Florida State University Journal of Transnational Law & Policy

Volume 26 | Issue 1 Article 1

2017

Data without Borders: Resolving Extraterritorial Data Disputes

Myra F. Din

DATA WITHOUT BORDERS: RESOLVING EXTRATERRITORIAL DATA DISPUTES

MYRA F. DIN*

"Were the Court to leave the world, the world would continue without our participation. By engaging the world and the borderless challenges it presents, we can promote adherence to and the adoption of those basic constitutional and legal values for which the Court and the Constitution stand, and which we have bequeathed to others."[1]

I. INTRODUCTION

Disputes highlighting the tension between American and foreign laws are on the rise.[2] This is largely due to rapid changes

* Myra Din is currently a judicial law clerk for a federal magistrate judge in the United States District Court for the Eastern District of New York. The views expressed in this article are solely those of the author.

1. STEPHEN BREYER, THE COURT AND THE WORLD: AMERICAN LAW AND NEW GLOBAL REALITIES 246 (2015).

2. *See generally*, Geoffrey Sant, *Court-Ordered Law Breaking: U.S. Courts Increasingly Order the Violation of Foreign Law*, 81 BROOK. L. REV. 181 (2015) (demonstrating the recent exponential growth in the number of cases in which U.S. requests

in technology over recent decades that allow businesses and governments to aggregate and store massive quantities of data that can reveal personal information.[3] In the commercial context, businesses use "big data"[4] and "metadata,"[5] to increase market efficiency and lower barriers to trade.[6] In the national security context, governments rely on metadata to conduct criminal investigations and combat grave threats to society, such as those posed by terrorism and transnational crimes.[7] At the same time,

---

for banking documents located abroad have been made); *see also id.* at 196, n.107 (listing 55 recent cases in which courts had to decide whether or not to order foreign litigants to violate foreign laws to comply with U.S. discovery requests); Zhang Yan, *Courts See More Foreign Legal Disputes*, CHINADAILY (Jan. 6, 2016, 7:14 A.M.), http://europe.chinadaily.com.cn/china/2016-01/06/content_22946811.

3. For example, the Privacy and Civil Liberties Oversight Board's 2014 report on the United States Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act explains two of the U.S. Government's metadata collection programs:

> Under one program, implemented under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata (i.e., call records) in bulk. Under the other program, implemented under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person located outside the United States.

PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 1 (2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB 702 Report]. Similarly, Facebook's Data Policy, located on its website, explains the breadth of data that Facebook collects from all of its users, including: information users provide about themselves, information users provide about other users, users' social networks and connections, information about payments users make for online goods and services, information about devices, websites, and applications that users use, and information from third party websites that users use. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited June 17, 2017).

4. "Big data is a term that describes the large volume of data—both structured and unstructured—that inundates a business on a day-to-day basis." *Big Data: What it is and Why it Matters*, SAS, http://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited June 17, 2017). "Big data is being generated by everything around us at all times. Every digital process and social media exchange produces it. Systems, sensors and mobile devices transmit it. Big data is arriving from multiple sources at an alarming velocity, volume and variety." *Big Data*, IBM, https://www.ibm.com/big-data/us/en/ (last visited June 17, 2017).

5. Metadata is "[s]econdary data that organize, manage, and facilitate the use and understanding of primary data. Metadata are evaluated when conducting and responding to electronic discovery. If privileged documents or final versions of computer files may contain metadata, they might be 'scrubbed' before release." *Metadata*, BLACK'S LAW DICTIONARY (10th ed. 2014).

6. For example, Google's privacy policy outlines how Google uses the bulk data that it collects to show users more relevant search results, make services it offers even better, generate relevant ads, connect users to more people, and make sharing things with others quicker and easier. *Google Privacy & Terms*, GOOGLE, https://www.google.com/policies/privacy/?hl=en (last visited June 17, 2017).

7.

> In the Board's assessment, the Section 702 program has proven valuable in enabling the government to prevent acts of terrorism within the United States

the proliferation of data collection jeopardizes important privacy rights. [8] The danger of infringing these rights is fictionally symbolized in Franz Kafka's *The Trial*, in which the protagonist K. is arbitrarily arrested and prosecuted by a remote unidentified authority without being informed of the nature of his crime or the scope of his misconduct.[9]

While it may seem extreme to think that something as personal as one's Facebook posts or 140-character tweets could be used to arbitrarily arrest a person, to many people, the nature of broad data collection poses that risk. The risk is not attenuated. For example, Section 215 of the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) allows the National Security Agency (NSA) to collect domestic telephone non-content information in bulk. [10] Section 702 of the Foreign Intelligence Surveillance Act (FISA) facilitates the warrantless collection of telephone and Internet metadata through numerous bulk data collection programs.[11] One of these programs, PRISM, is an upstream data collection program under which Internet Service Providers (ISPs) and Phone Service Providers are required to turn over to the NSA and FBI all email addresses, phone communications, and other Internet transactions relating to targets. [12] Similarly, Executive Order 12,333 permits the U.S. Government to do "vacuum cleaner" collection of Internet metadata, cellphone location data, [13] and

---

> and abroad, and to pursue other foreign intelligence goals. The program has helped the government to learn about the membership and activities of terrorist organizations, as well as to discover previously unknown terrorist operatives and disrupt specific terrorist plots.

PCLOB 702 Report, *supra* note 3, at 103.

8. "[T]he Board discusses the fact that privacy is a human right that has been recognized in the International Covenant on Civil and Political Rights, an international treaty ratified by the U.S. Senate, and that the treatment of non-U.S. persons in U.S. surveillance programs raises important but difficult legal and policy questions." *Id.* at 9.

9. " 'And why am I under arrest?' he then asked. 'That's something we're not allowed to tell you.' " FRANZ KAFKA, THE TRIAL 6–7 (Xist Classics, 2015).

10. PCLOB 702 Report, *supra* note 3, at 6.

11. *Id.* at 16–25; Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 344–54 (2015).

12. PCLOB 702 Report, *supra* note 3, at 7–8; Daskal, *supra* note 11, at 326, 348–49.

13. This is bulk non-content phone information like cellphone location, mailing addresses, phone numbers, and IP addresses that third parties, such as telephone service providers, are constantly collecting. *See* Ryan Felton, *Court Rules Warrantless Collection of Cellphone Location Data Constitutional*, LEGAL GUARDIAN (Apr. 14, 2016), https://www.theguardian.com/us-news/2016/apr/14/court-rules-warrantless-collection-of-cellphone-location-data-constitutional.

email address books of U.S. and non-U.S. based persons, often without filtering the collected information with search terms.[14]

The duality of the digital age is that, while it has efficiently shifted many traditional physical activities to a unified cyber realm, it has ominously created a single space where Internet users leave a digital footprint of all their regular activities, communications, and thoughts.[15] While most people value how widespread data collection allows businesses to better cater to consumer needs and facilitates intelligence-gathering,[16] many believe that data collection must be constrained at the point where the inherent value of protecting privacy rights outweighs the benefits of allowing businesses and governments to encroach them.[17] The difference between where the U.S. Government and the European Union believe this point exists has unsurprisingly led to fierce courtroom battles over how to properly handle digital data, both when it does and does not cross national borders.[18]

---

14. "Vacuum cleaner" or "bulk" data collection is broad untargeted data collection that lacks identifiers of specific people, and it is unlike traditional domestic surveillance because it is conducted without individualized court orders that are based on probable cause. PCLOB 702 Report, *supra* note 3, at 113; Daskal, *supra* note 11, at 351–52 (internal citations omitted).

15. For example, many users of Google are unaware of the breadth of information that Google collects, such as user's personal information, device information, location information, cookies and technological information from other sites, and general search queries. *Google Privacy & Terms*, GOOGLE, https://www.google.com/policies/privacy/?hl=en (last visited June 17, 2017).

16. *See, e.g.*, Myra Din, *Breaching and Entering: When Data Scraping Should be a Federal Computer Hacking Crime*, 81 BROOK. L. REV. 405, 412 (2016) (describing how businesses that use data aggregators such as search engines, business advertisers, auction compilers, financial data aggregators, and financial money managers generally increase market efficiency and benefit consumers). "Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence." PCLOB 702 Report, *supra* note 3, at 2.

17. For example, the FISA court must ensure government surveillance and collection of U.S. person's metadata meets the "totality of circumstances" standard for reasonableness under the Fourth Amendment. PCLOB 702 Report, *supra* note 3, at 9, 80, 88, 91, 98–102.

> "Whether a search is reasonable," therefore, "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Making this determination requires considering the "totality of the circumstances."

Id. at 91. FISA courts must also weigh the collection of non-U.S. person's data pursuant to their privacy rights granted under the ICCPR in order to justify the scope of their surveillance. *Id.* at 98.

18. *See generally* Geoffrey Sant, *supra* note 2 (discussing the recent exponential growth in the number of cases in which requests for violations of foreign law during discovery have been made); *see also* Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627 ¶¶ 74–104; *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) [hereinafter Warrant for Microsoft Corp. Email]; *In re* All Content & Other Info. Associated

On April 8, 2014, in the case *Digital Rights Ireland*, the European Court of Justice (ECJ) struck down the Data Retention Directive, an EU legislative act that allowed telecommunications service providers to retain metadata from every EU citizen's emails, text messages, and telephone calls for up to two years, finding that it failed to meet the proportionality requirement under EU law.[19] Similarly, on October 6, 2015, in *Maximillian Schrems v. Data Protection Commissioner*, the European Court of Justice struck down safe harbor agreements between the United States and European Union, finding that the U.S. Government's ability to require third-party ISPs to turn over metadata of EU citizens to the U.S. Government without "adequate protection" violated rights protected by the EU Data Protection Directive.[20] These decisions were the result of supranational European courts balancing domestic privacy rights against global security concerns and market interests.

A similar balancing test now faces U.S. judges, who must assess when it is appropriate to apply U.S. laws—such as those that provide for domestic data collection—outside the territorial bounds of the nation. For example, in the recent case *Microsoft Corp. v. United States*, the Second Circuit decided that it is unlawful for a U.S. magistrate judge to issue a warrant, pursuant to the Stored Communications Act (SCA), a domestic statute, to attain data exclusively stored abroad.[21] In arriving at this holding, the Second Circuit reversed the District Court for the Southern District of New York, which had issued a warrant requiring Microsoft, a U.S.-based company, to provide the U.S. Government with email content from an account located on a server in Ireland.[22]

A primary issue in that case was whether compelling Microsoft to turn over digital content data located in Ireland constituted an extraterritorial application of the SCA, given that the email "seizure" would take place in Ireland.[23] While the Second

---

with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386 (S.D.N.Y. 2014) (as amended Aug. 7, 2014).

19. Joined Cases C-293/12 & C-594/12, Dig. Rights Ireland Ltd. v. Minister for Commc'ns, 2014 E.C.R. I-238.

20. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627; Opinion of Advocate General Bot, Maximillian Schrems v. Data Prot. Comm'r, Case C-362/14, EU:C:2015:627 ¶¶ 74–104, 207.

21. Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

22. Warrant for Microsoft Corp. Email, 15 F. Supp. 3d 466, 466, 467–68 (S.D.N.Y. 2014).

23. Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

Circuit ultimately decided that it did constitute an unlawful extraterritorial application of the statute,[24] Judge Lynch pointedly observed in a compelling concurrence that the decision left open numerous questions. For example, he noted the open issues regarding: how to configure extraterritoriality when dealing with more complex criminal conduct that touches multiple jurisdictions, how to analyze extraterritoriality when the target is a known American national as opposed to a foreign national, and how to comprehend the SCA's "warrant" that is required for the U.S. Government to obtain emails when the SCA neither describes it as a "search warrant" nor implies that it functions like a traditional search warrant.[25]

The *Microsoft* case foretells that these tricky issues—stemming from both the collision of U.S. and foreign laws and the difficult task of applying traditional property and evidentiary laws to the digital realm—are here to stay. Jurists agree. In his recent book *The Court and the World,* Supreme Court Associate Justice Stephen Breyer emphasizes that the Supreme Court, too, has recently faced an increased number of cases dealing with foreign law conflicts. [26] Justice Breyer predicts that U.S. courts will increasingly be required to understand and accommodate foreign laws and policies.[27] This is particularly likely as the ubiquity of the Internet continues to grow and businesses and governments continue to depend on data collection. Thus, it is imperative for U.S. courts to develop robust analytical frameworks for key legal concepts, such as digital territoriality and sovereignty, upon which these data disputes hinge.

This paper does not undertake to reconfigure the territorial boundaries of the borderless digital world, though it discusses some suggestions that scholars have made. Rather, this paper

---

24. *Id.* at 220–22.

25. The warrant described in the SCA does not allow government agents to physically enter the premises of an ISP without notice, search for a computer, and "seize" documents. Rather, an SCA warrant functions like a subpoena in that it procedurally mandates an ISP to disclose certain electronic communications. *Id.* at 226–31 (Lynch, J., concurring).

26. *See generally* BREYER, *supra* note 1 (discussing throughout the book how globalization will continue presenting courts with issues involving the application or understanding of foreign law in order to resolve various domestic disputes in commercial and criminal contexts).

27.

> [S]omething new is under way: some activities that used to be predominantly local, including family life, now increasingly involve more than one nation. And that fact has required the Court to venture into unchartered legal territories, reckoning with (and at times applying) foreign laws concerning what once were almost exclusively local matters.

Id. at 170; *see also id.* at 195 ("I can predict only that as economic globalization marches on, such cases are ever likelier to fill our docket.").

proposes that judges more willingly engage in what Justice Breyer terms "active cross-referencing" when confronted with novel territorial conflicts, particularly those inherent in cross-border data disputes.[28] Active cross-referencing requires U.S. judges to analyze various foreign laws and policies and compare them to U.S. counterparts without presuming that one set is superior to the other. The value of active cross-referencing, beyond the intrinsic benefit of providing judges with a wider perspective on global challenges, is to help judges address the nuanced territorial issues that are arising in areas of the law that are challenged by digital borderlessness. One such area that this paper highlights is criminal procedure, where the gathering of digital evidence hinges on what U.S. courts construe as sufficient voluntary contacts to the United States.

This paper proceeds as follows. Part II explains the current structure of privacy and data collection laws in the United States. Part III explains privacy and data processing laws within the European Union and highlights the key differences between the two regions. This part discusses the 2014 case of *Digital Rights Ireland*, an ECJ decision that struck down the European Union Data Retention Directive, to show the current laws on data processing and data retention in the European Union.[29] Part IV focuses on recent transatlantic data transfers. First, it discusses general issues with framing the territorial bounds of data that arise from the borderless nature of data. It then discusses data transfers in both the commercial and criminal context, highlighting the case of *Maximillian Schrems v. Data Protection Commissioner*, a 2015 ECJ decision that struck down safe harbor agreements between the United States and European Union. Next, it discusses the Second Circuit's 2016 *Microsoft Corp. v. United States* decision to show the key issues with applying U.S. data collection laws to data stored abroad.[30] Part V then discusses

---

28. *Id.* at 236;

> "And if someone with a job roughly like my own, facing a legal problem roughly like the one confronting me, interpreting a document that resembles the one I look to, has written a legal opinion about a similar matter, why not read what that judge has said? I might learn from it, whether or not I end up agreeing with it."

Id. at 240.

29. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627 ¶¶ 74–106.

30. Warrant for Microsoft Corp. Email, 15 F. Supp. 3d 466, 466 (S.D.N.Y. 2014); Quinta Jurecic, *DOJ and Apple File Briefs in EDNY Encryption Case*, LAWFARE, https://www.lawfareblog.com/doj-and-apple-file-briefs-edny-encryption-case.

aspects of the extraterritoriality analysis that the Second Circuit did not address and illustrates how cross-referencing can help courts reconfigure the concept of digital territoriality.

II. PRIVACY WITHIN BORDERS: THE UNITED STATES

At the most basic level, both the United States and the European Union value individual privacy. National and international courts interpreting the U.S. Constitution and the EU Charter of Fundamental Rights have recognized that governmental interests in security and criminal deterrence must be weighed against people's privacy rights before those rights may be infringed.[31] But the two regions structure privacy and national security laws differently, including how they delegate responsibilities within their governmental branches. Thus, they protect individual privacy to different extents. The structural and substantive differences between U.S. and EU laws create thorny issues for businesses and courts.[32] Therefore, understanding the key similarities and differences between the U.S.'s and EU's privacy and data collection regimes is necessary to see how cross-referencing can help resolve complex data disputes.

To understand how data and privacy laws operate in the United States, it is helpful to consider the structure of the U.S. Government, particularly the separation of powers between the

31. Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Wyoming v. Houghton, 526 U.S. 295, 300 (1999); *see also* United States v. Jones, 565 U.S. 400, 411–12 (2012) (weighing the government's intrusiveness in attaching of a GPS tracking device to an individual's vehicle against individuals' reasonable expectations to privacy in automobiles); Riley v. California, 134 S. Ct. 2473, 2484, 2488–89, 2495 (2014) (weighing the governmental volatile interests in an arrest situation against people's privacy interests in the vast personal data stored on modern cells phones); Joined Cases C-293/12 & C-594/12, Dig. Rights Ireland Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238 (comparing the means by which private companies handle Europeans' electronic communications metadata for law enforcement purposes against Europeans' right to data protection and privacy pursuant to the EU Charter of Fundamental Rights); Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the United States*, 28 Harv. Hum. Rts. J. 65, 67 (2015) (discussing the ECJ's holding in *Digital Rights Ireland* as a milestone decision for protecting privacy rights from arbitrary governmental interference).

32. *See, e.g.*, Opinion of Advocate General Bot, Case C-362/14, EU:C:2015:627 ¶¶ 56, 57, 68–98 (finding that despite the needs for cross-border flows of personal data between the EU and United States to expand international trade, personal data of EU citizens cannot be transferred to third parties, such as the United States, that do not afford that data adequate levels of protection).

legislative, executive, and judicial branches. The separation of powers is important because each branch of the U.S. Government has unique authority, responsibilities, and limits. While the legislature has the express power to pass legislation that may bolster or compromise individual privacy rights, it is constrained by the electoral process, bureaucratic procedures, and inviolable constitutional rights that cannot be compromised. Similarly, while the executive branch is charged with executing the laws that Congress enacts, it is the President's role to serve as Commander in Chief of the U.S. military, to prioritize national security, and to conduct foreign relations.[33] Therefore, the executive branch is only capable of enforcing and upholding privacy rights to the extent that it is Constitutionally bound and to which the executive branch believes that these privacy rights do not interfere with its concomitant duties to protect national security and maintain foreign relations.

The U.S. system of separation of powers has institutional advantages and disadvantages for protecting individual privacy rights. The division helps to ensure that privacy interests cannot easily be encroached by any one branch of the government, since each branch employs checks on the others. A disadvantage of this fragmented system is that privacy rights are not clearly delineated by one branch. Rather, they are a consortium of rights granted through the Bill of Rights, acts passed by Congress, and the common law. While courts have interpreted all these sources of law in times of varying national security needs, the pillars of privacy law derive from bedrock principles enshrined in the Fourth Amendment to the Constitution.

The Fourth Amendment to the U.S. Constitution governs privacy jurisprudence.[34] The amendment protects "the right of

---

33. *The Executive Branch*, THE WHITE HOUSE, https://www.whitehouse.gov/1600/executive-branch (last visited June 17, 2017).

34. U.S. CONST. amend. IV. The language of the Fourth Amendment can be traced to the List of The Rights of the Colonists and a List of Infringements and Violations of Rights from 1772, which Samuel Adams used in drafting the Bill of Rights. The colonists' grievances stemmed from the complaint that prior to enacting the Bill of Rights, they had no protection against the employment of "writs of assistance." Under these pre-Revolution writs, British officials were allowed to enter private homes and businesses to conduct warrantless searches for smuggled goods or other evidence of criminal activity, blatantly encroaching on colonists' sacred personal spaces. Opposition to these writs was a driving force behind the Revolution. Mike Maharrey, *Fourth Amendment: The History Behind "Unreasonable"*, TENTH AMENDMENT CTR., http://tenthamendmentcenter.com/2014/09/25/fourth-amendment-history-behind-unreasonable/ (last visited June 17, 2017); Schwartz, THE BILL OF RIGHTS: A DOCUMENTARY HISTORY 199, 205–06 (Leon Friedman et al. eds., 1971); Katz v. United States, 389 U.S. 347, 367 (1967); Riley v. California, 134 S. Ct. 2473, 2494 (2014) (describing how concerned James Otis and John Adams were with abolishing the arbitrary writs of assistance).

people to be secure against unreasonable searches and seizures in their persons, houses, papers, and effects."[35] The Supreme Court has interpreted this language to mean that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' "[36] Because the Fourth Amendment specifically protects: persons, houses, papers, and effects,[37] the Supreme Court has interpreted the enumeration of these four categories to reflect that privacy rights are closely connected to property rights.[38] Thus, interests that fall within these four categories enjoy special protection from arbitrary governmental interference. The most foundational of these property-based interests is the privacy interest attached to one's home.[39] Consequently, the home has been deemed the "citadel of individual sovereignty."[40]

Privacy scholar Professor James Whitman explains how through decisions such as *Lawrence v. Texas* and *Roe v. Wade*, the Supreme Court has expanded privacy protections to include domains such as homosexual activities and abortion decisions.[41] He explains that American privacy law is not broad and universal, but rather, the product of "piecemeal" legislation.[42] Indeed, the fragmented nature of privacy law is evident from the fact that even though the Supreme Court has stated: "the Fourth Amendment protects people, not places,"[43] courts analyze the "reasonableness" of people's expectations to privacy differently based on the location and type of search taking place.[44]

---

35. U.S. CONST. amend. IV.

36. Riley v. California, 134 S. Ct. 2473, 2482 (2014) (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).

37. U.S. CONST. amend. IV.

38. "The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to the 'right of people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous". United States v. Jones, 565 U.S. 400, 405 (2012).

39. *See* Katz v. United States, 389 U.S. 347, 361 (1967). Recently, the Supreme Court in *United States v. Jones*, stated that the 1765 English case *Entick v. Carrington* still colors traditional Fourth Amendment search and seizure analysis. United States v. Jones, 565 U.S. 400, 405 (2012). In *Entick*, Lord Camden expressed, "[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave." *Id.* (quoting Entick v. Carrington, 95 Eng. Rep. 807 (C. P. 1765)).

40. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1162 (2004).

41. *Id.* at 1214 (citing the Supreme Court's decisions in Lawrence v. Texas, 539 U.S. 558 (2003) and Roe v. Wade, 410 U.S. 113 (1973)).

42. *Id.* at 1159.

43. Katz v. United States, 389 U.S. 347, 351 (1967).

44.

> As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a

In analyzing whether a governmental search is reasonable, courts have adopted a sliding scale approach, in which a person's privacy interest is weighed against the government's need for the intrusion.[45] The home is granted the highest level of privacy protection because it carries the most reasonable expectation of privacy.[46] Areas of special national interest, such our nation's borders, are granted the lowest levels of privacy protection because people can reasonably expect less protection at the borders, and the government's interest is at its "zenith" when regulating who and what enters the nation.[47] Between these extremes lie the varying reasonable expectations to privacy in things such as people's cars, mail, luggage, physical bodies, and—critically now—their data.

As technology has advanced and been used by the government for a variety of searches, the reasonability analysis has grown increasingly complex. For example, in *Silverman v. United States*, a 1961 case that arose when microphones were new technology, the Supreme Court had to determine the extent to which law enforcement officers could listen to conversations of suspected criminals that occurred within suspects' homes from outside.[48] Rather than contemplate how the Fourth Amendment would be affected by "frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society,"[49] the Court simply reasoned that the traditional privacy interest in the home was readily apparent, and therefore officers could not listen to such conversations without a warrant.[50] As technology has

---

> twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'

Id. at 361.

45. Scott E. Sundby, *"Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757, 1762 (1994).

46. "Thus a man's home is, for most purposes, a place where he expects privacy . . . ." *Katz*, 389 U.S. at 361.

47. United States v. Flores-Montano, 541 U.S. 149, 153 (2004) ("The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.").

48. Silverman v. United States, 365 U.S. 505, 506–507 (1961).

49. *Id.*

50.

> "The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard."

Id. at 511–12 (internal citations omitted).

continued to develop since *Silverman*, courts have had to confront how new technology affects traditional Fourth Amendment analysis, particularly in searches of data.

In two recent Supreme Court cases, the Court had to identify the reasonable expectations to privacy in Global-Positioning-System (GPS) data and cell phone data. First in 2011, in *United States v. Jones*, the Supreme Court had to decide whether attaching a GPS-tracking device to an individual's vehicle, and subsequently using that device to monitor a vehicle's movements on public streets, constituted a search or seizure under the Fourth Amendment.[51] The Court recognized the trouble with considering GPS data collection a Fourth Amendment search because GPS devices enabled efficient visual observation of an automobile's location, and visual observation of an automobile is not an unconstitutional search. [52] Ultimately, similar to the Court's reasoning in *Silverman*,[53] the Supreme Court held that using a GPS device without a warrant constituted an unconstitutional search because setting up the GPS device required temporarily trespassing into the automobile where there was a classic property-based reasonable expectation to privacy.

Relatedly, in June 2014, in *Riley v. California*, the Supreme Court was tasked with deciding whether police officers must obtain a warrant before searching the cellphone data of someone they arrest.[54] The Court confronted novel issues that arise with cell phones, such as how to categorize them,[55] particularly when they function much like "minicomputers," enable users to access data stored on remote "clouds," and have broad data storage capacities that the drafters of the Constitution could never have imagined. [56] Weighing the government's need to deter crime against people's reasonable expectations to privacy in their personal and intimate data, the Supreme Court recognized that cell phones today are "a pervasive and insistent part of daily life," and the vast personal data they contain is clearly within the

51. United States v. Jones, 565 U.S. 400, 402 (2012).

52. *Id.* at 410.

53. *Id.*

54. Riley v. California, 134 S. Ct. 2473, 2480, 2484 (2014) ("These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").

55. *Id.* at 2489 ("[Cell phones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

56. *Id.* at 2485, 2489–95.

ambits of what the Founding Fathers fought to protect. [57] Therefore, the Supreme Court held that police officers must attain a warrant prior to searching suspects' cell phones.[58]

These three Supreme Court cases illustrate how even though courts typically delineate the bounds of constitutional rights, modern technology-induced challenges have led judges to find it beyond their place to identify people's reasonable expectations to privacy in devices that store vast personal data.[59] Justice Alito, while concurring with the outcome in *United States v. Jones*, stated that the "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[60] Judge Lynch, too, while concurring with the outcome in *Microsoft Corp. v. United States*, urged Congress to take action to address the many shortcomings of the SCA, which was enacted long before the modern digital terrain developed.[61]

Although these judges have prodded Congress to undertake statutory reformation, their pleas invite the question of whether the legislature is committed to understanding and responding to people's changing expectations of privacy and the nature of electronic communications in a timely manner. Recent history tends to show that it is not. Consider the Computer Fraud and Abuse Act (CFAA). This act was passed in 1984, during the nascent days of the Internet, well before computer hacking was concretely conceptualized. [62] Although over two decades have passed since the act's initial ratification, and notwithstanding several amendments to the act, the statute is still plagued with

---

57. *Id.* at 2484, 2495.

58. *Id.* at 2495.

59. *See e.g.*, United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. (citation omitted) A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–6 (2004)).

60. *Id.* at 429–30.

61. Microsoft Corp. v. United States, 829 F. 3d 197, 232 (2016) (Lynch, J. concurring) ("The SCA was adopted in 1986, at a time when the kinds of services provided by 'remote computing services' were not remotely as extensive and complex as those provided today, and when the economic and security concerns presented by such services were not remotely as important as they are now."); *Id.* at 233 (Lynch, J. concurring) ("Congress would do well to take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs.").

62. Myra F. Din, *Breaching and Entering: When Data Scraping Should be a Federal Computer Hacking Crime*, 81 BROOK. L. REV. 405, 406 (2015) ("In proscribing computer fraud and the use of counterfeit access devices in the same act, Congress likened computer hacking to the crimes of credit card fraud and identity theft.").

ambiguity in key language that has resulted in a circuit split with no consensus about how broadly Congress intended the statute to apply and what actually constitutes "hacking." [63] Similarly, consider FISA, which was first passed in 1978 in the context of the Cold War as a response to warrantless governmental surveillance. [64] FISA was originally intended to preserve Americans' fundamental privacy rights and provide the government broad latitude to gather foreign intelligence. [65] FISA was expanded by the USA PATRIOT Act weeks after 9/11 when such expansion was deemed necessary to facilitate broad data collection of foreign and domestic intelligence. [66] But, more than 15 years have since passed and Section 702 of FISA still allows the Government to engage in warrantless collection of telephone and Internet metadata of citizens within the territorial bounds of the United States despite strong public sentiment opposing mass surveillance.[67]

---

63. *See generally id.*

64. Foreign Intelligence Surveillance Act of 1978, Law of Oct. 25, 1978, ch. 36, §§1801–1811, 2511, 2518–2519, 92 Stat. 1783 (1978) (current version at 50 U.S.C §§1801–1811 (2012 & 2015)); Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (codified at 50 U.S.C §§1801–1811 (1982 & Supp. III 1985)); SUSAN N. HERMAN, TAKING LIBERTIES: THE WAR ON TERROR AND THE EROSION OF AMERICAN DEMOCRACY 5, 111 (Oxford Univ. Press 2011) (describing how FISA was spurred by the public's outrage that President Richard Nixon was using what he claimed were inherent governmental powers to spy on Americans whom he thought posed a threat to national security).

65. David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 487–88 (2006);

> [I]nformation needed to recruit an international terrorist as a double agent was foreign intelligence information because recruitment is a method of protecting against terrorism that does not involve law enforcement. However, information needed to indict and prosecute an international terrorist was not foreign intelligence information. Although prosecution clearly can protect against terrorism—by deterring, incapacitating, or encouraging cooperation from terrorists in exchange for leniency—prosecution is a law enforcement method.

Id. at 496.

66. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107–56, 115 Stat. 272 (2001) [hereinafter Patriot Act] (codified in scattered titles of U.S.C.); HERMAN, *supra* note 64, at 5; *Surveillance Under the Patriot Act*, AM. C.L. UNION, https://www.aclu.org/infographic/surveillance-under-patriot-act (last visited June 17, 2017); Harold C. Relyea, *Terrorist Attacks and National Emergencies Act Declaration*, CRS REPORT FOR CONGRESS, (Jan. 7, 2005), http://fas.org/irp/crs/RS21017.pdf.

67. 50 U.S.C. §1881a (2015); PCLOB 702 Report, *supra* note 3, at 16–25; Jennifer Daskal, *supra* note 11, at 344–54 (2015); Nicole Perloth & Katie Benner, *Subpoenas and Gag Orders Show Government Overreach, Tech Companies Argue*, N.Y. TIMES (Oct. 4, 2016), http://www.nytimes.com/2016/10/05/technology/subpoenas-and-gag-orders-show-government-overreach-tech-companies-argue.html?_r=0; Jennifer S. Granick & Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html; M.S., *Verizon's Records: Why We Fear Broad Surveillance*, ECONOMIST (June 6, 2013, 4:39 P.M.), http://www.economist.com/blogs/democracyinamerica/2013/06/verizons-records; M.G., *Now Listen Here*, ECONOMIST (June 6,

Most relevant to this paper, consider the SCA.[68] Congress passed the SCA in 1986 to regulate law enforcement's ability to access electronic data.[69] Under the SCA, before the government or a law enforcement officer may attain electronic records from a third party provider such as an ISP, the government must show specific and articulable facts that the records are relevant and material to an ongoing criminal investigation.[70] But the SCA also imposes an arbitrary 180-day distinction, such that when an officer seeks communication that is less than six months old, the officer must obtain a search warrant and satisfy the more taxing requirement of "probable cause," whereas if the officer seeks records more than six months old, she need only attain a subpoena based on showing "reasonable grounds" for believing that the contents are relevant to a criminal investigation. Judges and scholars alike have pointed out the frivolity of this distinction, which may have made sense two decades ago, but now arbitrarily demarcates between emails that are very recent and those that are more than six months old.[71]

If the legislature has not kept pace with modern technological advancements, then neither have the judiciary and the executive branch, as they are required to interpret and enforce the laws as written. Hence, it is little surprise that courts are handicapped by

---

2013, 3:53 P.M.), http://www.economist.com/blogs/democracyinamerica/2013/06/domestic-surveillance; T.C. Sottek, *Can You Hear Us Now? Broad Coalition Sues NSA Over 'Illegal' Telephone Surveillance Dragnet*, VERGE (July 16, 2013, 2:28 P.M.), http://www.theverge.com/2013/7/16/4528796/nsa-telephone-surveillance-federal-lawsuit.

68. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat.1848 (codified as amended in various sections of 18 U.S.C.) [hereinafter ECPA]; *Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/ecpa/ [hereinafter ELECTRONIC PRIVACY INFO. CENTER].

69. ECPA, *supra* note 68; ELECTRONIC PRIVACY INFO. CENTER, *supra* note 68.

70. ECPA, *supra* note 68; ELECTRONIC PRIVACY INFO. CENTER, *supra* note 68.

71. 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, 1234 (2004) ("[T]he strange '180 day rule' dividing § 2703(a) from § 2703(b) may reflect the Fourth Amendment abandonment doctrine at work. Individuals lose the Fourth Amendment protection in property if they abandon the property, and the SCA's drafters may have figured that unretrieved files not accessed after 180 days have been abandoned.");

> More than a dozen years ago, a leading commentator was expressing the need to reform the Act. (citation omitted) It would seem to make sense to revisit, among other aspects of the statute, whether various distinctions, such as those between communications stored within the last 180 days and those that have been held longer, between electronic communication services and remote computing services, or between disclosures sought with or without notice to the customer, should be given the degree of significance that the Act accords them in determining the level of privacy protection it provides, or whether other factors should play some role in that determination.

Microsoft Corp. v. United States 829 F. 3d 197, 233 (2016) (Lynch, J. concurring) (internal citation omitted).

both insufficient guidance and limited authority to tailor current laws to the modern legal dilemmas presented in contentious privacy disputes. Coupling this insufficient guidance are the complicated laws governing data collection in the European Union.

III. DATA COLLECTION IN THE EUROPEAN UNION

European privacy law takes a different form than American privacy law. Much of the perception regarding the difference between EU and U.S. privacy laws derives from the notion that EU laws are more concerned with protecting "dignity" and American privacy laws are more concerned with protecting "liberty."[72] Professor James Whitman explains that in European states like Germany, privacy derives from an ethos of safeguarding one's public image.[73] As such, in many European states, the largest "enemies" of privacy are the media and other agents that gather and disseminate information in a way that endangers public dignity.[74] On the other hand, American privacy laws largely emphasize protecting liberty, particularly from unwanted intrusions by the state.[75] This ideology can be traced to the pre-Revolution era, when common writs allowed agents of the British crown to arbitrarily invade colonists' homes and rummage for incriminating evidence.[76]

But while the United States and European Union may have ideological differences underpinning their privacy regimes, the notion that American privacy rights are vastly different from European rights on the basis of this liberty-dignity paradigm is too simplistic.[77] Certainly, the different privacy regimes have led to varied outcomes in data-related litigation.[78] Yet, both the United

---

72. *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

73. *Id. See also* Hannah Bloch-Wehba, *Confronting Totalitarianism at Home: The Roots of European Privacy Protections*, 40 BROOK. J. INT'L L. 749, 760–64 (2015) (discussing how modern European privacy law, particularly that of Germany, developed against a culture of "intrusive policing of intimate relationships and choices," in which men defended their privacy rights and their family's privacy rights to protect their honor and social image).

74. Whitman, *supra* note 72.

75. *Id.*

76. *Id.*; *see infra* note 228 and accompanying text.

77. *See* Bloch-Wehba, *supra* note 73, at 765 (discussing how the concepts of liberty and dignity are "overlapping, complex, and used by scholars in unclear ways").

78. *Compare* Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1192 (9th Cir. 2007) (holding that targeted secret warrantless wiretapping surveillance of a charity by means outside the bounds of the FISA is not unconstitutional and is protected by the state secrets doctrine) *with* Joined Cases C-293/12 & C-594/12, Dig. Rights Ir. Ltd. v. Minister for

States and the European Union engage in extensive domestic and foreign surveillance, employing both targeted and bulk data collection systems.[79] And the concerns of protecting individual privacy and enhancing national security are vital to both regions. But, because the European Charter protects a broad "fundamental right to privacy,"[80] for which there is no perfect analogue in the U.S. Constitution,[81] and because the European Union has a different legal architecture than the United States, the regions have different mechanisms and procedural safeguards for data collection and transfers. These differences have led to frequent clashes regarding how to handle sensitive data in litigation. To understand the heart of these clashes, it is useful to take a look at relevant EU statutes.

A. A Fundamental Right to Privacy

The multilevel EU structure for protecting fundamental rights derives from the laws and constitutions of the member states, the European Convention on Human Rights (ECHR), and the Treaties and legislation of the European Union.[82] At the highest level, the European Union protects a "fundamental . . . right to privacy," codified in the Charter of Fundamental Rights of the European Union.[83] Article 7, which protects private and family life, states: "Everyone has the right to respect for his or her private and family life, home and communications."[84] Article 8, which specifically protects personal data, provides:

> 1. Everyone has the right to the protection of personal data concerning him or her.

Commc'n, 2014 E.C.R. I-238 (holding that a legislative act that allowed telecommunications service providers to retain metadata from every EU citizens' emails, text messages, and telephone calls for up to two years fails to meet the proportionality requirement under EU law).

79. *See* Jon L. Mills, *The Future of Privacy in the Surveillance Age*, *in* AFTER SNOWDEN: PRIVACY, SECRECY, AND SECURITY, IN THE INFORMATION AGE 191, 210–17 (Ronald Goldfarb ed., 2015); *see supra* Introduction; *see infra* Section II.B, C and accompanying notes.

80. Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1, 10.

81. Note that the term "privacy" does not appear anywhere in the text of the U.S. Constitution.

82. Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65, 68 (2015).

83. Charter of Fundamental Rights of the European Union, *supra* note 80, arts. 7–8.

84. *Id.* art. 7.

> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[85]

Similar language is found in Article 8 of the ECHR:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondents.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[86]

In addition, Article 16 of the Treaty on the Functioning of the EU (TFEU) reiterates: "Everyone has the right to the protection of personal data concerning them."[87] EU member states are bound to all these privacy provisions and must adopt adequate laws and constitutional provisions to abide by them.

At the state level, the fundamental rights guaranteed through provisions in EU Charter, the ECHR, and the TFEU are protected by member states' individual constitutions and domestic laws. According to International Law Professor Frederico Fabbrini, Central and Eastern European states, most of which enacted their constitutions after the Cold War, are more likely to protect a fundamental right to privacy explicitly in their constitutional provisions.[88] On the other hand, in many Western and Southern European states, "where privacy and data protection are not textually enshrined in domestic basic laws, constitutional courts have consistently interpreted their domestic laws as protecting

85. *Id.* art. 8.

86. European Convention on Human Rights art. 8, Nov. 4, 1950, 213 UNTS 221.

87. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012 O.J. (C326) 55 [hereinafter TFEU].

88. Fabbrini, *supra* note 82, at 69.

these rights."[89] Because EU law recognizes a fundamental right to privacy and attempts to harmonize member states' approaches to regulating privacy, the next section will discuss the acts that promote the harmonization of privacy law in the European Union.

B. A Top Down Legislative Approach

Several acts shape the current scope of privacy rights and data protection in the European Union. The first act is the prelude to the current Data Protection Directive. In 1980, the Organization for Economic Cooperation and Development (OECD) passed an international agreement concerning data privacy that promulgated measures to assist the free flow of personal data across European borders. [90] These guidelines offered basic principles that were intended to serve as templates for nations to mirror or adopt.[91] Although these guidelines were not binding and did not establish a maximum level of protection, they encouraged member states to share information with one another regarding effective methods to protect privacy on global networks.[92]

In 1998, after nearly three years of deliberation, [93] the European Commission, the executive body that proposes and monitors legislation for the European Union, [94] passed a declaration that codified the OECD's guidelines. This declaration, the European Union Data Protection Directive (Protection Directive), establishes a framework for all EU member states to protect personal data.[95] Notably, the Data Protection Directive is not self-implementing.[96] Rather, each EU member state must pass its own implementing legislation.[97] Since the Directive's goal is to harmonize data protection across member states, it sets a minimum level of data protection with which states must comply. It also establishes high levels of protection for personal data with narrow exceptions, directs each member state to create

89. *Id.*

90. Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERK. TECH. L.J. 461, 466 (2000).

91. *Id.*

92. *Id.* at 467.

93. Symposium, *From the Market to the Polis: the EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 445 (1995).

94. *The European Commission*, EUROPA, https://ec.europa.eu/commission/index_en (last visited June 17, 2017).

95. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

96. Fromholz, *supra* note 90, at 467.

97. *Id.* at 468.

independent supervisory bodies to regulate personal data protection, and establishes a right of redress when individuals believe their rights have been infringed.[98]

In 2006, the European Commission also enacted The European Union Data Retention Directive (Retention Directive).[99] Largely a response to both 9/11 and the 2005 terrorist attacks in London, the Retention Directive required member states to ensure that their internet and telephone service providers retain metadata from electronic communications for a minimum of six months and a maximum of two years for law enforcement needs.[100] It therefore mandated that providers of publically available information in EU member states derogate from the Protection Directive.[101] Member states had to ensure: 1) the presence of competent national authorities to ensure that data accessed was in accordance with necessity and proportionality requirements,[102] 2) that none of the data retained would reveal the content of the communication,[103] 3) that data retained would be secured with sufficient technical and organizational measures to prevent accidental or unlawful destruction, alteration, storage, access, or disclosure,[104] and 4) that the data would be destroyed at the end of the retention period.[105]

On April 8, 2014, in *Digital Rights Ireland*, the European Court of Justice (ECJ) monumentally held that the Retention Directive was invalid under the EU Charter of Fundamental Rights because it mandated unjustified data retention.[106] This decision reflects the ECJ's current stance of where the balance between national security and privacy tips. Shortly after the

---

98. *Id.* at 468–69.

99. Council Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54 [hereinafter Data Retention Directive].

100.

> Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

Data Retention Directive, *supra* note 99; *Id.* arts. 11, 6.

101. *Id.* art. 1.

102. *Id.* art. 4, 9.

103. *Id.* art. 5.

104. *Id.* art. 7.

105. *Id.*

106. Joined Cases C-293/12 & C-594/12, Dig. Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238.

decision, the Court of Justice of the European Union (CJEU) issued a similar milestone decision in *Maximillian Schrems v. Data Protection Commissioner*, which struck down the safe harbor agreements between U.S. companies and EU member states.[107] The ECJ's decision in *Digital Rights Ireland* will be discussed next to demonstrate the current data collection regime within the borders of the European Union. The subsequent section will discuss both *Maximillian Schrems* and *Microsoft v. United States* in order to build upon this analysis and show how domestic data collection regimes have effects that emanate beyond national borders.

C. Judicial Protection of Privacy in the EU

In *Digital Rights Ireland*, the ECJ had to decide whether the Retention Directive legally complied with the Protection Directive, Articles 7 and 8 of the EU Charter, and Article 8 of the ECHR.[108] The case involved an Irish plaintiff who claimed that national legislative measures in Ireland, which mandated the retention of his cell phone data pursuant to the Retention Directive, were disproportionate, unnecessary, and inappropriate for achieving Ireland's aims of ensuring that certain data be available for investigating, detecting, and prosecuting serious crime. [109] In analyzing whether the Retention Directive was incompatible with Article 8 of the ECHR, the ECJ focused on several considerations. One was the overly broad scope of the Retention Directive, which retained the data of all EU persons—even those who had no connection to crime, never committed suspicious activities, or were, by profession, required to maintain certain communication secrecy—for a minimum period of six months, regardless of the purpose for which it was collected.[110] A second was the inherent concern with the collection of vast metadata, as opposed to content data, since:

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence,

---

107. Opinion of Advocate General Bot, Maximillian Schrems v. Data Prot. Comm'r, Case C-362/14, EU:C:2015:627.

108. Joined Cases C-293/12 & C-594/12, Dig. Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238, at 3, ¶¶ 17–18.

109. *Id.* ¶ 18.

110. *Id.* ¶¶ 57–58, 66.

> daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[111]

A third concern for the ECJ was the risk of subsequent abuse of the data, particularly because the data was subject to automatic processing and the possible lack of adequate safeguards to access the data.[112] Ultimately, not only did the ECJ find metadata to be more revealing than content data, but because metadata was collected on all individuals, all persons "are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out their private lives and use those data for multiple purposes."[113] Lastly, the ECJ was concerned with the deficiency of procedural safeguards required of member states—specifically, the lack of objective criteria for accessing data,[114] the lack of organizational and technical measures for protecting the data,[115] and the fact that retained data could be stored outside of the EU, where it would not be subject to the control of an independent authority as required by EU law.[116]

Importantly, the ECJ acknowledged that, as a supranational court of review, it had to afford reasonable deference to domestic courts and the regulatory decisions of its member states.[117] But despite such deference to the Irish government on matters of domestic security[118] and its repeated acknowledgement of the global need to fight international terrorism and other serious crimes for which data retention was vitally important,[119] the ECJ continually reiterated that the right to privacy and the right to respect private life is fundamentally important; therefore no infringement of that right would be valid unless it met the three requirements of legality, necessity, and proportionality.[120] Thus, the ECJ required that EU legislation implicating privacy lay down clear and precise rules regarding its scope and application and

---

111. *Id.* ¶ 27.
112. *Id.* ¶¶ 54–55.
113. *Id.* ¶ 20.
114. *Id.* ¶ 62.
115. *Id.* ¶ 67. The Court was also concerned with the fact that Internet and telephone service providers could only provide security safeguards to the extent that it was economically feasible for them to do so.
116. *Id.* ¶ 68.
117. *Id.* ¶¶ 47–48.
118. *Id.*
119. *Id.* ¶¶ 48–49, 51–52.
120. *Id.* ¶ 38.

impose minimum safeguards to ensure that persons whose data has been retained have sufficient guarantees to protect their personal data against abuse and unlawful access.[121]

As a consequence of this decision, the ECJ expanded the scope of privacy rights, particularly from governmental encroachment. As the next section demonstrates, the EU has not only protected its members' privacy rights from the risk of infringment by governmental activities within the EU, but it has also protected the fundamental right to privacy from encroachments originating outside of the EU's borders. In sheltering privacy rights from remote infringements, the EU has expanded once territorial rights beyond the EU's borders and redefined digital territoriality.

To demonstrate this, the next section first discusses some of the novel challenges posed by borderless data itself and then discusses *Maximillian Schrems* and *Microsoft v. United States*,[122] both of which show how courts are inevitably redefining digital territoriality in dealing with transatlantic data transfers. This will set the stage for discussing how cross-referencing can help courts actively reconfigure the concept of extraterritoriality in modern data disputes.

IV. CROSSING CONTINENTAL BORDERS

The labyrinth of laws governing privacy, data collection, and data transfers is already confusing when applied to activities wholly within the United States or the European Union. The difficulty of administering either region's laws is amplified in disputes involving data transfers across the Atlantic Ocean, where legal systems clash and sovereign state interests are implicated. Adding to the challenges is the amorphous nature of data itself. Therefore, before discussing some of the contentious cross-border issues that have arisen in recent legal disputes, this section discusses some of the borderless characteristics of data that challenge a legal world defined by borders.

A. The Borderlessness of Data

Professor Jennifer Daskal, in her article *The Un-territoriality of Data*, argues that data disputes present courts with novel

121. *Id.* ¶ 54.

122. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627; Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

challenges because judges struggle to conceptualize the amorphous nature of data which conflicts with fundamental principles about territoriality that underlie the Fourth Amendment.[123] Professor Daskal explains that all U.S. Constitutional rights depend on a two-part inquiry accounting for citizenship and voluntary ties to the United States. She explains that a person's entitlement to constitutional rights depends on whether one is territorially bound to the United States as a citizen or whether one has sufficient voluntary connections to the nation.[124] She also notes several ways that data inherently challenges these territorial presumptions.[125]

The three main characteristics that Professor Daskal believes challenge the territoriality of data are its mobility, interconnectedness, and divisibility.[126] Because data moves in unpredictable ways, often crossing many sovereign state borders while en route from a user to a recipient, there is an inherent disconnect between the location of a user and the location of their data.[127] Further, unlike persons and their traditional personal belongings, the movement of data is not only quick and physically disconnected from the user, but it is also largely unknown to the user since it is not visible to the naked eye.[128] Professor Daskal also explains how, because data is inherently fragmented and often used with anonymizing features, digital footprints are often unidentifiable as "belonging" to a particular person.[129] Because

---

123. Daskal, *supra* note 11, at 330–31.

124. *Id.* at 329.

125. First, the "ease, speed, and unpredictability with which data flows across borders make its location an unstable and often arbitrary determinant of the rules that apply." *Id.* Second, "the physical disconnect between the location of data and the location of its user—with the user often having no idea where his or her data is stored at any given moment—undercuts the normative significance of data's location." *Id.*

126. *Id.* at 331.

127.

> When one Google chats with a friend in Philadelphia or uses FaceTime with a spouse on a business trip in California, the data may travel through France without the parties knowing that this is the case. Similarly, when data is stored in the cloud, it does not reside in a single fixed, observable location akin to a safe-deposit box. It may be moved around for technical processing or server maintenance reasons. It could also be copied or divided up into component parts and stored in multiple places—some territorially and some extraterritorially. At any given moment, the user may have no idea—and no ability to know—where his or her data is being stored or moved, or the path by which it is transiting.

Id. at 366–67.

128.

> Similarly, when one stores data in the cloud, one often has little control or even knowledge about the places where it is being held; these are decisions that are instead generally entrusted to computer algorithms. The user thus lacks knowledge and choice as to the rules that apply.

Id. at 368.

129. *Id.* at 331.

it is often difficult to attribute digital activities to their source, it follows that it is difficult to know whether digital activity is traceable to a U.S. citizen or someone with sufficient voluntary connections to the United States.[130] Further, she explains, because it is not even clear what sufficient voluntary connections are in the digital world, data destabilizes the territorial presumptions underlying the Fourth Amendment—which critically hinge on the "ability to define 'here' and 'there.' "[131]

A few ways in which the U.S. Supreme Court has also acknowledged that data is unique relate to its immense collection and storage capacities. Recall the U.S. Supreme Court case of *Riley v. California*. There, the Court was concerned with warrantless searches of cell phones that were seized from an individual during an arrest.[132] The majority discussed at length modern cell phones' immense storage capacities, noting how phones "can store millions of pages of text, thousands of pictures, or hundreds of videos."[133] Similarly, the Court noted how data lacks the physical properties of mail, wallets, purses, and other objects that can only be carried to the extent that is physically feasible.[134] In addition, it discussed how emails and text messages catalogue diverse information, dating back many years and revealing more in combination than any isolated record.[135] Critically, the Court was not concerned with cell phone searches due to any hardware properties of cell phones. The concerns were due to special traits of data: its portability, the breadth and duration of its storage capacities, and the extent to which it collectively reveals intimate details about a person's life.

Professor Daskal's solution to dealing with data's nuanced challenges is to reconfigure the scope of the Fourth Amendment.[136] She describes three ways that this can be done. The first proposal, which she attributes to Professor Orin Kerr, is to adopt an "Equilibrium-Adjusted Fourth Amendment." [137] This entails adapting the Fourth Amendment to new technological

130. Indeed, in the *Microsoft* case, the citizenship of the customer whose email content was sought was unknown to the court.

131. Daskal, *supra* note 11 at 329. Two more cases that Professor Daskal uses to illustrate the territorial presumptions underlying the Fourth Amendment are *Morrison v. National Australia Bank Ltd.* and *United States v. Verdugo-Urquidez.* In *Morrison,* the Supreme Court upended longstanding assumptions about the reach of U.S. securities law in order to fortify the presumption against the extraterritorial application of statutory law.

132. Riley v. California, 134 S. CT. 2473, 2480 (2014).

133. *Id.*

134. *Id.*

135. *Id.*

136. Daskal, *supra* note 11, at 379.

137. *Id.* at 380–83.

developments by "maintaining the status quo."[138] In other words, it upholds the Supreme Court's precedent that Fourth Amendment protections do not apply to searches and seizures of property owned by a non-resident alien in a foreign country due to the alien's insufficient voluntary relationship with the United States. [139] Thus, it maintains the current balance between government and individual needs.[140]

Her second proposal is for courts to adopt a "Presumptive Fourth Amendment," which assumes that the Fourth Amendment applies in all instances of U.S. data collection until proven otherwise.[141] This entails treating U.S. person targets and non-U.S. person targets alike, "absent clear and convincing evidence that collection does not encompass communications to or from a U.S. person or include other data . . . that have been generated in whole or in part by a U.S. person." [142] In other words, she explains, "if a warrant based on probable cause is required to collect the content of electronic communications, it should presumptively be required across the board, for both citizen and noncitizen targets—irrespective of the location of the data or the target."[143] Her third proposal is to adopt a "Universalist Fourth Amendment," which entirely rejects both the Fourth Amendment's territorial and identity-based limitations in order to provide a bright line response to incidental data collection. [144] This approach, while similar to the presumptive Fourth Amendment approach, involves applying the Fourth Amendment even to the collection of " 'wholly' noncitizen, nonresident communications."[145]

This paper does not insist that courts to go as far as adopting any of Professor Daskal's three territoriality paradigms. Rather, this paper encourages courts to start thinking about extraterritoriality in a more textured manner in the context of gathering criminal evidence, which is necessary due to the nuanced nature of data. Indeed, as this paper later discusses, the extraterritoriality analysis that the Second Circuit recently employed in the *Microsoft* decision was largely possible because the record was silent as to the nationality of the customer whose

138. *Id.* at 380.
139. United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).
140. Daskal, *supra* note 11, at 380.
141. *Id.* at 383–86.
142. *Id.* at 383.
143. *Id.* at 384.
144. *Id.* at 386–87.
145. *Id.* at 386.

email content was sought.[146] As such, the Court never had to assess the Fourth Amendment or SCA's extraterritorial application based on citizenship or voluntary connections to the United States, factors upon which a digital extraterritoriality analysis should hinge.

Because *Microsoft* left open numerous important issues that courts need to assess as they develop a framework for digital territoriality, this paper advocates the use of active cross-referencing to allow U.S. courts to compare Fourth Amendment reasonableness concerns with analogous foreign law concepts such as the EU's concerns of legality, necessity, and proportionality. Cross-referencing will also enable U.S. judges to see how privacy rights protected by EU law are already being vindicated in an extraterritorial manner. A case illustrating this is next discussed.

B. International Trade: Trials and Tribulations

The recent ECJ case of *Maximillian Schrems v. Data Protection Commissioner* involved Mr. Schrems, a user of Facebook, who resided in Ireland.[147] Upon registering for Facebook, Mr. Schrems signed a contract with Facebook, Ireland (a subsidiary of the U.S. company Facebook Inc.), accepting that some or all of his personal data on Facebook would be transferred to servers belonging to Facebook Inc. located in the United States, where it could undergo "processing."[148] On June 25, 2013, Mr. Schrems lodged a complaint to the Commissioner, asking him to exercise his statutory powers under the EU Data Processing Directive to prohibit Facebook Ireland from transferring his personal data to the United States, which he believed did not ensure "adequate protection" from U.S. surveillance authorities.[149] The Commissioner—relying on a prior Commission decision that found data transfer provisions between the United States and European Union sound—decided that he was not required to investigate Mr. Schrems's matter and rejected his complaint.[150] Mr. Schrems then appealed to the Irish High Court (High Court), which held that, although the surveillance and personal data interception occurring in the United States served

146. Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

147. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627 ¶ 26.

148. *Id.* ¶ 27.

149. *Id.* ¶ 28.

150. *Id.* ¶ 29.

necessary and indispensable aims, the National Security Administration (NSA) was significantly overreaching in how it was pursuing those aims.[151]

The High Court determined that EU citizens lacked appropriate redress in the United States, where oversight of intelligence services' actions is carried out through an *ex parte* framework and in a secret procedure.[152] Additionally, it held that the mass and undifferentiated accessing of personal data violated the proportionality principle from the Irish Constitution.[153] Much like the finding in *Digital Rights Ireland*, the High Court found that in order to be proportionate, data collection would have to be proven necessary, targeted towards specific groups of people, and objectively justified in the interests of national security or for the suppression of crime.[154] It would also need to occur with verifiable safeguards.[155] Because there was sufficient doubt as to whether the United States met these standards, the High Court held that the Commissioner was wrong to reject Mr. Schrems' complaint and recommended the case to the ECJ.[156]

In reviewing the questions raised by the High Court, the ECJ made several important points. First, it recognized that the Data Processing Directive sought to strike a balance between observing a fundamental right to privacy and promoting the free flow of personal data to expand international trade.[157] Second, it recognized that when EU member states transfer EU persons' data to third parties, the member states are required to comply with the Data Processing Directive by monitoring such transfers to ensure that the third party countries adequately protect EU persons' personal data.[158] Third, addressing the procedural matter, the High Court determined that member states and their organs could not adopt measures contrary to Commission decisions until those decisions were declared invalid—and since the ECJ had upheld the Safe Harbor Agreements between the United States and EU in a prior decision, that determination was binding.

The ECJ then held that it was incumbent on national supervisory authorities to examine claims regarding the adequate protection of personal data transferred to third parties "with all

151. *Id.* ¶ 30.
152. *Id.* ¶ 31.
153. *Id.* Recall that the proportionality principle is enshrined in EU law generally.
154. *Id.*
155. *Id.* ¶ 33.
156. *Id.* ¶ 36.
157. *Id.* ¶¶ 42–43, 48.
158. *Id.* ¶¶ 46–47.

due diligence."[159] In cases in which a Commission rejected a member's claim as unfounded, the EU member must have access to judicial remedies, enabling him to challenge such a decision before the national courts.[160] Regarding the validity of the ECJ's prior decision upholding the Safe Harbor provisions between the EU and United States, the ECJ found that decision to be invalid as it improperly denied national supervisory authorities the powers they derived from the Processing Directive to investigate a good faith claim by an EU member challenging the adequate protection of personal data transferred to third parties.[161]

Notably, in arriving at its decision, the ECJ actively cross-referenced U.S. data processing procedures and laws. It also explained that the United States did not need to employ identical levels of protection to the European Union, but needed measures that were "essentially equivalent."[162] Similarly, it stated that while the means of redress for aggrieved targets need not be the same in the United States and in the EU, targeted persons must have "effectively" the same recourse for challenging the collection of their personal data compared to what they have in the EU.[163] Further, the Court acknowledged how critical bulk data collection is for national security, public interest, and law enforcement.[164] Yet, it found that the United States derogated from the safe harbor provisions with too much latitude and no consideration for whose data it was collecting, thereby violating the principle of proportionality. [165] Moreover, the ECJ was troubled that no evidence suggested that the United States was trying to limit its interference with EU members' personal data or employing minimization procedures to reduce the risk of subsequent abuse of that data.[166] Thus, the ECJ concluded that the United States did not adequately protect data and infringed the EU Charter's right to private life.[167]

The holding of this case is profoundly important. It shows that the primary EU test governing the adequacy of transatlantic data transfers is proportionality, and a procedure for active cross-referencing is already built into the EU Data Processing Directive which assesses the *domestic* legality of data processing systems

159. *Id.* ¶ 63.
160. *Id.* ¶ 64.
161. *Id.* ¶¶ 102,106.
162. *Id.* ¶ 73.
163. *Id.* ¶ 74.
164. *Id.* ¶¶ 85–86.
165. *Id.* ¶¶ 87–88.
166. *Id.* ¶ 91.
167. *Id.* ¶¶ 93–95.

and the *domestic* necessity for states to implement data processing systems that are commensurate with their legitimate aims.[168] The holding also reflects that the ECJ readily undertakes active cross-referencing of foreign laws and compares them to EU laws when dealing with cross-continental disputes, particularly in cases like *Schrems*, which involved an EU national, residing in the EU, who voluntarily chose to register for Facebook, a U.S. company that was in full compliance with U.S. laws and provides its terms of service in plain sight to all its users. Consequently, the ECJ not only engaged in active cross-referencing, but it did so while enlarging the extraterritorial breadth of Mr. Schrems's EU-based privacy rights.

Notably, in cross-referencing U.S. laws, the ECJ still came to reasoned conclusions that protected EU Charter rights. Yet few U.S. federal courts engage in any comprehensive cross-referencing analysis when dealing with foreign law conflicts. Indeed, in recent decades, there has been a dearth of foreign law referencing and a surge of court-ordered law breaking abroad.[169] The prudency of this trend is questionable. As Supreme Court Associate Justice Breyer discusses in his book, legal analysis is likely to be enhanced, not diluted, through cross-referencing foreign laws.[170] Courts around the world face common legal challenges due to the borderless nature of data, and many countries strive to enhance national security while minimizing the costs to individual privacy. Further, many nations pursue these aims through similar frameworks that are only formalistically different. In a deeply interconnected world involving common threats and interests, the rule of law is bolstered, not diminished, when courts share insights with one another.

---

168. 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, art 26(1)(d), 1995 O.J. (L 281) 31, 46; *see also* Alan Charles Raul, Edward McNicholas & Elisa Jillson, *Reconciling European Data Privacy Concerns with US Discovery Rules: Conflict and Comity*, 3 GLOBAL COMPETITION LITIG. REV. 119, 123 (2009).

169. *See* Sant, *supra* note 2, at 197–232 (chronicling and graphing the recent exponential growth in the number of cases in which requests for violations of foreign law during discovery have been made); C. Todd Jones, *Compulsion over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 NW. J. INT'L L. & BUS. 454 (1992); Russell J. Weintraub, *The Need for Awareness of International Standards When Construing Multilateral Conventions: The Arbitration, Evidence, and Service Conventions*, 28 TEX. INT'L L.J. 441 (1993); Joseph F. Weis, Jr., *The Federal Rules and the Hague Conventions: Concerns of Conformity and Comity*, 50 U. PITT. L. REV. 903 (1989).

170. BREYER, *supra* note 1, at 240 ("To learn from foreign opinions or to consider their reasoning is to find in them something of use in interpreting *American*, not foreign, law. It is not to treat law as an abstract 'brooding omnipresence.' Foreign as well as domestic experience can be of help in understanding the commands of American sovereigns, whether federal or state, that have enacted the particular legal phrase in question.").

The final case discussed in this paper illustrates how the U.S. Government attempted to attain digital evidence but was hindered by a foreign-law conflict. It further shows how the judges adjudicating the case ascertained extraterritoriality mainly by interpreting the text of the SCA, the method proscribed by the Supreme Court. The next section explains why, although the Second Circuit correctly approached its extraterritoriality analysis based on binding Supreme Court precedent, the method that it was compelled to use is ill-suited for criminal procedure and digital evidence gathering. Thus, even though the Second Circuit recommended that Congress promptly amend the the SCA and provide more clarity as to its extraterritorial scope, the Second Circuit did not shed much light on how lower courts should think about digital evidence requests in situations that may differ slightly from the one that was presented. For example, the Court alluded to the multiple types of related situations that could ultimately be deemed territorial enough for the presumption against extraterritoriality not to be triggered at all. The next section explains *Microsoft Corp. v. United States* and then discusses how courts can use cross-referencing to assist them when assessing the territoriality of digital warrants.

C. Cross-Border Crimes: Warrants and Whereabouts

Microsoft v. United States began on December 4, 2013, when the United States Government presented Magistrate Judge Francis IV of the Southern District of New York with an affidavit that established probable cause for the Government to believe that a Microsoft-based email account, located on a server in Ireland, was being used to further narcotics trafficking.[171] After making an independent determination, pursuant to Federal Rule of Criminal Procedure Rule 41 (Rule 41) and the SCA, Judge Francis issued Microsoft a warrant (the Order) directing it to disclose to the U.S. Government any contents of the email account that were in its possession, custody, or control.[172]

---

171. *Id.* at 467–68.

172. The SCA warrant required Microsoft to disclose: a) the contents of all e-mails stored in the specified user's account, including those sent; b) all records or other information regarding the identification of the user of the account (such as name, address, phone number, etc.); c) all records or information stored on account including address books, contact lists, pictures, and files; and d) all records of communication between the user and Microsoft Network (MSN). Warrant for Microsoft Corp. Email, 15 F. Supp. 3d 466, 468 (S.D.N.Y. 2014).

In issuing the Order, Judge Francis recognized the unique challenge of borderless data, noting: "[t]he 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 any current territorially based sovereign."[173] In addition, Judge Francis explained that the unusual nature of data made the warrant "a hybrid: part search warrant and part subpoena."[174] He noted that it was procedurally like a warrant because the Government had to provide reasonable grounds for believing that the content of the email account was relevant and material to an ongoing investigation.[175] But, he explained, it was executed like a subpoena in that it would be served on the ISP in possession of the information and would not involve government agents entering Microsoft's premises to search its servers and seize the e-mail account in question.[176]

Microsoft moved to quash the Order, arguing that it violated the long-held presumption against extraterritoriality because the SCA was a statute that only had domestic reach.[177] Judge Francis rejected Microsoft's extraterritorial argument, finding that, "the SCA does not criminalize conduct taking place in a foreign country, . . . does not involve the deployment of American law enforcement personnel abroad, [and] . . . does not require even the physical presence of service provider employees at the location where [the] data [is] stored."[178] Thus, it involved "solely the purport of municipal law which establishes the duty of a citizen in relation to his own government,"[179] and only "places obligations . . . on the service provider to act within the United States."[180] Judge Francis noted that even if the SCA, a domestic law, was intended to be a territorial statute, the question of its application to citizens and non-citizens of the United States "is one of construction and not of legislative power."[181] Thus, he indicated that, although Congress defines the territorial scope, determining a domestic statute's

---

173. *Id.* at 466, 467 (quoting David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996)).

174. *Id.* at 471.

175. *Id.*

176. *Id.*

177. *Id.* at 467. This presumption states: an act of Congress does not apply outside the United States unless Congress clearly says so. EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991).

178. Warrant for Microsoft Corp. Email, 15 F. Supp. 3d 466, 475 (S.D.N.Y. 2014).

179. *Id.* at 476 (citing Blackmer v. United States, 284 U.S. 421, 437 (1932)).

180. *Id.* at 476.

181. *Id.* at 477 (citing *Blackmer*, 284 U.S. at 437).

scope based upon the connections between the United States and the target was within the purview of the court.

In response to the Order, Microsoft filed a motion to stay the execution of the warrant.[182] The issue was then brought before Chief District Judge Loretta Preska of the Southern District of New York.[183] Upon reviewing the Order, Microsoft's Motion to Stay the Warrant, and the Government's Motion to Lift the Stay; and after hearing arguments from both the Government and Microsoft, Chief Judge Preska granted the Government's Motion to Lift the Stay, upholding the validity of SCA warrant.[184] In so doing, Judge Preska agreed with Judge Francis that the structure, language, legislative history, and Congressional knowledge of precedent indicated that Congress intended the SCA to allow ISPs to produce information under their control, regardless of the information's location.[185]

Microsoft then appealed to the Second Circuit. In its brief, Microsoft made several key arguments. First, focusing on extraterritoriality, it conjured images of foreign banks ordering their U.S. subsidiaries to go rummaging through a safe deposit box in search of items for foreign discovery—what it claimed was the reverse analogy of the Order.[186] Microsoft emphasized the Court's long-held policy against applying a U.S. law outside of U.S. territory absent a clear Congressional mandate to do so, a principle known as the presumption against extraterritoriality.[187] It argued that while no U.S. personnel had to enter premises in Ireland, the warrant still remotely compelled Microsoft to complete a search and seizure of an email account that was located exclusively in Ireland, thereby infringing Irish sovereignty.[188]

Microsoft also challenged the District Court's employment of the "hybrid" subpoena, arguing that such a construction would be inconsistent with what Congress actually wrote and intended in

---

182. Although Microsoft filed a motion to stay the execution pending review by the court of appeals, its notice of appeal in response to Judge Francis's order was deemed immature as the order had to first be reviewed by the District Court. *In re* A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624, at *1 (S.D.N.Y. Aug. 29, 2014).

183. *Id.* at *1–2.

184. *See generally id.*; Transcript of Oral Argument at 69, *In re* A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014).

185. *See generally Microsoft Corp.*, 2014 WL 4629624; Transcript of Oral Argument at 69, *In re* A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014).

186. Brief for Appellant at 1–2, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

187. *Id.* at 19.

188. *Id.* at 31–35.

the SCA.[189] It argued that there is a difference between ordering a company with a foreign subsidiary to produce its own records and ordering a company functioning as a *caretaker* of private records to produce records.[190] It pointed out that email customers are akin to bank account holders or FedEx customers in that they lack any legitimate expectations of privacy to non-content information that they have voluntarily conveyed to providers, but they maintain a legitimate expectation to privacy in the private intimate contents of their electronic messages, and thus providers have only limited control over those emails.[191] Microsoft addressed foreign policy concerns as well. Emphasizing reciprocity, Microsoft warned that a breach of sovereignty in one instance would lead to similar breaches all over the world and diminish foreign relations.[192]

The U.S. Government emphasized several key counter-points. First, it emphasized that the SCA clearly authorized the use of warrants to compel the production of records "in a manner functionally similar to subpoenas, orders, summonses, and other instruments compelling the production of records."[193] Therefore, Microsoft's warrant-subpoena distinction ignored the basic fact that SCA warrants were designed to function as a form of compelled disclosure.[194] Second, it noted that nothing in the SCA's text, structure, purpose, or legislative history indicated that compelled production of records was limited to records stored domestically.[195]

Again, it emphasized that the SCA was written with a focus on disclosure, such that as long as the entity in control of the records was subject to the jurisdiction of the court ordering their disclosure, the location of the records did not matter.[196] It also argued that compliance with the warrant did not implicate the presumption against extraterritoriality because Microsoft's challenge to the warrant had nothing to do with the substantive provisions of any U.S. law.[197] Further, it claimed that because the U.S. Court had clear personal jurisdiction over Microsoft, the

189. *Id.* at 36–40.

190. *Id.* at 41–43. Microsoft further bolstered this argument by emphasizing that it is not free to peruse the records of its clients as it pleases. *Id.* at 43.

191. *Id.* at 43.

192. *Id.* at 48–52.

193. Brief for Appellee at 18, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

194. *Id.* at 19.

195. *Id.* at 26.

196. The Government also pointed out that at the time the SCA was enacted in 1986, it was a settled point of law that compulsory process could reach records stored overseas—a point it believes Congress must have understood when it legislated. *Id.* at 27.

197. *Id.* at 31.

Court had the authority to compel Microsoft to disclose relevant records in its possession, custody, and control.[198] Also, because the issue at hand was merely evidentiary, none of the cases that involved the extraterritoriality of substantive U.S. law applied.[199] In fact, the Government argued, the Fourth Amendment was not designed to interfere with the power of courts to compel production of documentary evidence when regulating conduct occurring within the United States. And irrespective of where Microsoft stored records, no search and seizure occured without an attempt to enter an entity's premises against its will.[200]

The Government also countered Microsoft's argument that compelled production can only reach an entity's own business records and not those that it holds on behalf of others.[201] It emphasized that neither the Supreme Court nor the Second Circuit has ever recognized any restriction on compelled production of records or employed a test other than simple "control."[202] The Government even challenged the premise that Microsoft served as a caretaker for its customers' accounts.[203] Rather, it argued that Microsoft informed its customers that when they transmit or upload content to Microsoft's services, they provide Microsoft the right to use that content as necessary.[204] Regarding the territorial scope of the Fourth Amendment based on citizenship, the Government challenged the idea that Fourth Amendment protections extended to parties who are non-citizens located outside of U.S. territory; but even if they did, the Government argued that compulsory process always enabled the Government to obtain Fourth Amendment-protected records in the custody of a third party.[205]

---

198. *Id.* at 31–32. Here the Government cited *United States v. First Nat'l City Bank*, 379 U.S. 378, 384 (1965) which held that "Once personal jurisdiction of a party is obtained, the District Court has authority to order it to 'freeze' property be within or without the United States." *Id.* at 32.

199. *Id.* at 33 ("The concern of the presumption against extraterritoriality is with the substance of laws reaching beyond U.S. borders, not the overseas consequences of U.S. laws applied domestically.").

200. The Government also noted that any other reading of the SCA's Warrant provision would invalidate the Internal Revenue Code, requiring that any time a corporation had to pay its taxes, it would have to first transfer funds held abroad to the U.S. or else those funds would not fall within the ambits of U.S. tax laws. *Id.* at 33.

201. *Id.* at 36.

202. The Government also noted that nothing in the law prohibits using compulsory process to obtain Fourth Amendment-protected records under the control of a third party, and that holding in *United States v. First City Nat'l Bank*, 379 U.S. 378 (1965), also weakened Microsoft's position. Brief for Appellee at 37–38, Microsoft Corp. v. Unitd States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

203. *Id.* at 41.

204. *Id.* at 41–42.

205. *Id.* at 44.

The Government also addressed foreign policy concerns. First, the Government argued that compliance with the warrant would not raise any comity concerns because the order did not require Microsoft to violate the law of Ireland or the EU.[206] Second, it argued that Microsoft's belief that the warrant would be "offensive to foreign sovereignty" was "vague," and that such orders did not violate international norms.[207] As a more pressing public policy concern, the Government argued that because the physical location where an email gets stored depended upon the location that a Microsoft user purported to be in when the user registered for an account, stronger policy considerations weighed against creating an easily abused loophole in the SCA that could lead to arbitrary outcomes and criminal abuse by fraudsters, hackers, and drug dealers.[208]

Interestingly, while both Microsoft and the Government's briefs addressed foreign policy concerns towards the end, the majority of amicus briefs that were filed focused on the foreign policy implications of the dispute.[209] Microsoft argued that addressing sovereignty concerns on a case-by-case basis would be impractical, and therefore emphasized that the court simply focus on the presumption against extraterritoriality that applied to the SCA.[210]

---

206. *Id.* at 44.

207. *Id.* at 45–46. The Government also stated: "Microsoft's concern for comity is more rhetorical than real." *Id.* at 47.

208. *Id.* at 53.

209. *See, e.g.*, Brief for Anthony J. Colangelo, Int'l Law Scholar as Amici Curiae Supporting Appellants, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985) (describing how the principles of sovereignty and non-intervention are well-established under customary international law and preclude one state from exercising law enforcement jurisdiction in the territory of another state); Brief for Ireland as Amici Curiae Supporting Appellants, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985) (arguing that national sovereignty is never waived by non-intervention in foreign domestic court proceedings and endorsing application of the MLAT process in order to avoid conflicts as much as possible); Brief for Apple as Amici Curiae Supporting Appellants, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985) (explaining that both European and Irish law provide access for law enforcement bodies to personal data and that the self-executing MLAT procedure would have been the most efficient and diplomatic channel to avoid unilaterally infringing on fundamental Irish human rights); Brief for Brennan Center for Justice at NYU School of Law, Am. Civil Liberties Union, The Constitution Project, and Elec. Frontier Found. as Amici Curiae Supporting Appellants, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985) (discussing how because reciprocity is implicated in cross-border privacy disputes, the U.S. Government's unilateral actions would embolden foreign governments to access American data under far weaker standards); Brief for Dig. Rights Ir. Ltd., Liberty, and the Open Rights Grp. as Amici Curiae Supporting Appellants, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985) (describing how although data is a human right protected by Irish law, both EU and Irish law provide law enforcement access to personal data through the MLAT procedures, which therefore should have been used in order to protect both sovereigns interests).

210. Brief for Appellant at 52–53, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985). Microsoft endorsed the Supreme Court's position regarding the

The U.S. Government argued that sovereignty concerns were not implicated because Microsoft had never proven that any Irish or EU laws were violated by the warrant.[211]

As the following section demonstrates, the Second Circuit ultimately adopted the majority of Microsoft's arguments, but less out of a concern for Irish sovereignty, and more so due to the text and structure of the SCA. Moreover, in Judge Lynch's well-reasoned concurrence, he addressed why, although Microsoft had the better of arguments based on how courts are required to assess extraterritoriality, the implications of the holding do not align with the important policies that underly criminal procedure jurisprudence. Therefore, this next section reviews the Second Circuit's holding, explains relevant aspects of the SCA and Rule 41, discusses the extraterritorial issues that the Court must still address, and explains how courts can cross-reference foreign cases to deal with future digital evidence disputes.

V. DIGITAL EXTRATERRITORIALITY

One of the most interesting aspects of the *Microsoft* case is that it was not initially a dispute over the meaning of extra-territoriality. As the Second Circuit noted, Microsoft continually tried to frame the issue as one regarding the extent of U.S. laws and warrants, whereas the Government consistently framed the issue as one about compelled disclosure.[212] For this reason, the Second Circuit focused on setting the correct frame of reference as opposed to developing a robust framework for lower courts to apply when confronted with similar novel requests.

A. The Second Circuit's Reasoning

The Second Circuit arrived at its holding largely by engaging in a statutory and legislative analysis of both the SCA and Rule 41. Turning first to the SCA, it explained how the statute was created as part of the Electronic Communications Privacy Act (ECPA) in 1986, before the Internet became an integral part of daily life and two years before the creation of the World Wide Web.[213] The Court

---

presumption against extraterritoriality in the case of *Morrison v. National Australia Bank*, 561 U.S. 247 (2010) (regarded the Securities Exchange Act). *Id.* at 50.

211. Brief for Appellee at 45, Microsoft Corp. v. Unitd States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

212. Microsoft Corp. v. United States, 829 F.3d 197, 201 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

213. *Id.* at 205–06.

explained how the SCA was designed to afford privacy protections to electronic records in a manner analogous to the Fourth Amendment.[214] Further, where the SCA required a warrant (to access more recent communications), it directed the Government to use the procedures described in Rule 41.[215] The Court then laid out the analytic framework for discussing extraterritoriality. Echoing the Supreme Court's reasoning in *RJR Nabisco, Inc. v. European Cmty.* [216] and relying upon the framework set out previously in *Morrison v. National Australian Bank*,[217] the Court decided that it had to engage in a two-part inquiry to assess the statute's extraterritorially.[218] First, it had to ascertain whether the relevant statutory provisions "contemplate extraterritorial application," and second—if it found that they did not—the Court would have to identify the statute's "focus."[219]

Looking at the text of the SCA and comparing it with statutes where courts found affirmative indications of extraterritorial intent, the Court was unable to find comparable textual support in the SCA.[220] Further, because the parties did not dispute that the SCA failed to expressly discuss extraterritoriality, the Court directed its attention to ascertaining the statute's focus to determine whether the statute could, in fact, be applied extraterritorially.[221] The Court also acknowledged that it would be a rare case where there are no contacts at all with U.S. territory. Therefore, determining whether there was a "prohibited application" of the statute really depended on "whether the domestic contacts [were] sufficient to avoid triggering the presumption at all."[222]

The Court then determined that the focus or "object of the statute's solicitude" for the SCA was to protect private content of the user's stored electronic communications. [223] The Court discerned this after analyzing the statute's legislative history—

---

214. *Id.* at 206.

215. *Id.* at 208.

216. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016).

217. Morrison v. Nat'l Australian Bank Ltd., 561 U.S. 247 (2010).

218. Microsoft Corp. v. United States, 829 F.3d 197, 209–10 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

219. *Id.* at 210.

220. *Id.* at 211 (describing the examples of § 18 U.S.C. 2331(1), which refers to acts that "occur primarily outside the territorial jurisdiction of the United States" and 18 U.S.C. § 2423(b), which expressly criminalizes "travel in foreign commerce undertaken with the intent to commit sexual acts with minors.").

221. *Id.* at 216.

222. *Id.*

223. *Id.* at 217 (citing Morrison v. Nat'l Australian Bank Ltd., 561 U.S. 247, 267 (2010)).

referring to the title of the statute, congressional hearings, the history of the Internet's development, and other provisions within the statute that also provide means to protect the content of stored electronic communications.[224] It also noted how the compelled disclosure process in the statute adopted the procedures found in the Federal Rules of Criminal Procedure.[225]

The Court also addressed the Government's argument that the statute used "warrant" to describe what was functionally a subpoena; the Court did so by delving into the special meaning and history of warrants.[226] The Court noted that the term warrant "is endowed with a legal lineage that is centuries old,"[227] and that the "chief evil that prompted the framing and adoption of the Fourth Amendment was the indiscriminate nature of searches and seizures conducted by the British under the authority of general warrants."[228] It concluded that warrants are distinct legal instruments from subpoenas and are anchored to privacy concepts applicable within U.S. territory.[229] The Court also noted that if U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have "dubious legal significance, if any, in a foreign nation."[230] Accordingly, it determined that warrants are distinctly territorial instruments, and any cases that involved compelling foreign banks or other entities to produce their own communications stored overseas, pursuant to subpoenas, were inapposite.[231]

* * *

Indeed, a warrant is the linchpin of the Fourth Amendment. The amendment protects against unreasonable searches or seizures, *unless* justified by a warrant.[232] The Federal Rules of Criminal Procedure, which govern search and seizure law, derive from this framework. The most relevant rule concerning searches and seizures of digital data is Rule 41, which provides the procedure for how a federal law enforcement officer or government attorney may attain a warrant from a magistrate judge so as to

224. *Id.* at 217–20.
225. *Id.*
226. *Id.* at 212.
227. *Id.*
228. *Id.* (citing United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013)).
229. *Id.*
230. *Id.* (quoting United States v. Mohamed Sadeek Odeh, 552 F.3d 157, 171 (2008)).
231. *Id.* at 201-202, 212–13, 216.
232. U.S. CONST. amend. IV.

conduct a search or seizure.[233] Rule 41(d)(1) allows a magistrate judge, after receiving an affidavit or other information, to issue a warrant if he believes there is probable cause to justify the search or seizure.[234]

Importantly, Rule 41(b) articulates five territorial paradigms under which a magistrate judge may issue such a warrant.[235] A magistrate judge may issue a warrant: (1) for property located within the district,[236] (2) for property outside the district if the property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed,[237] (3) in terrorism investigations—for property in any district in which the activities related to the terrorism may have occurred, [238] (4) for moving property—to track movement of property within a district, outside the district, or both,[239] and (5) for property outside the jurisdiction of any state or district but within the United States' premises—if related to crime that occurred within the magistrate judge's district. [240] Notably, the rules define "property" to include "information," [241] and the Supreme Court has held that "property" under Rule 41 includes intangible property, such as computer data. [242] Further, Rule 41(e)(2)(B) authorizes a magistrate judge to issue a warrant to seize electronic media or information and permits a later review of that media or information.[243]

The Second Circuit, in finding that the SCA did not contain an express or implied extraterritorial capability, relied on the method prescribed by the Supreme Court in *Morrison* to analyze extraterritoriality in statutes. But even though *Morrison* held that the presumption against extraterritoriality is applicable in all cases where a party seeks to give any federal legislation extraterritorial effect, the underlying premise that Congress would be equally likely to include extraterritorial language in substantive laws and procedural laws is dubious. As the Second Circuit noted,

---

233. FED. R. CRIM. P. 41.
234. *Id.* r. 41(d)(1).
235. *Id.* r. 41(b).
236. *Id.* r. 41(b)(1).
237. *Id.* r. 41(b)(2).
238. *Id.* r. 41(b)(3).
239. *Id.* r. 41(b)(4).
240. *Id.* r. 41(b)(5).
241. *Id.* r. 41(a)(2)(A).
242. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp. 2d 753, 756-57 (S.D. Tex. 2013) (citing United States v. New York Tel. Co., 434 U.S. 159, 170 (1977)).
243. FED. R. CRIM. P. 41(e)(2)(b).

the record was silent as to the citizenship and location of the customer.[244] The Court indicated that, had these factors been known and created sufficient ties to the United States, the issue of extraterritoriality may not have been triggered at all, even if the emails were still located in a foreign state.[245]

Although the Supreme Court in *Morrison* was rightly concerned with legislative and adjudicative consistency, Judge Lynch and Professor Daskal have both emphasized that extraterritoriality in the digital realm cannot be an overly simplified test that fails to take into account the unique borderless characteristics of data or any of the attributes about the target whose data is sought. Therefore, the next section discusses the holes that the Second Circuit's holding left open as well as some of the practical consequences and policy implications of the decision. The final section then explains how courts can use the body of recent EU jurisprudence to more fully develop the extraterritoriality framework going forward.

B. Lingering Issues

Although the Second Circuit comprehensively analyzed the relevant statutes at issue and employed the framework for assessing the presumption against extraterritoriality that was promulgated by the Supreme Court in *Morrison*, the decision left open numerous complex issues that are unique to data disputes.

1. Data is Unique

In his concurrence to *Microsoft*, Judge Lynch emphasized that because the presumption against extraterritoriality provides that Congress legislates with domestic concerns in mind, when Congress enacts legislation that provides tools to law enforcement, it is legislating not with a singular focus on privacy, but rather, with a focus on finding the right *balance* between domestic law enforcement needs and domestic persons' liberty interests.[246] In

244. Microsoft Corp. v. United States, 829 F.3d 197, 212 (2d Cir. 2016) (citing United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013)), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

245. *Id.* at 216. The Court here implied that had the Government shown sufficient domestic contacts with the United States, the presumption against extraterritoriality would never have been triggered. It is possible that the requisite domestic contacts existed; however, the record was silent as to the nature of the contacts.

246. *Id.* at 229 ("[I]n connection with statutes that provide tools to law enforcement, one imagines that Congress is concerned with balancing liberty interests of various kinds against the need to enforce *domestic* law.").

other words, Judge Lynch posited that Congress enacts legislation pertaining to electronic information with a keen focus on the unique structural design of the Fourth Amendment.

Judge Lynch also noted how transnational crimes are likely to grow increasingly complex and involve multiple jurisdictions, and electronic documents are likely to be stored in increasingly virtual, as opposed to physical, locations.[247] Recall that Professor Daskal explained that some of the unique properties of data are its mobility, interconnectedness, and divisibility. [248] She explained that data moves in unpredictable ways when en route from one destination to another—traversing paths unknown to the sender and recipient, and that it often crosses many sovereign borders while being transmitted.[249] Although in this case, there was no question that the relevant data was stored in a physical server located in Ireland, as opposed to a completely non-territorial "cloud," if courts use an overly simple bright-line test for ascertaining the extraterritorial reach of U.S. laws, it will leave unaccounted data that is intercepted en route to a particular destination, data that touches U.S. borders temporarily, and other multi-border paradigms that flow from data's inherent mobility, divisibility, and interconnectedness.

A closely related issue that Judge Lynch mentioned and Professor Daskal described is that data is not tangible like other objects that traditional search warrants allow law enforcement to access. Indeed, data is defined as:

> 1) factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation;
>
> 2) information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful;
>
> 3) information in numerical form that can be digitally transmitted or processed.[250]

---

247. *Id.* at 231.

248. Daskal, *supra* note 11, at 331.

249. *Id.* at 368 ("Similarly, when one stores data in the cloud, one often has little control or even knowledge about the places where it is being held; these are decisions that are instead generally entrusted to computer algorithms. The user thus lacks knowledge and choice as to the rules that apply.").

250. *Data*, MERRIAM-WEBSTER.COM http://www.merriam-webster.com/dictionary/data (internal references omitted) (last visited June 17, 2017).

These definitions show that data is more akin to a language than to traditional objects that fall within the purview of search warrants such as contraband. It is why the traditional Fourth Amendment arguments, stemming from the policy of protecting people from unwarranted physical intrusions into their home to conduct physical searches for tangible objects, begin to ring hollow. It is why fewer and fewer courts analogize items like cell phones and computers, with massive data storage capacities, to mere containers of contraband, which could never relay similar quantities and types of information.[251] It is why the Government's argument regarding the difference between a warrant requiring U.S. personnel to enter the premises in Ireland and a digital request for information is important. Although courts need to gradually transcribe a territorial legal system to a less territorial digital world, the Supreme Court has long held that physical intrusions implicate unique dignitary interests compared to non-physical intrusions.[252] Indeed, this is why physical intrusions still underlie the very concepts of individual and national sovereignty.[253]

---

251. *See, e.g*, Riley v. California, 134 S. Ct. 2473, 2489 (2014) ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy."); United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013) ("When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind. When carrying a laptop, tablet or other device, however, removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files."); United States v. Galpin, 720 F.3d 436, 446–47 (2nd Cir. 2013) (noting the enormity of digital storage renders search of a hard drive akin to that of a residence); United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) ([A computer's potential] to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs . . . ."); United States v. Payton, 573 F.3d 859, 861 (9th Cir. 2009) ("[C]omputers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (stating a computer cannot be akin to a container under the territorial limits of a Rule 41 search warrant because the court has found no support that would permit an unlimited search of the world until such time that a computer is found).

252. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531 (1985) (describing detention of the defendant though long and embarrassing was necessary due to the respondent's occupation as an alimentary canal cocaine smuggler.); United States v. Flores-Montano, 541 U.S. 149 (2004) (stating the search of a repository for fuel cannot be anymore invasive than the search of an automobile's passenger compartment and does not qualify as a serious invasion of privacy).

253. Recall that in *Silverman v. United States*, 365 U.S. 505 (1961), and in *United States v. Jones*, 565 U.S. 400 (2012), the Supreme Court intentionally dodged ascertaining the reasonable expectations to privacy in: intangible conversations that took place inside the home and GPS and cell phone data, respectively. Instead, the court found traditional physical property-based interests in the home and automobile, which it used to find Fourth Amendment searches and seizures taking place. *See supra*, Part I.

2. Identity Matters

Another important issue left open that Judge Lynch emphasized stems from the dearth of information regarding the citizenship or location of the email account user. Judge Lynch noted that the Supreme Court has stated that the presumption against extraterritoriality is more than simply a means for avoiding conflict with foreign laws.[254] He indicated that it is also about ensuring the integrity of U.S. laws.[255] This means that if a law was designed to apply to interactions between the U.S. Government and U.S. citizens or persons with sufficient connections to the United States, casting the net of extraterritoriality too wide would actually undermine the integrity of the statute.

Professor Daskal, too, explained the importance of focusing on the characteristics of the target and not just national borders when assessing extraterritoriality. She explained the extraterritoriality jurisprudence of the Fourth Amendment, which the Supreme Court largely shaped in *Verdugo-Urquidez*.[256] That case was about a Mexican drug-lord who was temporarily detained in a U.S. prison and who was a non-citizen with no other voluntary ties to the United States. He claimed that he was subjected to an unconstitutional search and seizure when U.S. law enforcement personnel searched his home in Mexico without a warrant.[257] The Supreme Court found that he was not protected by the Fourth Amendment and thus held that the Fourth Amendment did not prohibit U.S. agents from conducting a search or seizure to a noncitizen outside the United States who had no "significant voluntary connection" to the country.[258]

In arriving at its holding, the Supreme Court established that the extraterritoriality inquiry involved two layers of considerations—what Daskal called a "two-step decision tree."[259] While the first inquiry simply asked where the search or seizure took place, the second part of the inquiry—only triggered when the search occured outside the United States—focused on the characteristics of the target, namely, whether the target was a U.S. citizen or alien with substantial voluntary connections to the

254. Microsoft Corp. v. United States, 829 F.3d 197, 226 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

255. *Id.* at 14.

256. United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).

257. *Id.* at 265.

258. *Id.*; Daskal, *supra* note 11, at 339.

259. Daskal, *supra* note 11, at 340.

United States.[260] If the target was either of these, the Fourth Amendment applied and the test was one of reasonableness; but if instead the target was a noncitizen lacking substantial connections to the United States, the Fourth Amendment did not apply.[261]

This two-step inquiry is similar to the one that was promulgated in *Morrison*. *Morrison*'s first step asked a court to look at the text of the statute to ascertain extraterritorial intent and then at the statute's "focus" to see whether the domestic contacts were sufficient to avoid triggering the presumption at all, whereas *Verdugo-Urquidez*'s test asked a court to look first at the location of the search or seizure and next at the specific relationship between the target and the nation whose laws were being applied. It is interesting that the Second Circuit employed *Morrison*'s test rather than *Verdugo-Urquidez* when in *Morrison* the Court was deciding whether conduct that occurred abroad could be proscribed by a U.S. statute, whereas in *Verdugo-Urquidez* the Court was deciding whether certain criminal procedures for gathering evidence abroad were permissible for a prosecution in the United States—a seemingly closer fit to *Microsoft*.

Ultimately, however, the Court focused on *Morrison*, as it was one of the Supreme Court's most recent iterations on extraterritoriality. Therefore, what is important is that the Second Circuit ascertained the SCA's "focus" by conducting a natural reading of the text, examining other procedural and substantive provisions in the SCA, and looking at the statute's legislative history.[262] Despite acknowledging that the record was silent as to the citizenship and location of the customer, the Court concluded that these factors would not be important to the extraterritoriality analysis since the focus of the statute was on the location of the "invasion of a customer's privacy."[263] Although this analysis of the statute's "focus" provided useful statutory context for the Court, ultimately, it was an entirely different inquiry than one specifically directed at "sufficient contacts" or "voluntary connections" to the relevant nation, which is what *Verdugo-Urquidez* had emphasized.

That is not to say that if the Court had known the nationality of the account-holder, the analysis would have been easier.

---

260. *Id.*

261. *Id.*

262. Microsoft Corp. v. United States, 829 F.3d 197, 216–20 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

263. *Id.* at 220.

Professor Daskal notes that *Verdugo-Urquidez*, like many older territoriality cases, is "failing on its own terms" due to the "world of highly mobile and intermingled data."[264] But because the Second Circuit never considered how the analysis would apply if it were determined that the account-holder were in fact a U.S. citizen or an Irish national with sufficient voluntary connections to the United States, the Court has not resolved the matter. Indeed, the hardest part of both tests, which is challenging even in non-digital contexts, is determining what constitutes sufficient "voluntary connections" or "sufficient contacts" to the United States, such that conduct that is physically outside the borders of the United States falls under the purview of U.S. statutes.[265]

In *Verdugo-Urquidez*, the Supreme Court found that merely being detained in a U.S. prison for two days was an insufficient voluntary connection for the Fourth Amendment to govern a search and seizure that occurred abroad.[266] In a world where voluntary connections are now digital, one must ask: is there a sufficient voluntary connection to the United States when a foreign nonresident alien knowingly decides to use a U.S. business that provides a prevalent web-based service? The Second Circuit decision suggests that there is not. One can then ask: is there a sufficient voluntary connection when that same person uses a U.S. web-based service and has also been linked to a crime that occurred on U.S. soil? The Second Circuit did not address this question in Microsoft, but U.S. courts must eventually construct a consistent framework for analyzing digital extraterritoriality—one that is clearer than *Morrison*'s nebulous "focus" test. Court's need to explain, in the digitial context, what it means to apply a U.S. law abroad. And to do so, they must explain what types of voluntary digital connections are sufficient to put an individual who is not a U.S. citizen or national within the purview of the Fourth Amendment's framework.

3. Procedure versus Substance

A final unresolved issue in *Microsoft* regards the difference between applying *substantive* law abroad versus *procedural* law.[267]

264. Daskal, *supra* note 11, at 387.

265. *Id.* at 330–31.

266. *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

267. Consider the important distinction the courts have observed between procedural and substantive laws in federal courts. One of the fundamental doctrines regarding federal procedure is the Erie Doctrine. Derived from the Federal Rules of Civil Procedure and the Supreme Court case *Erie v. Railroad Co. v. Tompkins*, 304 U.S. 64 (1938), this doctrine holds that when U.S. federal courts hear diversity cases, they are required to apply state

Throughout its extraterritoriality analysis, the four main cases that the Court cited were: *RJR Nabisco, Inc. v. European Cmty.*; *Kiobel v. Royal Dutch Petroleum Co.*; *Morrison v. National Australian Bank Ltd.*; and *EEOC v. Arabian American Oil Co.*[268] Notably, each of these cases dealt with ascertaining the extraterritoriality of U.S. substantive law and proscribing *conduct* that was occurring outside the United States.[269] None of them dealt with the unique paradigm of a criminal investigation initiated domestically to prosecute conduct occurring in or affecting the United States, where an accompanying statute was merely a *procedural* tool to assist law enforcement. Indeed, Judge Lynch pointed out as much. The Second Circuit, however, never satisfactorily explained why this critical distinction was not important to its analysis. Rather, the Court's discussion of procedure was limited to explaining why the case law dealing with court-ordered subpoenas was inapposite.[270]

C. Practical and Policy Consequences

This paper does not suggest that the Second Circuit interpreted the SCA or Rule 41 incorrectly. Nor does it argue that the Second Circuit's holding is deleterious for the government. From the perspective of preserving governmental and cross-border collaboration, the decision endorses deference to other branches of government and sovereign states, if not out of obligation, then out of comity. But the decision also has undeniable commercial consequences that do not necessarily promote global privacy

---

substantive laws, but they are not required to apply state laws that are procedural or "arguably procedural."

268. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016); Kiobel v. Royal Dutch Petroleum Co., 133 S.Ct. 1659 (2013); Morrison v. National Australian Bank Ltd., 561 U.S. 247 (2010); EEOC v. Arabian American Oil Co., 499 U.S. 244 (1991).

269. *RJR Nabisco*, 136 S. Ct. 2090 (determining that RICO's provisions apply extraterritorially to members of the European Community who were harmed by racketeering activities that occurred across several continents); *Kiobel*, 133 S.Ct. 1659 (holding that the presumption against extraterritoriality could apply to claims brought under the Alien Tort Statute for crimes that were committed entirely overseas); *Morrison*, 561 U.S. 247 (holding that Section 10(b) of the Securities Exchange Act of 1934 does not apply extraterritorially for plaintiffs suing U.S. defendants for misconduct connected to securities traded on foreign exchanges); *Arabian American Oil Co.*, 499 U.S. 244 (finding that Title VII's protections do not extent to U.S. citizens employed by foreign employers abroad).

270. Microsoft Corp. v. United States, 829 F.3d 197, 218–19 (2d Cir. 2016), *cert. granted* 2017 WL 2869958 (Oct. 16, 2017).

and information-sharing at a time when data is an invaluable commodity.[271] For example, Judge Lynch pointed out that:

> [N]either privacy interests nor the needs of law enforcement vary on whether a private company chooses to store records here or abroad – particularly when the 'records' are electronic zeroes and ones that can be moved around the world in seconds, and will be so moved whenever it suits the convenience or commercial purposes of the company.[272]

His point gets at the fact that although businesses like Microsoft and Apple advertise to customers about how they arduously protect privacy,[273] the outcome of the case does not really bolster individual privacy rights in any meaningful way. What the outcome of the case does do is fragment the Internet by effectively providing that whichever country a server is located in will be the country whose privacy laws will apply to the data stored within that server. This means that companies will now have tremendous leeway to shape the scope of criminal investigations through their business decisions of which countries to set up servers in – and those countries may have more stringent or *lenient* privacy rights compared to the United States.

Thus, it is unsurprising that just a few months after the Second Circuit decision, the *New York Times* ran a story entitled *U.S. Tech Giants Are Investing Billions to Keep Data in Europe.*[274] It explained the very recent surge of investments that U.S. tech companies have made in Europe in order to build servers and dominate Europe's cloud computing market:

---

271. *The World's Most Valuable Resource is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

272. *Id.* at 224.

273. *See, e.g.*, Brad Smith, *Our Search Warrant Case: An Important Decision for People Everywhere*, MICROSOFT (July 14, 2016), http://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.0001vn2n3990oe13rxf24chyrr3ay; *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/; Mark Hachman, *Tim Cook: Apple 'Will Not Shrink' from Responsibility to Protect Customer Privacy*, MACWORLD (Mar. 21, 2016 10:33 A.M.), http://www.macworld.com/article/3046479/apple-phone/tim-cook-apple-will-not-shrink-from-responsibility-to-protect-customer-privacy.html.

274. Mark Scott, *U.S. Tech Giants Are Investing Billions to Keep Data in Europe*, N.Y. TIMES (Oct. 3, 2016), http://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html?_r=0.

> Amazon Web Services, the largest player, announced last week that it would soon open multiple data centers in France and Britain. Google, which already has sites in countries like Finland and Belgium, is expected to finish a new multimillion-dollar data complex in the Netherlands by the end of the year.
>
> And Microsoft, by some measures the second-largest cloud computing provider in Europe, said on Monday that it had spent $1 billion in the last 12 months to expand its offerings, taking its total investment in European-based cloud services to $3 billion since 2005.
>
> . . . .
>
> Apple . . . is spending almost $2 billion building two data centers in the region. The facilities, its first such centers in Europe, will open in Denmark and Ireland by early 2018.[275]

The article also described how a chief executive for Microsoft reported that the purpose behind such drastic expansion was to meet the data needs of European customers, who expect access to U.S. web-based services and compliance of those services with their more stringent privacy laws in the EU.[276] The article further described how the outcome of the *Microsoft* case has assisted the European Union, which has been "clamp[ing] down on the perceived misuse of people's digital information" and focusing on the importance of "local data sovereignty."[277]

Again, the outcome of the case, with the consequence of U.S. businesses profiting from customer growth in Europe is not a bad result in and of itself. But as discussed, "local data sovereignty" can be a dangerous thing. While this paper has discussed privacy law in the European Union at length, it is only a matter of time before technology companies will seek to expand their market share to other parts of the world, where privacy laws are less stringent than in the United States. And what is even more troubling than the fact that customers of each region will be subject to the data and privacy laws of that region is that this fragmentation diminishes the shared gains of the Internet itself and simultaneously impedes law enforcement's access to digital evidence.[278]

---

275. *Id.*

276. *Id.*

277. *Id.*

278. *See generally,* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003).

The Second Circuit was rightly concerned with the consequences of issuing a decision that could allow U.S. law enforcement unfettered access to digital files located all over the world vis-à-vis U.S. court-issued warrants. But an equally serious concern is the ability for potential criminals to now exploit the Second Circuit's warrant loophole. As Professor Orin Kerr tweeted immediately following the decision: "Want to stymie U.S. law enforcement? Store your data in the cloud fragmented over many locations outside the U.S."[279]

D. Cross-Referencing to Reconfigure Territoriality

The bulk of this paper explained the nature of privacy and data collection laws in the United States and the European Union. It also discussed key legislation and case law that shaped surveillance efforts in recent years. By going into the details of key cases, such as *Digital Rights Ireland*, *Maximillian Schrems*, and *Microsoft Corp. v. United States*, this paper also showed an area of the law where there is an opportunity for U.S. courts to engage in active cross-referencing, which can allow judges to take advantage of one another's insights when presented with novel dilemmas.

For people who have been following the trend of EU case law, neither the Second Circuit's decision nor the *New York Times* article reflecting the surge in European data center investments is surprising. Had the lower court judges been following these trends or actively cross-referencing EU cases, perhaps they would have come to a different result in the *Microsoft* litigation before the case reached the Second Circuit. It is interesting to note that many of the parties that filed amicus briefs in the *Microsoft* case were EU parties that litigated or had serious stakes in *Digital Rights Ireland* and *Maximillian Schrems*.

These cases provided valuable insight, beyond just showing the direction that supranational courts have taken when protecting privacy rights. They underscored that in the EU, privacy law is not governed by a regime analogous to the Fourth Amendment—rather, it is a fundamental right codified in the EU Charter and the European Convention on Human Rights.[280] Recall

---

279. Brian Jacobs, *The Microsoft Warrant Case: Unintended Consequences of the Second Circuit's Ruling*, FORBES (Aug. 2, 2016, 5:04 P.M.), http://www.forbes.com/sites/insider/2016/08/02/the-microsoft-warrant-case-unintended-consequences-of-the-second-circuits-ruling/#69a2b4bd1629.

280. Charter of Fundamental Rights, *supra* note 80, art. 8; European Convention on Human Rights, *supra* note 86, art 8.

also that in *Digital Rights Ireland* the ECJ monumentally struck down the Retention Directive, legislation that facilitated intelligence gathering. Importantly, it was struck for failing to meet the element of proportionality. Knowing that proportionality is the bulwark of EU privacy analysis—much like reasonability is at the crux of Fourth Amendment analysis—is incredibly useful not only for judges dealing with EU data transfers, but also for Congressmen enacting statutes that compell data collection from companies with EU customers.

Consider the unique insights about extraterritoriality that the U.S. courts could have gained from *Schrems*. There, the ECJ dealt with an Irish national who voluntarily signed up for a Facebook account and accepted a user agreement granting permission to Facebook to transfer all or some of his personal to the United States where it would undergo "processing" in accordance with U.S. laws.[281] Notwithstanding that he voluntary availed himself of a U.S. web-service with clear contractual terms, Mr. Schrems wanted to vindicate the full panoply of privacy rights afforded to him as an EU citizen even after his data was transferred to a sovereign nation with its own data processing laws. Recall too that ultimately the ECJ in *Schrems* actively cross-referenced the U.S.'s data processing laws and compared them to the EU.[282] After doing so, it determined that U.S. laws did not provide "adequate protection" by EU standards.[283] By affirming Mr. Schrems's fundamental right to privacy for data that was physically located in another country to which he was only connected by virtue of his Facebook account, the EU demonstrated that the Fundamental Rights protected by the EU Charter have extraterritorial reach.

One may wonder whether the Second Circuit referenced *Schrems* when deciding that the Fourth Amendment and Rule 41 could not apply extraterritorially even through EU privacy rights do apply extraterritorially. It seems unlikely as the Second Circuit focused on analyzing U.S. precedent and framing the matter as a domestic as opposed to an international legal issue. And although the Court's analysis there was helpful for domestic legislative interpretation, it was less so for issues involving conflicts of law, foreign sovereignty, and digital territoriality. When U.S. courts are tasked with defining what extraterritorial application of the law is

281. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627 ¶ 27.
282. *Id.* ¶ 28–48.
283. *Id.* ¶¶ 87–88.

in the modern age, they should look at how other regions—particularly those with whom disputes frequently arise—frame the same legal quandaries.

VI. CONCLUSION

As privacy disputes continue to ignite legal debate, gaining deeper understanding of foreign laws from reputable sources and learning how to compare foreign and domestic laws is critical for courts and litigants who will increasingly be required to possess a sophisticated understanding of modern legal issues. To that end, this paper endorses the use of cross-referencing because it will equip litigants and the courts with effective tools and insights that have already been formulated. It will help courts develop frameworks to apply in complex data disputes and other areas of the law that are being challenged by technology and globalism. Further, given the similar privacy regimes in the United States and the European Union, the uniquely technical nature of data, and the deep interdependency that all regions of the world have on one another—especially in combatting transnational crimes—it will enable nations to cooperate with one another in gathering and sharing data, while also respecting one another's core values.

As Justice Breyer repeatedly explains in his book, the main impetus for courts to engage in active cross-referencing is the synergistic results that it will necessarily achieve. Cross-referencing does more than just allow courts to be informed about foreign laws and reasoning. It does more than reduce the likelihood of offending foreign legal values and rights in an age that demands global cooperation. It does more than make litigants and judges global thinkers in a multi-dimensional world. Cross-referencing deconstructs the arbitrary divisions between sovereign states that are more similar than they are different. In doing so, it promotes: harmony between global citizens, cooperation between law enforcement authorities across nations, trust in the rule of law, and unity in a world that data is already making borderless.