orin Kerr, the solution is to revise the SCA so that it could help to distinguish between:

> [P]eople in the [United States] who use U.S. providers that just happen to store their contents on [foreign servers] (those e-mails should be obtainable with a U.S. warrant), and people abroad whose providers store e-mails abroad but [may] also [just happen to] have an office in the U.S. (those e-mails should be obtained through MLATs).[241]

There are obviously some gaps in Kerr's scenarios. For instance, it seems that the citizenship of the suspect, not merely her physical location, should matter. But this leaves the issue of what should be done with e-mails of a non-citizen residing in the United States, but who has an account with a foreign provider that uses U.S.-based data warehouse storage. The sound idea behind Professor Kerr's proposal is to tie the use of MLATs to the situations in which the interests of the foreign nation are strongest.

The Internet is a distributed network, and the Internet ecosystem is constantly shifting. As part of that evolution, there has been a raft of new measures making their way through foreign governments such as Russia, Brazil, India, and China to impose data localization requirements, under which data relating to a given country's nationals must remain within that county.[242] These kinds of developments could have the eventual effect of fragmenting the Internet. In support of Microsoft in the Second Circuit, Verizon argues that the District Court's interpretation of the SCA will encourage this type of activity, and that Congress—not the judiciary—needs to make an express decision to extend the SCA extraterritorially.[243] Otherwise, if data localization becomes the norm, law enforcement-to-law enforcement cooperation under MLATs will remain the only means for the U.S. government to obtain data located abroad.

> location. But a savvy user can determine that location by sending 'tracing' packets over the Internet . . . when the databases are cross-referenced and analyzed, the location of Internet users can be determined with over 99 percent accuracy at the country level.

Id.

241 *See* Kerr, *Legal Protections, supra* note 13.

242 *See* Gillian Wong, *U.S. Business Group Urges China to Ease Data Restrictions*, WALL ST. J. (Apr. 13, 2015, 10:19 PM), http://www.wsj.com/articles/u-s-business-group-urges-china-to-ease-data-restrictions-1428974445.

243 Brief of Verizon Commc'n Inc., et al. as Amici Curiae Supporting Appellant at 14, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

While it is clear that Congress needs to act, a more comprehensive and nuanced approach is necessary.[244]

SCA WARRANT/MLAT FRAMEWORK
(Is the U.S. government required to use MLATs?)

	Subpoena (S)	**Court Order (C)**	**Warrant (W)**
U.S.-Co. data stored domestically	No[245]	N/A	No[246]
U.S.-Co. data stored abroad	No[247]	N/A	No/Yes[248]
Non-U.S. Co. with subsidiary in U.S.	N/A	N/A	N/A
Non-U.S. Co. in foreign territory	N/A	N/A	N/A

[244] Brief of Appellant at 56, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8, 2014) (according to Microsoft, "Congress might seek to authorize the extraterritorial application of § 2703(a) only for investigations of certain crimes and national security matters. It might extend § 2703(a) to reach e-mails overseas, but only those belonging to U.S. citizens and permanent residents. Indeed, pending Senate bills would do just that. *See* Law Enforcement Access to Data Stored Aboard Act, S. 2871, 113th Cong. §§ 2(4), (3)(a)(2), (3)(a)(5) (2014).").

[245] Somewhat paradoxically, the government's unilateral use of the hybrid warrant may be the most privacy protecting option since subpoena would require a showing of probable cause and other countries privacy standards may not be as high. Hill, *supra* note 16.

[246] *Id.*

[247] *In re* Microsoft, 15 F.Supp.3d at 477.

[248] This quadrant is being decided by the Microsoft case.

SCA WARRANT/MLAT FRAMEWORK
(Should the U.S. government be required to use MLATs?)

	Subpoena (S)	**Court Order (C)**	**Warrant (W)**
U.S.-Co. data stored domestically	No[249]	N/A	No[250]
U.S.-Co. data stored abroad	No[251]	N/A	No[252]
Non-U.S. Co. with subsidiary in U.S.	No[253]	N/A	No/Yes[254]
Non-U.S. Co. in foreign territory	N/A	N/A	N/A

2. U.S.-company with data stored abroad (warrant)

Accepting as the premise that the principle of territoriality should be defined in terms of the company's location, the District Court and the Government have a stronger argument for the validity of using a warrant for obtaining the content of an electronic communication from a U.S.-based company. The SCA, as written, appears to support the government's authority to unilaterally obtain customer records or information from a U.S. company, for records that may be stored abroad, by way of a SCA warrant.[255] A warrant is not a subpoena; but the unique features of digital data, in particular an e-mail, in terms of how it is stored, processed, and transmitted should be taken into account. This distinction should support the treatment of SCA warrants as a hybrid of both a warrant and a subpoena, as suggested by the District Court.[256] While the data

[249] *In re* Microsoft, 15 F.Supp.3d at 477.
[250] Hill, *supra* note 16.
[251] Brief of Media Org. as Amici Curiae Supporting Appellant at 32, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).
[252] Kerr, *Legal Protections, supra* note 13.
[253] Brief of Media Org. as Amici Curiae Supporting Appellant at 14, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).
[254] Kerr suggested that people abroad whose providers store e-mails abroad but also have an office in the U.S. should be obtained through MLATs. Kerr, *Legal Protections, supra* note 13.
[255] *Privacy Law – Stored Communications Act – District Court Holds that SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign Servers*, *supra* note 13, at 1019.
[256] Brief for the United States of America at 23-24, Microsoft Corp., No. 14-2985-cv (2d

would be coming from abroad, in practical terms the distant records would be retrieved from a company headquartered within the United States, and doing so would not require any physical intrusion by United States law enforcement or other personnel onto the territory of the foreign sovereign.

3. Non-U.S. Company with subsidiary in the United States

Territoriality for purposes of the SCA must be clearly defined in terms of the location of the company that controls access to the data, and not the communication itself.[257] In light of the distributed nature of stored data on the Internet, defining the relevant territoriality in terms of the location of the data would create significant problems. Among other things, the location of the data can change over time, based on the business decisions or mere whims of the company storing them. Accordingly, the principle would work both ways: U.S.-based and non-U.S. based. If the U.S. government wanted information relating to an Internet user using a Chinese Internet company such as Baidu, it should have to request it through the MLAT.[258] Yet if Baidu's data center is serving a particular client determined to be located within the United States, the U.S. government should be able to procure such data through a warrant. However, in the case of a subpoena in which only metadata may be disclosed, there is no meaningful invasion of privacy. Therefore, the government should not be required to use the MLAT process.

V. CONCLUSION

The two scenarios offered at the outset of this note do not exactly mimic the Microsoft case, but they serve to underscore the very real challenges that Internet users, Internet companies, and governments around the world must contend with due to digital globalization. In the *Microsoft* case, the United States and Ireland have good relations, generally;[259] even so, the case has provoked controversy, and the practical considerations of concern to both governments as well as to the parties must be given more weight. While a government must have legitimate access to stored digital communications, giving it unfettered access to data stored in other countries—which the District Court effectively did—does not provide adequate consideration to the wide-ranging economic,

---

Cir. Mar. 9, 2015).

257 *In re* Microsoft, 15 F.Supp.3d at 470.

258 BAIDU, http://www.baidu.com/ (last visited Sep. 13, 2015).

259 *U.S. Relations with Ireland*, U.S. DEP'T OF STATE, (Apr. 3, 2014), http://www.state.gov/r/pa/ei/bgn/3180.htm ("U.S. relations with Ireland have long been based on common ancestral ties and shared values, and emigration has been a foundation of the U.S.-Irish relationship.").

political, and social impacts that this approach will have on the Internet.

The practical effects of how the "district court's ruling will encourage foreign governments to sidestep their own MLAT commitments and unilaterally seek data stored in the United States from providers that operate in their jurisdiction"[260] is perhaps Microsoft's strongest policy point. There is, conceivably, a slippery slope in which the world's superpower, the United States, in bypassing international law concerning cyberspace, would precipitate digital lawlessness by encouraging other countries to disregard international norms in favor of each country's narrow interests, however defined.[261]

On the other hand, it is unlikely that anything the United States does will motivate nations such as China and Russia to change their laws promoting data nationalism and more government control over user data. These nations, which are fairly characterized as somewhere between rivals and adversaries of the United States in the geopolitical sense, and are adversely disposed to the ideas of democratic and human rights, will not change their attitude towards the availability of "their" data to the United States based on the scope of hybrid warrants/subpoenas under the SCA. Furthermore, the persuasiveness of Microsoft's argument is attenuated by the fact that "during the prior three years that the Dublin datacenter was in operation,[262] Microsoft never raised this objection as a basis to avoid compliance with the SCA."[263] This interesting fact raises the probability that Microsoft's about-face objection to the SCA is motivated less by a sudden discovery of legal rights or high principal than by the economic ramifications caused by National Security Agency contractor Edward Snowden's leaks—with business losses estimated to being between $35 billion and $180 billion, depending on the metrics.[264] As the government noted,

---

[260] Brief for the United States of America at 59, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 8, 2014).

[261] Brief of Media Orgs. as Amici Curiae Supporting Appellant at 28, Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

> At oral argument, Microsoft pointed out to the court that just that week, Chinese authorities raided four Microsoft locations. The authorities took servers from Microsoft's offices and "demanded a password to seek e-mail information in the United States … Microsoft refused because the Chinese government did not have jurisdiction over e-mails located outside China.

Id.

[262] Indeed, Microsoft's Dublin datacenter has been operational since September 2010. *See* Brief for the United States of America at 45, Microsoft Corp., No. 14-2985-cv (2d Cir. Mar. 9, 2015).

[263] *Id.* at 3-4.

[264] Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0 ("[The] cloud computing industry could lose $35 billion by 2016…Forrester Research, a technology research firm, said the losses could be as high as $180 billion, or 25 percent of industry revenue, based on the size

"the protection of the foreign economic interests of the United States must be left to the appropriate departments of our government."[265]

Either way, Internet companies are in a difficult bind, and the future of the Internet is sliding towards a bordered reality. What is needed is an international consensus on how matters described in the case and scenarios may be resolved in a reasonable manner that protects data privacy while not becoming ensnared in the more complex debate over government surveillance. Coupled with efficacious use of encryption, the proposed new framework set out above should be governed by a comprehensive data service agreement that creates narrowly tailored exceptions that both facilitate legitimate law enforcement needs, while balancing the peoples' reasonable expectations of privacy over communications in cyberspace.[266]

---

of the cloud computing, web hosting and outsourcing markets and the worst case for damages.").

[265] Brief for the United States of America at 56, Microsoft Corp., No. 14-2985-cv (2d Cir. Mar. 9, 2015).

[266] DANIEL CASTRO & ALAN MCQUINN, THE INFO. TECH. & INNOVATION FOUND., CROSS-BORDER DATA FLOWS ENABLE GROWTH IN ALL INDUSTRIES (2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.