UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 16
Issue 5 *Online Issue*

Article 6

4-1-2015

Railing Against Cyber Imperialism: Discussing the Issues Surrounding the Pending Appeal of United States v. Microsoft Corp.

Jason Green

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
16 N.C. J.L. & TECH. ON. 172 (2015)

RAILING AGAINST CYBER IMPERIALISM: DISCUSSING THE ISSUES SURROUNDING THE PENDING APPEAL OF *UNITED STATES V. MICROSOFT CORP.*

Jason Young Green*

The United States government was granted a wide berth of surveillance powers post 9/11. At a time when Americans felt vulnerable to foreign attack, the executive branch passed the USA PATRIOT Act that balanced a reduction of privacy rights with a promise of increased national security. Twelve years later, Edward Snowden released documents showing exactly how pervasive U.S. intelligence gathering had become. Now, in a post-Snowden world, Americans are struggling to balance privacy rights with national security and effective law enforcement. The recent appeal of the Microsoft Corporation, which involves a warrant for the extraterritorial information of a foreign subject, highlights this struggle and brings it into the spotlight. This Recent Development argues that such extraterritorial warrants are beyond the powers of the executive branch, and need to be tempered by judicial, if not congressional, review. Further, the United States bypassing established treaties and the privacy laws of those nations in order to obtain this information could be seen as aggression against foreign nations. This Article further explores and recommends legal reforms that better accommodate the international nature of the internet and the laws of sovereign nations.

I. INTRODUCTION

The privacy debate is reaching critical mass in the United States as foreign and domestic policy makers attempt to make sense of a post-Snowden world. In the summer of 2013, Edward

* J.D. Candidate 2016, University of North Carolina School of Law. CIPP/US. I would like to thank the outstanding staff of JOLT who have helped me develop this paper.

Snowden, a former National Security Agency ("NSA") systems administrator, shocked the world with the revelation that Big Brother[1] really was watching.[2] The documents he released revealed that the United States government was not only spying on foreigners, but also on its own citizens.[3] In the fervor that followed the terrorist attacks of September 11, 2001 the government granted sweeping powers to its intelligence agencies in its War on Terror. When Snowden blew the whistle on the breadth of the NSA's spying—such as bullying tech giants Verizon, Sprint, and Google into handing over customer information—it became clear that the government had overstepped its bounds.[4] Since the first Snowden release, the media has been inundated with stories of privacy breaches and hacks.

Tech firms are now fighting back. In what should prove to be a landmark decision for international and privacy law, the United States Court of Appeals for the Second Circuit is currently weighing whether information stored by a United States company on foreign servers can bypass international laws and treaties and be recovered under a search and seizure warrant.[5] In December 2013, a U.S. magistrate judge issued a search warrant on the Microsoft Corporation ("Microsoft"), demanding access to emails stored on a server in Dublin, Ireland.[6] The United States District Court for the

---

[1] "Big Brother" alludes to George Orwell's dystopian novel 1984. The novel is set in world of perpetual war, omnipresent government surveillance, and public manipulation. *See generally* GEORGE ORWELL, 1984 (Signet Classic 1950).

[2] Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html.

[3] *Id.*

[4] *See* Evan Perez, *Telecom Firm Pushed Back on NSA Data Collection, Papers Show*, CNN (May 15, 2014), http://www.cnn.com/2014/05/14/us/nsa-phone-data-telecoms/; *see also* Shane Harris, *Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State,* SALON (Nov. 16, 2014), http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/.

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

[6] *Id.*

Southern District of New York agreed with the magistrate judge's grounds to issue the warrant.[7] However, Microsoft was allowed to appeal to the Second Circuit.[8] Now the world waits for a decision that will change the way nations regard the United States and its privacy policies, as this is the first case in which an international corporation has challenged a United States search warrant seeking data held abroad.[9]

The ramifications of this decision will be of a global scale, with far-reaching implications for the privacy rights of the citizens of every nation as well as the American companies that collect their private data.[10] Major international technology companies eagerly anticipate the Second Circuit's decision.[11] Regardless of whether

---

[7] *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, 2014 WL 4629624 (S.D.N.Y. Aug 29, 2014).

[8] Brief for Appellant at 2, Microsoft v. United States, No. 14-2985-cv (2nd Cir. 2014).

[9] Joseph Ax, *U.S. Judge Orders Microsoft to Submit Customer's Emails from Abroad*, REUTERS (July 31, 2014, 4:25PM EDT), http://www.reuters.com/article/2014/07/31/usa-tech-warrants-idUSL2N0Q61WN20140731.

[10] *See generally* Katrina vanden Heuvel & Stephen F. Cohen, *Edward Snowden: A 'Nation' Interview*, THE NATION (Oct. 28, 2014), http://www.thenation.com/article/186129/snowden-exile-exclusive-interview (during the interview, Snowden discusses the actions countries are already taking, such as Russia's new privacy regime, and how a ruling in the government's favor in the present case would encourage other countries to seek similar data localization laws. These efforts will be explained further in Part II and III); *see also* Kate Westmoreland, *Whose Laws Control your Data? The Implications of the Microsoft Search Warrant Challenge*, STANFORD L. SCH. CTR. FOR INTERNET & SOC'Y BLOG (June 23, 2014), http://cyberlaw.stanford.edu/blog/2014/06/whose-laws-control-your-data-implications-microsoft-search-warrant-challenge.

[11] The overwhelming support Microsoft has received from its peers and competitors is telling. *See* Brad Smith, *Business, Media and Civil Society Speak Up in Key Privacy Case,* THE OFFICIAL MICROSOFT BLOG (Dec. 15, 2014), http://blogs.microsoft.com/blog/2014/12/15/business-media-civil-society-speak-key-privacy-case/ (discussing the ten amici briefs submitted by: twenty-eight Tech and Media companies, thirty-five leading computer scientists, and twenty-three trade associations and advocacy groups on Microsoft's behalf). The companies represented include Verizon, Apple, Amazon, Cisco, Salesforce, HP, eBay, Infor, AT&T, and Rackspace. *Id*. They also include business organizations such as the U.S. Chamber of Commerce and the National

the decision survives the appeals process, the most important aspect of this case is what it reveals about the interaction between United States privacy laws, international treaties, and the Electronic Communications Protection Act of 1986 ("ECPA").[12] This decision should inspire the judiciary to rein in overbroad executive power and prompt Congress to legislate this matter properly.[13]

If the United States gets a favorable verdict, the judiciary will be approving the executive branch's continued expansion of power; if Microsoft wins, the judiciary will be exercising its hallmark right of judicial review, and reinforcing the checks and balances that are built into the United States Constitution.

This Recent Development argues for congressional and judicial oversight with respect to prevailing U.S. executive branch attitudes towards foreign and domestic privacy affairs. Specifically, the Executive has bypassed the review process by the loose use of warrants issued under the ECPA and the violation of fundamental privacy principles that both the United States and European Union ("EU") adhere to in their unique approaches to privacy policy. Part II begins with a survey of the development of EU and U.S. privacy policy, both before Snowden's revelations and after. Part III will use that backdrop to frame the privacy issues the Second Circuit faces in *United States v. Microsoft Corp.* Part IV analyzes the

---

Association of Manufacturers; civil liberties organizations such as the Center for Democracy & Technology, the American Civil Liberties Union, the Electronic Frontier Foundation, the Brennan Center for Justice at New York University School of Law, and the Berkman Center for Internet & Society at Harvard; major media companies such as CNN, ABC, Fox News, Forbes, the Guardian, Gannett, McClatchy, the Washington Post, the New York Daily News, and the Seattle Times. *Id.* For a complete list, visit http://mscorp.blob.core.windows.net/mscorpmedia/2014/12/Amicus-Briefing-Filers_Supporters2.pdf.

[12] 18 U.S.C. § 2510 et. seq.

[13] Orin Kerr, a computer crime law professor at the George Washington School of Law, discusses his suggestions for Congress in a Volokh Conspiracy blog post. *See generally* Orin Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?* VOLOKH CONSPIRACY (July 7, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/.

ramifications of a decision for each party with discussion of international response.

II. WHAT A DIFFERENCE A FEW YEARS MAKES: THE 2012–2014 LANDSCAPE OF EU AND U.S. PRIVACY LAWS

Before delving into the intricacies of the *Microsoft*[14] case, it is important to understand the state of privacy relations between the United States and the EU before and after Snowden began leaking classified NSA documents. First, this section examines EU and U.S. privacy policies that were in place in 2012, the year before Snowden began his progressive leak. Second, it will briefly discuss what Snowden did in 2013. Lastly, this section reviews the changes to EU and U.S. policy post-Snowden. This overview of privacy policy provides the background necessary to discuss the consequences that the Second Circuit must confront in the *Microsoft* decision.

A. *2012: EU/U.S. Privacy Pre-Snowden*

Privacy law and the belief that there is a fundamental right to privacy is a legal idea that has been percolating for little more than a century, with most discussions starting with the 1890 Warren and Brandeis piece *The Right to Privacy* published in the Harvard Law Review.[15] Advocating for the "right to be let alone" in the context of invasive high society articles in the newspapers, the two authors started a national and international discussion of whether there is a fundamental right to privacy.[16]

Fast forwarding to 1980, the Organization for Economic Co-operation and Development ("OECD") issued its privacy guidelines based primarily on the Fair Information Practice Principles ("FIPPs"), which are focused on empowering people to control their personal information and safeguards to ensure

[14] Brief for Appellant, *supra* note 8.
[15] 4 HARV. L. REV. 193 (1890).
[16] *Id.* at 195.

adequate data security.[17] The five FIPPs are: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement.[18] The OECD report became the basis for modern U.S. and EU privacy law; interestingly, both entities took diverging views implementing the FIPPs.[19]

In the United States, where privacy concerns are counterbalanced by First Amendment rights of free expression, a "sectoral" approach to privacy developed.[20] The sectoral model does not have one overarching privacy law, but rather it regulates citizen privacy with sector-specific[21] laws. Some of these sector-specific laws include the Gramm-Leach-Bliley Act ("GLBA"),[22] which protects

---

[17] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm, (last visited Feb. 27, 2015).

[18] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS, 1, 7–11 (June 1998), *available at* http://www.ftc.gov/sites/default/files/documents/ reports/privacy-online-report-congress/priv-23a.pdf. The five basic FIPPS were defined as: (1) notice and awareness: "[c]onsumers should be given notice of an organization's information practices before any personal information is collected from them;" (2) choice and consent: consumers should have options to control how their data is used; (3) access and participation: ". . . an individual's ability both to access data about him or herself . . . and to contest that data's accuracy and completeness," (4) integrity and security: organizations that collect data should ensure that the collected data is accurate and secure; and (5) enforcement and redress: enforcement measures, such as regulatory oversight with civil and/or criminal penalties for noncompliance, should be implemented to ensure that organizations follow the FIPPs. *Id.*

[19] Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: The EU and U.S. Visions of a New Privacy Framework*, 26 ANTITRUST 8, 9–10 (summer 2012).

[20] Natasha Singer, *Data Privacy Protection Laws, an Ocean Apart*, N.Y. TIMES (Feb. 2, 2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?_r=0.

[21] The sectoral approach simply refers to certain industries being regulated (Healthcare), and certain individuals being regulated (children on the internet), while other industries or individuals are left to their own devices. See Robert Schriver, *You Cheated, You Lied: the Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2779 (2002).

[22] 15 U.S.C. § 6801 et seq.; 16 C.F.R. § 313.1 et seq.; 16 C.F.R. § 314.1 et seq.

a person's privacy interests held by financial institutions, the Health Insurance Portability and Accountability Act ("HIPAA"),[23] which protects private health information, and the Child Online Privacy Protection Act ("COPPA")[24], which protects the personal information of children under the age of thirteen. The majority of these Acts do not provide private rights of action for citizens when their private data has been breached.[25]

The prevailing feature of United States privacy law is accountability: with few statutes allowing for a private right of action, U.S. citizens depend on the Federal Trade Commission ("FTC") to prosecute privacy violations. In addition to the sector-specific laws, the FTC has created standards for how businesses may collect, use, and protect the personal information of their clients.[26] The FTC regulates privacy by taking action against businesses for "unfair or deceptive" practices.[27] Some examples of the FTC's earliest actions include those against Eli Lilly,[28] Microsoft,[29] and Gateway Learning.[30] In addition, in 2011, the FTC filed actions against tech giants Google and Facebook.[31] Both companies settled and adopted comprehensive privacy programs patterned on the FIPPs.[32] These outcomes, at the time, were seen as wins—positive signs that the privacy regime in the United States was improving; the FTC was heralded as having a

---

[23] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[24] 15 U.S.C. §§ 6501-6506.
[25] *See id.*; Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[26] Wolf & Maxwell, *supra* note 19, at 9.
[27] 15 U.S.C. 45(a).
[28] *In re* Eli Lilly & Co., 133 F.T.C. 763 (2002).
[29] *See* Microsoft Corp., FTC File No. 012-3240 (2002), https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter.
[30] *See* Gateway Learning Corp., FTC File No. 042-3047 (2004), https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter.
[31] *See* Google, Inc., FTC File No. 102-3136 (2011), https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter; Facebook, Inc., FTC File No. 092-3184 (2011), https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.
[32] *See* Google, Inc., *supra* note 31; Facebook, Inc., *supra* note 31; *see also* Wolf & Maxwell, *supra* note 19.

"major role in preventing violations of consumers' expectations of privacy in the United States."[33]

On the other side of the Atlantic, the EU enacted a comprehensive Directive that regulates every piece of personal information and establishes privacy as a fundamental human right.[34] This across-the-board privacy regime gives each EU citizen a right of action should their rights be violated. So zealously does the EU guard its citizens' privacy rights that lawsuits that would be standard in the United States end with seemingly bizarre results in Europe. For example, in Italy, three Google executives were convicted of invasion of privacy for failing to block a YouTube video of a group of students bullying a disabled classmate.[35]

Perhaps the most succinct difference between EU and U.S. privacy policy is the European Court of Justice's ("ECJ") declaration that EU citizens have a "right to be forgotten,"[36] a sentiment that would seem strange to most Americans.[37] The case was filed in 2010, when a Spanish plaintiff complained to Google Spain, Google Inc., and a Spanish newspaper that notice of the plaintiff's repossessed home on Google's Spanish search engine infringed his right to privacy.[38] The plaintiff's argument before the

---

[33] Wolf & Maxwell, *supra* note 19, at 9.

[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data, 1995 O.J. (L 281) 31 (1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[35] Kit Eaton, *Italy Convicts Google Execs on Privacy Invasion Charges, Revisits Dark Ages*, FAST CO. (Feb. 24, 2010, 12:55AM), http://www.fastcompany.com/1560995/italy-convicts-google-execs-privacy-invasion-charges-revisits-dark-ages.

[36] *See* Google Spain v. Agencia Espanola De Proteccion de Datos, *infra* note 38.

[37] California has enacted a limited form of this effective January 2015, called the Children's Right to be Forgotten Act, dealing primarily with access to information about a person prior to their 18th birthday (social media, etc). S.B. 568, 2013-14 Sess., (Ca. 2013).

[38] Case C-131/12, Google Spain v. Agencia Espanola De Proteccion de Datos, 2013 CURIA (June 25, 2013), http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dda9fa02f973a74005a72486437479f81b.e34KaxiLc3qMb40Rch0SaxuPb3n0?text=&docid=138782&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=416611. In its decision, the ECJ held that

ECJ was that he, as a realtor, had the right to have the information removed because the incident had been fully addressed years before, and the information posted harmed his business.[39] The ECJ granted the plaintiff's request that the newspaper be required to remove or alter the pages in question and that Google Spain or Google Inc. be required to remove the information from the internet.[40]

Furthermore, the EU so vigorously protects the privacy of its citizens that before any data containing personal information about an EU citizen is sent overseas, the receiving country's privacy policies must be reviewed and approved by the EU Commission.[41] The EU has deemed U.S. privacy policies as being inadequate.[42] As such, companies in the United States that wish to receive and process data about European customers must implement and adhere to strict rules that follow EU privacy guidelines.[43]

---

an Internet search engine operator is responsible for the processing that it carries out of personal information that appears on web pages published by third parties. The outcome of the ruling is that an Internet search engine must consider requests from individuals to remove links to freely accessible web pages resulting from a search on their name. Grounds for removal include cases where the search result(s) appear to be inadequate, irrelevant, or excessive in the light of the time that had elapsed. If the search engine rejects the request, the individual may ask relevant authorities to consider the case. Under certain conditions, the search engine may be ordered to remove the links from search results.

[39] *Id.*

[40] *Id.*

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data, 1995 O.J. (L 281) 31 (1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; Frequently Asked Questions Related to Transfers of Personal Data from the EU?EEA to Third Countries, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[42] *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, http://export.gov/safeharbor/ (last updated Feb. 19, 2015, 11:47 AM).

[43] Binding Corporate Rules ("BCRs"), utilization of Model Contracts set forth by the EU, or participation in the EU-US Safe Harbor program are currently the

Despite this U.S. sectoral approach versus the EU's comprehensive approach to privacy, efforts were underway in 2012 to harmonize existing laws and to set a global standard for protection. United States officials even conjectured that the divergent approaches were at least equal, with the "sum of the parts of U.S. privacy protection [being] equal to or greater than the single whole of Europe."[44] In 2012, President Obama submitted a proposed Consumer Bill of Rights, which would move U.S. privacy policies more in line with those of the EU.[45] It appeared that a golden age of global privacy was being ushered in.

B. *2013: The Snowden Event*

Before June 5, 2013, the world did not know the name Edward Snowden. On June 5, he released the first wave of documents he had obtained while working as a high-ranking systems administrator for the NSA.[46] Overnight, he became famous: the world obsessed over the revelation that the U.S. government had ordered telecommunications giant Verizon to hand over data under the USA PATRIOT Act.[47] On the following day, more classified documents that Snowden had collected were released, unveiling the NSA's PRISM program whereby the government had access to voicemails, emails, texts, photos, videos, and files from the biggest tech firms in the United States.[48]

---

only ways in which U.S. companies are allowed to handle the personal data of EU citizens.

[44] *See* Singer, *supra* note 20 (quoting Cameron Kerry, General Counsel for the U.S. Department of Commerce).

[45] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[46] Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[47] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[48] *Id.*

As the months rolled by, Snowden slowly released more documents revealing the breadth of U.S. surveillance, both domestically and abroad.[49] The world reeled with the revelation that the NSA operated with a "collect it all" mentality.[50] The method was developed in 2005 by the then newly appointed NSA director, General Keith B. Alexander, as a means to mitigate U.S. troop loss from improvised explosive devices ("IEDs").[51] The plan, Real Time Regional Gateway, which collected every Iraqi text message, phone call, and e-mail, played a role in breaking up Iraqi insurgent networks and significantly reduced the IED death toll by late 2008.[52] Alexander's driving goal, spurred by the lack of intelligence that preceded the September 11, 2001, terrorist attacks,

---

[49] *See* Nicole Perlroth, et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0; *see also* Barton Gellman & Ashkan Soltani, *NSA Collections Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html; James Ball, et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN (Sept. 6, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[50] Glenn Greenwald, *The Crux of the NSA Story in One Phrase: Collect it All*, THE GUARDIAN (July 15, 2013), http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all; Ellen Nakashima & Joby Warrick, *For NSA Cheif, Terrorist Threat Drives Passion to 'Collect it All,'* WASH. POST (July 14, 2013), http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html. ("[N]ew details of the spy agency's vast reach were brought to light last month by former NSA contractor Edward Snowden, . . . who leaked classified information on government programs that sweep up 'metadata' on phone calls and e-mails by Americans. Those revelations in turn have spotlighted the role played by Alexander, the NSA's avuncular leader and, by all accounts, a driving force behind a post-Sept. 11, 2001, quest to transform an agency inundated by the data revolution into one that can exploit it to defend the nation.").

[51] Nakashima & Warrick, *supra* note 50.

[52] *Id.*

was to transform the NSA from "an agency inundated by the data revolution into one that can exploit it to defend the nation."[53]

Privacy rights of the individual are constantly at war with effective law enforcement principles. Alexander, as head of the NSA, was entrusted with the duty to protect the United States from terrorist threats both at home and abroad. The steps that he took to analyze and act on data that he collected that led to the reduction of U.S. soldier deaths are noteworthy.[54] However, the government did not fail in its mission to "collect it all" in its execution, but in its oversight.[55] Gen. Alexander frequently points out that the NSA collection programs are subject to oversight by Congress as well as the U.S. Foreign Intelligence Surveillance Court.[56] However, the proceedings of these two bodies are secret.[57] This lack of transparent oversight has given the NSA a wide berth in its operations, in violation of the FIPPS that both EU and U.S. privacy frameworks are based on, specifically the fundamentals of Notice and Consent.[58] By having secret FISA court orders and ECPA warrants that are rarely, if ever, unsealed, citizens targeted by NSA are never notified of the invasion of their privacy, and thus have no control over it.[59] It is this lack of oversight that has allowed the NSA collection mechanism to run rampant and is precisely what must be addressed.

---

[53] *Id.*

[54] *Id.*

[55] Charlie Savage & Laura Poitras, *How a Court Secretly Evolved, Extending U.S. Spies' Reach*, N. Y. TIMES (Mar. 11, 2014), http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extended-spies-reach.html.

[56] Nakashima & Warrick, *supra* note 50.

[57] ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CENTER FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 3 (2015), *available at* https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

[58] Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming the ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 601, 615 (2012).

[59] *Id.*

C. *2014 and Beyond: EU/US Privacy Post-Snowden*

The White House has moved slowly in reforming the NSA and U.S. spy policies, reportedly maintaining that the system was legal, but needs to be changed in order to "reassure a skeptical public."[60] Proposals have been met with resistance, however, as the makeup of Congress has shifted to become Republican-dominated and political pressure from outside threats, such as the Paris terrorist attacks, keep the world on edge.[61] U.S. tech companies have lost significant business and are concerned the impact of the Snowden revelations will continue to hurt their bottom lines.[62] Foreign governments are instituting new policies that seek alternatives to American technology for fear of NSA spying. In March 2014, the European Parliament passed the Data Protection Regulation and Directive, imposing strict limits on the handling of EU citizens' data.[63] This law requires that anyone handling the data of European

---

[60] Tom Cohen, et al, *Obama, Congress Working on Changes to NSA*, CNN (Mar. 25, 2014, 4:32 PM), http://www.cnn.com/2014/03/25/politics/white-house-nsa/; *see also* Julian Hattem, *NSA Reform Facing Hard Sell Following Paris Terror Attacks*, THE HILL (Jan. 11, 2015, 6:00 AM), http://thehill.com/policy/technology/229096-nsa-reform-faces-hard-sell-after-paris-attack. (Noting that reforms proposed by President Obama in January of 2014, which called for the end of the NSA's mass collection of metadata, failed in the Senate by two votes).

[61] Ellen Nakashima & Ed O'Keefe, *Senate Fails to Advance Legislation on NSA Reform*, WASH. POST (Nov. 18, 2014) http://www.washingtonpost.com/world/national-security/senate-fails-to-advance-legislation-on-nsa-reform/2014/11/18/a72eb7fc-6f70-11e4-8808-afaa1e3a33ef_story.html; Hattem *supra* note 60 ("'That metadata doesn't look all that scary this morning,' former NSA head Michael Hayden said on MSNBC after Wednesday's shooting [in Paris], the worst act of Terror France has seen in generations.").

[62] Laura Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, BUS. L. REV. (forthcoming) (citing Michael Hickens, *Spying Fears Abroad Hurt U.S. Tech Firms*, WALL ST. J. (Feb. 3, 2014), http://www.wsj.com/articles/SB10001424052702303743604579350611848246016) ("The Information Technology and Innovation Fund estimates that data privacy rules could retard the growth of the technology industry by up to four percent, impacting U.S. companies' ability to expand and forcing them out of existing markets.").

[63] *Id.* European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation

citizens "must obtain the consent of the data subjects to having their personal information processed," and further requires that the citizens retain a right to later withdraw this consent.[64] Too, the Civil Liberties, Justice, and Home Affairs Committee of the European Parliament recently passed a resolution that calls for the end of the U.S./EU Safe Harbor program.[65]

Other nations around the world are also altering how they treat cloud data and how they interact with the United States. Russia passed a law that requires foreign Internet companies to store Russian users' personal data within Russian borders to prevent tampering by the United States.[66] Brazil passed a new law that prohibits the disclosure, absent a Brazilian court order, of communications stored, collected, or processed in Brazil or for communications in which one party is in Brazil.[67] The Chinese are even ripping American technology out of their systems for fear of NSA spying or circumstances similar to the present issue in Ireland.[68]

The Snowden revelations made privacy an international concern. From its humble beginnings in the Warren and Brandeis piece in 1890 to today's constant stream of corporate and government intrusion, the feeling that there is some fundamental right to be protected has grown exponentially. The cause of this

---

(Com(2012)0011 — C7-0025/2012 — 2012/0011(COD)), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

[64] Donohue, *supra* note 62.

[65] *Id.*

[66] Paul Sonne & Olga Razumovskaya, *Russia Steps Up New Law to Control Foreign Internet Companies*, WALL ST. J. (Sept. 24, 2014), http://www.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

[67] *See* Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), Law No. 12.965 (Apr. 23, 2014) (Braz.). Unofficial English translation, *available at* https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf.

[68] *China is Planning to Purge Foreign Technology and Replace With Homegrown Suppliers*, BLOOMBERG NEWS (Dec. 18, 2014), https://www.bloomberg.com/news/2014-12-17/china-said-to-plan-sweeping-shift-from-foreign-technology-to-own.html.

exponential-explosion is the pervasive nature of the modern Internet. The Warren and Brandeis "right to be let alone" at social events has evolved into the European Court of Justice's declaration that E.U. citizens have a "right to be forgotten" by search engines. This radical leap has been greatly influenced by the advent of the Internet. The Internet is pervasive in today's business and society, and the implications of data farms and cloud computing complicate privacy regimes that differ from state to state, and nation to nation.

III. *UNITED STATES V. MICROSOFT, CORP.* IN THE POST-SNOWDEN WORLD

On December 4, 2013, a magistrate in the Southern District of New York issued a warrant that directed Microsoft to produce content and non-content information about a user whose account is associated with its Dublin, Ireland datacenter.[69] Microsoft's wholly-owned subsidiary, Microsoft Ireland Operations, Ltd., leases and operates the datacenter.[70] Microsoft began storing email data there in September 2010.[71] Microsoft stores users' email information at datacenters around the world and assigns users to different datacenters according to proximity in order to increase communications quality and decrease network latency.[72] When a user signs up for email service, he or she is prompted to enter a country code that Microsoft uses to decide where to locate the user's data.[73] Microsoft maintains non-content metadata associated with the account in the US.

The warrant was issued under Rule 41 of the Federal Rules of Criminal Procedure.[74] Rule 41 is silent as to whether it has

[69] Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant, Exhibit A, In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 13 Mag 2814 (S.D.N.Y. 2014), *available at* http://digitalconstitution.com/wp-content/uploads/2014/11/government-warrant.pdf.

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

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *See* Fed. R. Crim. P. 41.

extraterritorial effect.[75] Microsoft produced the non-content data stored in the United States but objected to producing the content information stored in the Ireland datacenter.[76] On December 18, 2013, Microsoft moved to vacate the warrant for that content.[77] The magistrate judge rejected Microsoft's motion to vacate.[78]

On July 31, 2014, the Southern District of New York upheld the magistrate judge on appeal.[79] It upheld the extraterritorial execution of the warrant and held Microsoft in contempt for refusing to comply.[80] The Southern District of New York ruled that when Congress used the term "warrant," it actually meant a "hybrid" subpoena, indistinguishable from the type that can compel a bank to produce its own transaction records from a foreign branch.[81] It concluded that, so long as no federal agents go on Irish soil, no impermissible extraterritorial action occurs.[82]

Microsoft argues that the courts presume that federal statutes do not apply extraterritorially unless Congress expresses a clear intent for them to do so.[83] It also contends that Congress did not indicate in the ECPA that Congress intended to authorize federal and local police to commandeer service providers to execute searches and seizures of private emails located in foreign countries.[84] In addition, Microsoft's brief argues that Congress did not express any intention to permit the U.S. government to ignore

---

[75] *Id.*

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

[77] *Id.*

[78] *Id.*

[79] *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, 2014 WL 4629624, at *1 (S.D.N.Y. Aug 29, 2014).

[80] *Id*.

[81] *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d at 472 (S.D.N.Y 2014).

[82] *Id. In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, 2014 WL 4629624, at *1 (S.D.N.Y. Aug 29, 2014).

[83] Brief for Appellant, *supra* note 8.

[84] *Id.*

established avenues for international cooperation, such as Mutual Legal Assistance Treaties, to obtain such evidence.[85] The question on appeal, Microsoft states, is whether US law enforcement may nevertheless invoke ECPA to conscript providers to search and seize private emails in a foreign country.[86]

The U.S. government filed its response on March 9, 2015.[87] It continues to applaud Magistrate Judge Francis' conclusion that nothing in the text, structure, or legislative history of the SCA indicated that "Congress intended to limit the ability of law enforcement agents to obtain account information from domestic service providers who happen to store that information overseas."[88] The U.S. government's chief argument echoes that of Judge Francis, stating that the "purpose of the SCA demonstrates that the imposition of a warrant requirement has nothing to do with the physical location of the relevant records."[89]

Thus a central issue in the Second Circuit's deliberation of *Microsoft* is that of location: the U.S. government wants to obtain, through Microsoft, a subject's personal information that is located in the EU member country of Ireland.[90] In its appeal to the Second Circuit, Microsoft argues, along with numerous amici, that the U.S. government has placed the company between the proverbial rock and a hard place.[91] Their options are either to respect Irish laws and

---

[85] *Id.*

[86] *Id.*

[87] Brief for Appellee, Microsoft v. United States, No. 14-29850cv (2nd Cir. 2014).

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

[89] Brief for Appellee, *supra* note 88 at 30; *see also In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d at 471.

[90] Brief for Appellant, *supra* note 8 at 2.

[91] *See id.* at 2–4; Brief for Verizon Comm. Inc. et al. as Amici Curiae Supporting Appellants at 1–3, Microsoft v. United States, 2014 WL 7213175 2d Cir.) (2014) (No. 14-2985-cv) ("Moreover, because they operate in multiple countries, and locate at least some of their servers outside the United States, the *amici* are subject to foreign data protection and privacy laws, which at times may conflict with U. S. law. The District Court's ruling threatens to force

violate the court order (and suffer resulting sanctions from the U.S. government), or to violate both Irish laws and international treaties in order to comply with the U.S. court order.

Before discussing how a verdict in either direction will affect EU/U.S. privacy concerns, especially in the realm of U.S. tech companies, this Recent Development provides an overview of the technology involved. Microsoft stores its emails in the cloud, and alleges that the data the US seeks is physically located on a server in an Irish data center.[92] Is information stored in the cloud really located in any one specific, physical location if it can be accessed from anywhere? While the U.S. government seems to think not, the private sector overwhelmingly agrees that it is.[93]

A. *The "Cloud:" What it is Exactly, and its Implications in the Microsoft Case*

As the Center for Democracy and Technology succinctly points out, the "animating question in this case is whether a U.S. law enforcement agency can compel a U.S. provider of communications service to disclose the content of digital information the provider stores outside of the U.S."[94] The Stored Communications Act ("SCA"),[95] part of the ECPA, does not address this specific issue of cloud-based data storage. The SCA authorizes the government to seek the contents of stored communications that are more than 180 days old; using a

---

companies like the *amici* to choose between complying with a U. S. search warrant and violating foreign law, on the one hand, or complying with foreign law and disobeying a U. S. court order, on the other.").

[92] Brief for Appellant, *supra* note 8.

[93] Brief for Computer and Data Science Experts as Amici Curiae Supporting Appellant, Microsoft Corp. v. United States, No. 14-2985, (2d Cir. Dec. 15, 2014) ("while 'the cloud' has become a widely-used buzzword in recent years, many people have little idea what it is or how it works," said Philip Warrick of Klarquist Sparkman LLP).

[94] *Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?,* CENTER FOR DEMOCRACY AND TECHNOLOGY (July 30, 2014), https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/.

[95] 18 U.S.C. §§ 2701–2712.

subpoena, a warrant, or a court order issued under U.S.C. § 2703(d).[96] However, the SCA is silent on whether it is supposed to apply only domestically, or whether it applies to data stored overseas as well.[97] Thus, of central importance is determining whether the data the US government seeks is located domestically or abroad, and if abroad, whether Congress intended the SCA to apply.

Determining just where particular bits of information are stored at any one time in the cloud can be a confusing concept to grasp. The U.S. government argues that due to the nebulous nature of Microsoft's cloud, paired with Microsoft's status as a United States corporation, Microsoft has no need to consult Ireland about the emails stored in its servers there.[98] Microsoft and its amici contend that while the cloud seems nebulous, individual files are stored on specific servers in specific locations.[99]

The cloud can be a funny thing. During a 2014 Super Bowl commercial, comedian Amy Poehler campily runs through a Best Buy electronic retail store asking employees, "What's the cloud? Where is the cloud? *Are we in the cloud now*?!"[100] To help the courts comprehend exactly what the cloud is, computer and data science experts told the Second Circuit Court of Appeals in their amici briefs that storing data "in the cloud" allows users to access the data from anywhere in the world, but that the stored information still has a physical location.[101] Further, the amici contend that network administrators should physically locate the

---

[96] *Id*. § 2703.

[97] *Id*. § 2703; *see also* Kerr, *supra* note 13 (discussing what Congress needs to do to amend the SCA for use in extraterritorial situations).

[98] Brief of Government in Support of the Magistrate Judge's Decision to Uphold a Warrant at 12, In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 13-2814).

[99] Brief for Computer and Data Science Experts, *supra* note 93.

[100] *Super Bowl Extended Amy Poehler Commercial for Best Buy* (ABC television broadcast Feb. 2 2014), *available at* http://abcnews.go.com/Business/video/super-bowl-extended-commercial-amy-poehler-best-buy-18400277.

[101] Brief for Computer and Data Science Experts, *supra* note 93.

data in the cloud server close to the physical location of the user in order to enhance network speed and efficiency.[102]

Due to the nature of cloud storage, the subject of the warrant in the Microsoft case is likely an Irish citizen; or, in the least, someone who lives in or spends significant time near Dublin, Ireland, since the particular emails requested are stored there. For the U.S. government to take action against this individual, it must cooperate with the Irish government via its Mutual Legal Assistance Treaty ("MLAT").[103] However, because this is an action against a foreign individual's data stored on servers owned by a United States corporation, is the government bypassing international law by using a SCA warrant?

Irish law requires that the United States seek authorization from an Irish district court judge in order to obtain the content of emails from an electronic communications provider.[104] The U.S. government has previously recognized international privacy law and foreign relations as concerns, even if the prosecutors in this case have not.[105] The Supreme Court has held that there is a "presumption that United States law governs domestically but does not rule the world."[106] This presumption would preclude the Southern District of New York's view that the SCA silently authorizes U.S. officials to reach any information abroad that foreign companies with a U.S. presence can reach from within the

---

[102] Brief for Appellant, *supra* note 8.

[103] *See* Criminal Justice (Mutual Assistance) Act of 2008, (Act No. 7/2008) (Ir.), *available at* http://www.irishstatutebook.ie/2008/en/act/pub/0007/index.html.

[104] *See* Criminal Justice Act 2011 (Act No. 22/2011) (Ir.) § 15, *available at* http://www.irishstatutebook.ie/pdf/2011/en.act.2011.0022.pdf.

[105] *See, e.g.*, Dep't of Justice, The Electronic Frontier: The Challenge Of Unlawful Conduct Involving The Use Of The Internet, A Report Of The President's Working Group On Unlawful Conduct On The Internet (Feb. 2000), *available at* http://www.politechbot.com/docs/unlawfulconduct.html ("If law enforcement agents in the United States . . . remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? . . . [C]onsider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts.").

[106] Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 454 (2007).

United States.[107] Microsoft contends that the district court's decision has created international friction that courts are supposed to avoid by "ensur[ing] that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches."[108] Orin Kerr, professor of law at George Washington University School of Law and scholar on computer crime law and internet surveillance, also agrees that the SCA is territorial and should only apply to domestic issues.[109]

This argument that the SCA only applies domestically solidifies that this case is all about location. Is it the location of Microsoft's data servers in Dublin that matters (thus making this an international issue seemingly beyond the SCA), or is it the location of Microsoft's headquarters in the United States that matters (thus making it susceptible to SCA warrants)? The Second Circuit will have to make this particular distinction in this case, and the decision is not an easy one. If territoriality is defined by where the provider is, then the U.S. government's act is territorial, as it is obtaining data from a U.S. company operating in the United States. The location of the data makes no functional difference; Microsoft can simply obtain the data remotely via a terminal. Further, because the magistrate judge ruled that ECPA warrants are hybrids of warrants and subpoenas, it is plausible that all future ECPA warrants will resemble that of subpoenas.[110]

---

[107] *Id.*

[108] Brief for Appellant, *supra* note 8 at 19 (citing *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013)).

[109] Kerr, *supra* note 13 ("On one hand, I agree that 2703 is territorial. The SCA is a close cousin of the Wiretap Act; it is integrated into the Wiretap Act and uses several similar concepts. We know that the Wiretap Act only applies inside the territory of the U.S., so it makes sense that the SCA does as well.").

[110] This was the argument made by Magistrate Judge Francis. *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 471 (S.D.N.Y. 2014) ("It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the

On the other hand, if territoriality is defined by the location of the data, then the government's act is extraterritorial. After all, the purpose of the statute is to provide privacy protections in the cloud. If the statute only applies territorially, then it only applies to the data stored in the cloud on servers in the United States. Whether a § 2703(a) warrant is a hybrid subpoena is immaterial; it is a creature of statute and has the territoriality limits of the statute that enacted it. Thus, the other plausible holding is that the data location matters rather than the corporate location. The Second Circuit must decide whether the location of Microsoft matters and confirm the district court's decision, or side with Microsoft and reverse the decision based on the fact that the data is stored in Dublin.

B. *Implications of a Ruling in Favor of the United States*

Either way it rules, the Second Circuit will change the law for U.S.-based cloud service providers and foreign governments. If Microsoft loses this case, the court will create precedent allowing the U.S. government to obtain data stored anywhere in the world by a U.S. company with just a search warrant. Such policy will be a major concern for cloud companies that host customer data outside of the U.S, as evidenced by the overwhelming number of amici briefs filed on behalf of Microsoft.[111]

Verizon Communications, Inc. argues in its amici brief that the decision "could cost U.S. businesses billions of dollars in lost revenue, undermine international agreements and understandings, and prompt . . . foreign affiliates of American companies to turn over the content of customer data stored in the United States."[112] Apple adds that "failure to address issues of international comity, reciprocity and to properly consider the ramifications of applying

---

information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question.").

[111] Smith, *supra* note 11.

[112] Brief of Verizon Comm. Inc. as Amici Curiae Supporting Appellants at 6, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 13-2814).

ECPA extraterritorially, makes it difficult . . . to navigate overlapping international laws."[113]

Foreign nations would likely respond with data segregation regimes, declaring that all electronic information concerning their citizens be stored locally, within that nation's borders. This would be an astronomical cost to major U.S. corporations like Facebook, Google, and Apple, which maintain millions of international customers. The cost of building and maintaining datacenters in every sovereign nation would also set an incredibly high bar for entry into the international internet market, limiting the growth of small companies here in the United States.

NSA dissident Edward Snowden has commented on this case, echoing similar concerns. In a recent interview he stated that *Microsoft*:

> . . . matters because if we allow the United States to set the precedent that national borders don't matter when it comes to the protection of people's information, other countries are watching. They're paying attention to our examples and what is normative behavior in terms of dealing with digital information.[114]

He further warned:

> So the question becomes what does, for example, the government in the Democratic Republic of Congo or China do the next time they've got a dissident Nobel Peace Prize nominee and they want to read his e-mail, and it's in an Irish data center? They're going to say to Microsoft, "You handed this stuff over to the DOJ; you're going to hand the same thing over to us."[115]

In such a scenario, China would levy sanctions against a balking Microsoft—sanctions that would make Microsoft less competitive in the Asian market, simultaneously hurting Microsoft and the American economy.[116]

---

[113] Brief for Apple Inc. as Amici Curiae Supporting Appellants at 3, Microsoft v. United States, No. 14-2985 (2d Cir. Dec. 15, 2014), 2014 WL 7213176.
[114] Heuvel & Cohen, *supra* note 10.
[115] *Id*.
[116] *Id*.

Recall the international effect that the Snowden revelations already had on the U.S. tech industry.[117] A decision for the U.S. government would most likely exacerbate this international distrust of American technology, further hindering the U.S. tech industry—specifically those dealing with cloud technology.

C. *Implications of a Ruling in Favor of Microsoft*

A decision affirming Microsoft's position would be a win for privacy rights and encourage multinational cooperation towards establishing a new regime of privacy and internet laws. In the words of Microsoft Vice President and General Counsel Brad Smith after Ireland filed its amici curiae brief, "The Irish government's engagement underscores that an international dialogue on this issue is not only necessary but possible. We've long argued that it's best for law enforcement to move forward in a way that respects people's rights under their local laws."[118] Indeed, a Second Circuit finding for Microsoft would force the government to use the MLAT and cooperate with the Irish, not compel them.

A ruling for Microsoft would show that companies, if not the individuals, are the owners of their cloud-based information, and that to get at that information legally the U.S. government must follow the laws of the other nations involved. This would prevent reactions such as the law Russia has passed, and promote the efficient use and growth of the internet.[119] This would be a win for U.S. tech companies that are trying to restore their global reputation post-Snowden and assure customers that using a U.S. product is not the same as giving the NSA an open invitation to peruse their data.[120]

---

[117] *See supra* Part II, C.

[118] Brad Smith, *Government of Ireland, European MEP File Amicus Briefs in New York Privacy Case*, MICROSOFT (Dec. 23, 2014), http://blogs.microsoft.com/on-the-issues/2014/12/23/government-ireland-european-mep-file-amicus-briefs-new-york-privacy-case/.

[119] Sonne & Razumovskaya, *supra* note 66.

[120] Katie Benner, *Microsoft and Google in a Post-Snowden World,* BLOOMBERG VIEW (Dec. 19, 2014), http://www.bloombergview.com/articles/2014-12-19/microsoft-and-google-in-a-postsnowden-world.

If the U.S. government is worried about the speed of criminal investigation and prosecution—which is exactly what it argued before the district court and what the district court agreed with—then it needs to amend the MLAT to provide for expediency. Otherwise the Department of Justice is single-handedly determining foreign policy precedent for the United States, which is something that the State Department and Congress are supposed to negotiate. In the end, a ruling for Microsoft would put a stop to the Executive branch's exploitation of privacy rights and reaffirm the judiciary's role in the system of checks and balances.

IV. PROPOSED CHANGES TO RESTORE OVERSIGHT IN U.S. SURVEILLANCE PROGRAMS

The *Microsoft* decision should be a catalyst for change as it brings the overreaching powers of the Executive branch (in the form of the NSA) into the spotlight. The time is ripe for Congress or the judiciary to act as a check. As noted above, countries are already changing privacy and technology policies with regard to the United States. How should the United States. shape its own policies going forward: by running roughshod over established treaties with other sovereign nations, or by stepping back and reevaluating the protections and policies that should protect the privacy rights of individuals?

When you give a soldier an order, he or she follows it. In the outrage over the terrorist attacks of 9/11, the United States ordered its security agencies to seek out threats to the United States and its citizens, giving them sweeping powers in the USA PATRIOT Act. The NSA should almost be applauded for what it achieved; the "collect it all" mentality of data interception gave the NSA the drive to be able to collect the data of nearly any person, whether a U.S. citizen or foreign national. This collection machine, if it is to be used to protect the United States and its citizens, must be regulated.

A. *Suggested Revisions to Law: Promoting Congressional Oversight and Judicial Review*

The ECPA was enacted in 1986 while the Internet was in its infancy and cloud computing was still on the horizon. Congress, in enacting the Act, could not have imagined that warrants would breach international protocol. Quite simply, a procedure used to fight crime in the United States should not be capable of obtaining information about foreign citizens of sovereign nations that is stored extraterritorially. This has the potential to set precedent for other nations to adopt equivalent procedures, which would inevitably result international chaos. The ECPA should be amended with international comity in mind.

Similarly, Orin Kerr asserts that *Microsoft* all but obligates Congress to amend the SCA.[121] "The statute just wasn't drafted with this problem in mind, and Congressional action to create explicit rules for how the statute applies abroad would be very very welcome."[122] He posits that, "[i]n a perfect world . . . the statute would distinguish between people in the U.S. who use U.S. providers that just happen to store their contents on servers abroad . . . and people abroad whose providers store e-mails abroad but also have an office in the U.S."[123] The former would require the execution of a U.S. warrant, and the latter would require utilization of the MLATs.[124]

A proper reform should align the ECPA with the FIPPs, discussed above.[125] Primarily, any amendment should provide for reasonable notice and control to subjects targeted by SCA warrants. Currently, individuals targeted by electronic surveillance are kept unaware by the presence of gag orders silencing their service providers.[126] In addition, warrants are generally sealed, often indefinitely, with the result that the target is never put on notice.[127]

---

[121] Kerr, *supra* note 13.
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *See supra* Part II.A.
[126] Smith, *supra* note 58.
[127] *Id.*

An amended ECPA should allow for notice to the target of any electronic surveillance order. Such an amendment could allow for the sealing of orders for up to six months, with an extension applicable in extenuating circumstances, but disallow the current practice of indefinite sealing. Thus targets would be put on notice of their private data being collected by U.S. authorities, and have the chance to respond. This change to the law would not only effectuate transparency in the government, but also allow for judicial review. Further, government agencies are less likely to seek warrants wantonly—they would be put on a six-month clock to make actionable use of the information gathered or their efforts would be revealed to the subject. This would be a burden for law enforcement officials, but such should be the cost of policing a free society.

Coupled with the inability to permanently seal a record would be the insertion of a private right to action. Just as citizens are allowed to bring suits against authorities for abuse of power (racial profiling, etc.), the ECPA should have a provision that allows a citizen to recover damages for the violation of their privacy rights, in the form of sanctions against the government, and allowing for the recovery of attorney's fees. This too should deter U.S. authorities from frivolously collecting data about subjects without a proper cause. Coupled with the notice requirement above, this would allow for appropriate judicial review of executive action while still allowing the NSA to do its job; except this time, Big Brother would also be actively watched.

Lastly, to assuage the U.S. government's fears that the MLAT process takes too long, there should be a revision to the MLAT for expediency in certain situations. For countries that do not have MLATs with the United States, standard operating procedures and policies should be put into place that allows for higher-ranking government officials (at least higher ranking that magistrate judges) to call upon foreign state departments for aid.

B. *Policy Considerations: Privacy Policies Moving Forward*

By amending the ECPA to realign with the FIPPs, the United States would adopt an international policy of comity and

reciprocity. This is not the only type of policy that is implicated, however. As noted above, in the United States, the FTC is the strong arm of privacy law, regulating based on unfair and deceptive trade practices.[128] The FTC holds companies accountable for the terms and conditions placed within their privacy policies. Thus, technology companies are also changing their policies to keep government intrusion out and to protect their users.

Apple, Google, and Facebook have begun encrypting phones, data centers, and WhatsApp messages, respectively.[129] Currently, companies sidestep the government and avoid producing any legible documents for review by using data encryption software that is accessed by a key that only the user possesses.[130] This is good for privacy advocates and bad for people who feel that the government should have access to that sort of information under certain circumstances, especially where national security is concerned. If the Second Circuit rules for the United States, more companies are likely to adopt policies like these to bypass the system altogether.[131] Ultimately, for criminal investigation purposes, it might be in the government's best interest to root for a ruling in Microsoft's favor so that fewer tech companies adopt such policies and access could be granted in some situations. That is to say, if companies keep encrypting their data with strong algorithms—which they should—ECPA warrants will only return encrypted data.

A second policy to consider is users' terms of service agreements with tech companies. For example, Microsoft's terms of service provide an interesting nuance to the Second Circuit's

---

[128] *See supra* Part II.A.

[129] Devlin Barrett et al., *Apple and Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J. (Nov. 18, 2014, 10:30 PM), http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801.

[130] *Id.*

[131] There is also potential for a third-party privacy company to step in and encrypt data, which is a growing trend. *See, e.g.*, *About Us*, F-SECURE CORP, https://www.f-secure.com/en/web/about_global/about-us (Last visited Jan. 25, 2014) ("We offer millions of people around the globe the power to surf invisibly and store and share stuff, safe from online threats.")

deliberations. Microsoft specifies "that different jurisdictions' laws apply depending on where in the world the user is located (which presumably has some correlation with the data location)."[132] Thus, the position that Microsoft takes in the current case conforms to the business decisions that they have already made about how to operate as an international corporation.[133] Microsoft's general counsel, Brad Smith, states in a blog post, "We've long argued that it's best for law enforcement to move forward in a way that respects people's rights under their local laws."[134]

Microsoft's perspective contrasts with similar companies like Facebook, Twitter, and Google, which "specify that the laws of their headquarters' location (California) always apply."[135] This provides an advantage by "sheltering behind Californian jurisdiction [to give] the companies the ability to set their own, US-based [sic] standards for when data should be handed over. This means that they can provide services internationally, but can still refuse to hand over data to foreign governments who seek that data for nefarious purposes."[136] While this gives the Second Circuit another wrinkle to consider, companies should look closely at their own terms of service and rule of law clauses. Careful crafting of these contracts empowers companies to choose the laws that protect themselves and their users.

V. CONCLUSION

Judge Francis chose the correct quote to open his opinion in his district court ruling: "The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by

---

[132] Westmoreland, *supra* note 10; *Microsoft Services Agreement*, MICROSOFT, http://windows.microsoft.com/en-us/windows/microsoft-services-agreement (last visited Jan. 25, 2015).

[133] *Id.*

[134] Smith, supra note 118.

[135] Westmoreland, *supra* note 10.

[136] *Id.*

any current territorially based sovereign."[137] His statement succinctly clarifies the issue faced in the Microsoft case: for the first time a court is going to have to seriously deliberate where the boundaries of international jurisdiction apply concerning information on the internet. "This is something that we need to get right. The Microsoft case is a wakeup call that the current system is not doing a good job at serving either the needs of users or the needs of business."[138]

The United States government is unlikely to back down, trading its access to foreign data for economic growth and corporate competitiveness. While there are valid arguments for swiftly acting for law enforcement purposes, the judiciary should rule for Microsoft to preserve international civility and allow the U.S. tech sector to begin regaining trust across the globe. As Facebook's Director of Public Policy Sarah Wynn-Williams stated in the fall of 2014, ". . . the bottom line is, people won't use technology they don't trust."[139]

---

[137] David R. Johnson & David Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996).

[138] Westmoreland, *supra* note 10 ("What is clear is that we need to take a nuanced approach to jurisdiction; basing jurisdiction solely on the location of the data, user, or company headquarters will give uneven and often unsatisfactory results. We also need to engage with the complexity to understand where 'searches' and 'seizures' actually occur in the online context.").

[139] Gabey Goh, *Post-Snowden Revelations, Action Still a Long Way Away*, DIGITAL NEWS ASIA (Sept. 5, 2014), http://www.digitalnewsasia.com/digital-economy/post-snowden-revelations-action-still-a-long-way-away.