American University Law Review

Volume 67 | Issue 3 Article 6

2018

Data Localization The Unintended Consequences Of Privacy Litigation

H Jacqueline Brehmer
American University Washington College of Law

Follow this and additional works at: http://digitalcommons.wcl.american.edu/aulr

 Part of the Computer Law Commons, and the Privacy Law Commons

Recommended Citation
Brehmer, H Jacqueline (2018) "Data Localization The Unintended Consequences Of Privacy Litigation," *American University Law Review*: Vol. 67 : Iss. 3 , Article 6.
Available at: http://digitalcommons.wcl.american.edu/aulr/vol67/iss3/6

This Comment is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

Data Localization The Unintended Consequences Of Privacy Litigation

Keywords
cybersecurity threats, data localization, data privacy, Electronic Communications Privacy Act, Microsoft Ireland

This comment is available in American University Law Review: http://digitalcommons.wcl.american.edu/aulr/vol67/iss3/6

NOTE

DATA LOCALIZATION: THE UNINTENDED CONSEQUENCES OF PRIVACY LITIGATION

H JACQUELINE BREHMER*

This Note addresses a key unintended consequence of recent data privacy litigation before the European Court of Justice and the U.S. Supreme Court. Two cases—Data Protection Commissioner v. Schrems *and* United States v. Microsoft Corp.—*contravene the principles upon which the internet was founded by removing legal and scalable mechanisms for cross-border data transfers. While these cases do not directly create data localization regimes, they highlight the irreconcilably different approaches to data privacy held by the United States and the European Union and eliminate valid options for transfer such that localization is the only remaining scalable solution. Data localization is not solely expensive for companies; it also puts user privacy and global enterprise security at risk by creating greater government access to data, expanding the attack surface for cybersecurity threats, and minimizing the efficacy of data security tools. Thus, while these cases may increase user trust and privacy in the short-term, they are likely to lead to data localization and have long-term effects on internet use and access worldwide.*

---

* Law Clerk, Debevoise & Plimpton LLP—Cybersecurity & Data Privacy; Articles Editor, *American University Law Review*, Volume 67; J.D. Candidate, May 2018, *American University Washington College of Law*; B.A., International Studies, *University of Washington, Seattle.* I would like to thank Elizabeth Beske, Jennifer Daskal, Luke Dembosky, Melanie Teplinsky, and Sean Zadig for their contributions to and support of this piece. I would also like to thank the hard-working staff at the *American University Law Review*, especially Annie Anderson, Laura Collins, and Jordan Helton, for their thoughtful feedback and support during the publication process. The views expressed herein are those of the author and do not necessarily reflect those of Debevoise & Plimpton LLP.

TABLE OF CONTENTS

Introduction 928
I. Background 931
A. Data Localization 932
B. EU and U.S. Approaches to Data Privacy 933
1. EU data privacy 934
2. U.S. data privacy 937
a. Challenged surveillance laws and programs 938
b. Electronic Communications Privacy Act (ECPA) 940
c. Redress mechanisms 941
II. Cross-Border Data Transfer Mechanisms 944
A. Commercial Data Transfers 944
B. Law Enforcement Access 950
III. Cases 951
A. *Schrems II* 952
B. *Microsoft Corp. v. United States* (*Microsoft Ireland*) 953
IV. The Unintended Consequences 956
A. Impact of Localization 956
1. The CJEU data privacy cases and data localization 957
2. *Microsoft Ireland* and data localization 959
B. Privacy Impact 960
C. Security Impact 964
Conclusion 968

INTRODUCTION

When litigation is used to create policy, it can have unintended consequences.[1] This is especially true in the data security and privacy sectors, where the law and technology are developing at different rates. Thus, when lawyers and judges do not fully consider the legal and

1. *See* Mary Mitchell & Dana A. Remus, *Interstitial Exclusivities After Association for Molecular Pathology*, 109 MICH. L. REV. FIRST IMPRESSIONS 34, 39 (2014) (commenting that "[i]mpact litigation can be an effective means of placing pressure on the other branches of government . . . , but courts are not as effective as the other branches of government at crafting and implementing long-term solutions that adequately account for costs and second order consequences").

practical repercussions of technology, they run the risk of undermining the successful advocates' original position. Nothing illustrates this risk more than the recent data privacy cases in the United States and European Union. Advocates in these cases brought their claims to defend privacy rights; however, their success before the European Court of Justice (CJEU)[2] and the Second Circuit will paradoxically have the opposite effect by negatively impacting global user privacy and enterprise cybersecurity.[3]

Two cases—*Data Protection Commissioner v. Schrems* (*Schrems II*)[4] before the CJEU and *United States v. Microsoft Corp.* (*Microsoft Ireland*)[5] before the U.S. Supreme Court—along with pending challenges to the EU-U.S. Privacy Shield, are forcing this issue. In the former case, the plaintiff, Mr. Schrems, is challenging the ability of U.S. companies to transfer EU user data from the European Union to the United States using Standard Contractual Clauses (SCCs), which are EU-issued contractual clauses that seek to establish safeguards for cross-border data transfers.[6] Mr. Schrems claims that such mechanisms fail to provide adequate safeguards for transfer.[7] Simultaneously, in *Microsoft Ireland*, Microsoft is arguing that the application of U.S. law to law enforcement's ability to compel user data stored abroad by American companies is an inappropriate extraterritorial extension of law

---

2. This Note uses the phrase "CJEU data privacy cases" to collectively refer to *Data Protection Commissioner v. Schrems* ("*Schrems I*") and *Data Protection Commissioner v. Schrems* ("*Schrems II*"). Data Prot. Comm'r v. Schrems (*Schrems II*) [2016] IEHC 414 (Hi. Ct.) (Ir.); Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), 2014 E.C.R. 6.

3. *See In re* Search of Info. Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., Case No. 16-mj-00757 (BAH), 2017 WL 3445634, at *27 (D.D.C. July 31, 2017) (commenting that "the *Microsoft* decision may incentivize states to pass data localization laws to restrict their nationals from locating customer data abroad"); Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015) ("Data localization increases the ability of governments to *surveil* and even oppress their own populations . . . . By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe.").

4. [2016] IEHC 414 (Hi. Ct.) (Ir.).

5. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467–68 (S.D.N.Y. 2014), *rev'd*, 829 F.3d 197 (2d Cir. 2016), *petition for cert. granted sub nom.* United States v. Microsoft Corp., No. 17-2 (U.S. Oct. 16, 2017).

6. Complaint against Facebook Ireland Ltd from Maximilian Schrems, to Data Prot. Comm'r at 10 (Dec. 1, 2015), https://www.scribd.com/document/292096534/Complaint-against-Facebook-Ireland-Ltd.

7. *Id.*

enforcement powers.[8] Though the former argument restrains commercial transfers of user data and the latter limits law enforcement access to data, they both ultimately impede cross-border data transfers such that data localization is the sole scalable legal and business solution available to U.S. companies.

While these cases do not directly cause the implementation of data localization laws or regulations, they do highlight the irreconcilable differences between the EU and U.S. approaches to data privacy. Unfortunately, these differences ultimately boil down to key aspects of the U.S. legal system, such as Article III standing.[9] Thus, if the CJEU and the U.S. Supreme Court find for the original plaintiffs, the United States will be forced to either walk back foundational aspects of the U.S. legal system or put U.S. corporations in a position where they must localize data.[10]

Data localization is not new, and governments normally implement localization through restrictive laws and regulations that bar the movement of data in and out of a country.[11] Such laws are generally criticized for being expensive for corporations and protectionist.[12] Unfortunately, the costs are not only financial.[13] Localization will also negatively impact user privacy and enterprise security worldwide by creating greater government access to user data,[14] minimizing the efficacy of corporate privacy and security controls, and expanding the

---

8. Brief for Appellant at 1–2, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 14-2985-cv), 2014 WL 7004807, at *1–2.

9. *See* Affidavit of Stephen I. Vladeck ¶¶ 80–95, *Schrems II* [2016] IEHC 414 (Hi. Ct.) (Ir.).

10. This Note recognizes that there are other alternatives for data transfers to the United States besides Privacy Shield and SCCs; however, these bases, such as consent, are highly fact-specific, specialized, and may be subject to disclosure requirements. Additionally, the legal diversity and complexity of these options likely make them out of reach for many companies.

11. UNITED NATIONS CONFERENCE ON TRADE & DEV., DATA PROTECTION REGULATION AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT 13 (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

12. *Id.* at 4.

13. *See infra* Sections V.B–C.

14. This Note uses "user data" to describe a wide range of data that is collected and processed by commercial entities and law enforcement. This includes: (1) non-content information, such as personal identifying information or subscriber information (e.g., username, registration IP address, or date of birth); (2) transactional information, such IP address logs or billing records; and (3) content information, such as production of emails or a wiretaps. H. MARSHALL JARRETT ET AL., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 121–24 (2009) https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

corporate network.[15] The CJEU's data privacy and *Microsoft Ireland* cases facilitate localization by highlighting the unamenable differences between EU and U.S. approaches to privacy and by assigning a territorial identity to data. Thus, while these cases may provide an appearance of greater protection, they place user privacy and security at greater risk of exposure to good and bad actors alike.

This Note explores data localization as a key unintended consequence of the CJEU's data privacy cases and the Second Circuit's *Microsoft Ireland* case. It argues that these cases will undermine user privacy and global enterprise security by restricting the movement of data across borders and forcing corporations to localize by invalidating key data transfer mechanisms. Part I first outlines the concept of data localization and then details EU and U.S. data privacy laws and the various mechanisms for transfer from the European Union to the United States. This Part also discusses the EU and U.S. perspectives on standing and notes that this irreconcilable difference could undermine cross-border data transfers between the European Union and United States. Part II discusses the legal mechanisms used for data transfers by commercial entities and law enforcement. Part III analyzes two pending cases—*Schrems II* and *Microsoft Ireland*—and how these cases affect the validity of data transfer mechanisms.

Part IV addresses how these cases erect barriers to the movement of data and remove key mechanisms for data transfer. This Part also discusses how localization undermines user privacy and security by providing governments with greater access to user data and limiting the efficacy of data security tools. Finally, Part V concludes by asking the CJEU and U.S. Supreme Court to rule in favor of greater security and privacy.

I. BACKGROUND

If the courts in *Schrems II* and *Microsoft Ireland* hold for the plaintiffs, data localization will be a practical rather than legal consequence. To reach this conclusion, it is necessary to understand how the United States and the European Union conceptualize and implement data privacy protections, including an analysis of key U.S. surveillance

15. *See infra* Sections V.B–C (explaining that localization benefits foreign governments at the cost of user privacy by limiting the ability of companies to shift data across national borders when the political climate changes); *see also* Stephen Northcutt, *Security Laboratory: Defense in Depth Series*, SANS TECH. INSTIT. (last visited Feb. 7, 2018) https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface (defining attack surface as "our exposure, the reachable and exploitable vulnerabilities that we have").

programs and redress mechanisms available when a privacy violation has occurred. Ultimately, the validity of EU-U.S. cross-border data transfers turns on whether the transfers from the European Union are conducted pursuant to a privacy regime commensurate with, but not necessarily identical to, those provided in the European Union. The U.S. system is unlikely to meet the EU standard because the United States and European Union have such fundamentally different approaches to privacy law that it is unlikely the European Union would deem the U.S. system adequate. Consequently, because transfers are no longer an option, localizing data will become the norm, rather than the exception.

A. Data Localization

Generally, countries maintain three primary justifications for implementing data localization regulations. First, some countries view localization as critical to protecting their respective citizens from U.S. surveillance.[16] Second, others justify localization because it benefits their domestic law enforcement by increasing the accessibility of user data through local legal processes.[17] Third, data localization also has a protectionist motive, and countries have used it as means to bolster domestic markets.[18]

Despite these purported benefits, data localization has several negative consequences. One particularly worrisome consequence is the direct financial burden placed on companies and consumers.[19] In 2013, data localization was predicted to cost cloud computing services

---

16. *See* Chander & Lê, *supra* note 3, at 713–14 (explaining that the propensity to pass data localization laws may have stemmed from the 2013 leak of classified U.S. surveillance documents by National Security Agency (NSA) employee Edward Snowden).

17. *See* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 478 (2016) (explaining that "[s]uch laws also facilitate domestic surveillance"); *infra* Section II.B (discussing the structure and issues with the current mutual legal assistance treaty (MLAT) process).

18. *See* Chander & Lê, *supra* note 3, at 714 (noting that data localization hinders global markets in favor of local markets by barring foreign services access across borders and inviting reciprocal treatment in return).

19. *Id.* at 699, 723–24. This cost is derived from many expenses including, but not limited to, building data centers, employing new teams, and complying with local regulations. *Id.* In response to this, some companies have begun pre-emptively expanding their global footprint. *See, e.g.*, Tony Kontzer, *IBM Spends $1.2 Billion on New Cloud Data Centers*, NETWORK COMPUTING (Jan. 23, 2014, 12:48 PM) (describing IBM's investment in data centers world-wide to satisfy growing localization requirements); Nick Wingfield & Mark Scott, *Microsoft Suggests Wider Options for Foreign Data*, N.Y. TIMES (Jan. 23, 2014, 5:00 PM) (commenting on Microsoft's potential plans for expansion in response to new data localization laws).

between $21.5 billion and $35 billion by 2016.[20] The majority of this high cost stems from the development and staffing of necessary technical infrastructure essential for compliance with data localization requirements, which can amount to upwards of $60.9 million.[21]

Further, a long-term financial impact study of data localization in seven major countries concluded that recently proposed or implemented data localization legislation substantially impacted the gross domestic products of all seven countries studied, finding welfare losses of $63 billion in China and $193 billion in the European Union.[22] The report also suggested that while localization will increase costs for U.S. companies, consumers worldwide will actually pay the price as companies shift the cost of localization onto consumers.[23] Despite the known financial costs of data localization, several countries have still legislated and implemented these regimes. Though the United States and European Union have generally permitted the free and open flow of information, the trend towards data localization reflects each nation's approach to data privacy.

B. EU and U.S. Approaches to Data Privacy

The United States' and European Union's different perspectives on privacy turn on the recognition of privacy either as an aspect of individual dignity or as a function of individual liberty.[24] In Europe,

---

20. *See* DANIEL CASTRO, HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 1 (2013), http://www2.itif.org/2013-cloud-computing-costs.pdf (noting this figure is limited to the cost of cloud computing service providers).

21. *See* Anupam Chander & Uyên P. Lê, *Breaking the Web: Data Localization v. the Global Internet* 36–37 (U.C. Davis Legal Studies Res. Paper No. 378), https://ssrn.com/abstract=2407858 (breaking down the construction and maintenance costs of foreign data centers); Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill*, WALL ST. J. (Nov. 13, 2013, 6:45 PM), https://www.wsj.com/articles/brazil-legislators-bear-down-on-internet-bill-1384384450 (explaining that data localization "could cost U.S. companies tens of billions of dollars").

22. *See* Matthias Bauer et al., THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY 2 (2014) (arguing that unilateral data restrictions create larger economic losses).

23. *Id.*; *see also* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 753 (2016) (clarifying that internet companies have to increase user fees or reduce services because of the high costs brought about by localization requirements).

24. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004) ("Continental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*. The core continental privacy rights are *rights to one's image, name, and reputation* . . . . By contrast, America . . . is much more oriented toward values of liberty, and especially liberty against the state. At its

privacy is considered a part of the individual's dignity, and citizens have the "right to be shielded against unwanted public exposure."[25] As such, the right to privacy, and more specifically the right to privacy in communications, is enshrined in the EU Charter of Fundamental Rights.[26] Conversely, the U.S. approach to privacy derives from the concept of liberty and hinges on the idea that citizens should be free from state intrusion.[27] Consequently, U.S. privacy protections were originally derived from the Fourth Amendment but have developed in U.S. jurisprudence within the penumbras of the First, Third, Fourth, and Fifth Amendments.

These theoretical differences are reflected in substantive distinctions in EU and U.S. data privacy laws and regulations.[28] As described below, the European Union uses a comprehensive approach with broad, overarching data protection laws that expands across various sectors, applies extraterritorially, and protects individuals located in the European Union regardless of citizenship.[29] Unlike the European Union, the United States employs a sectoral approach, consisting of different laws and regulations for each commercial sector.[30] This seemingly inconsequential distinction is at the basis of the data privacy disputes before the CJEU.

1. EU data privacy

The EU Data Protection Directive (Directive) is the foundation of the European data privacy regulation.[31] Adopted in 1995, the Directive

---

conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home.").

25. *Id.*

26. *See id.* at 1153; *see also* Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1 [hereinafter Charter of Rights].

27. *See* Whitman, *supra* note 24, at 1161.

28. *Id.*

29. *EU General Data Protection Regulation*, EPIC (last visited Feb. 7, 2018), https://epic.org/international/eu_general_data_protection_reg.html (describing the multiple key points of the General Data Protection Regulation (GDPR) that collectively make it a comprehensive data regulation regime).

30. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 505–06 (1995) (addressing the American anti-comprehensive model sentiment and analyzing the U.S. privacy law by sector).

31. 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. 25, 1995 O.J. (L 281) 31 [hereinafter

comprehensively details the data rights of EU citizens, outlines the obligations of governments and corporations with respect to those rights, and requires that all data transfers maintain adequate safeguards to protect the personal information of EU individuals.[32] The Directive is being replaced in May 2018 by the General Data Protection Regulation (GDPR).[33] In terms of data transfer provisions, the GDPR expands and clarifies the mechanisms and requirements for data transfer from the European Union to third-party countries.[34] However, the change in laws from the Directive to the GDPR is unlikely to have any impact on the admissibility of the claims in *Schrems II* and *Microsoft Ireland* because the underlying issues in question are so fundamental to rights guaranteed under the EU Charter.

The principles for cross-border data transfers are laid out in Articles 25 and 26 of the Directive.[35] Article 25 requires that transfers of personal data from the European Union to a third-party country ensure an adequate level of protection.[36] This determination depends on the country's domestic laws, the nature of the data transferred, and

---

Directive]; Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 617–18 (2013).

32. *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 2 (2016), https://fas.org/sgp/crs/misc/R44257.pdf.

33. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L. 119) 1 [hereinafter GDPR]. The GDPR is a comprehensive data privacy regime that implements several new and aggressive requirements for the handling of EU resident data. Detlev Gabel & Tim Hickman, *Cross-Border Data Transfers—Unlocking the EU General Data Protection Regulation*, *in* UNLOCKING THE EU GENERAL DATA PROTECTION REGULATION: A PRACTICAL HANDBOOK ON THE EU'S NEW DATA PROTECTION LAW (2017), https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection. The more notable changes from the Directive to the GDPR include: increased fines for non-compliance of up to 4% of global turnover, express territorial application, and the right to be forgotten. *Id.* With some exceptions, the provisions on transfer remain largely the same. *Id.* The provisions governing cross-border data transfers are reflected in Articles 44 through 50, which primarily clarifies the different methodologies of transfer. *Id.*

34. *See* Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 640–41 (2013).

35. *See* Directive, *supra* note 31, art. 25–26. Under the GDPR, data transfer provisions are located in articles 44 through 50. GDPR, arts. 44–50.

36. *Id.* art. 25.

the purpose of the transfer.[37] Even if a third-party country's domestic laws do not ensure sufficient safeguards, a country can still meet the requisite standard based upon international commitments negotiated between the third-party country and the European Commission.[38] Notably, the Directive does not require identical laws but instead requires that the third-party country employ domestic laws or maintain international obligations that create protections "essentially equivalent" to those provided to EU citizens.[39] The Directive empowers the European Commission to render an adequacy decision[40] determining whether the domestic law of the third-party state "ensures an adequate level of protection . . . for the protection of private lives and basic freedoms and rights of individuals."[41]

If Article 25 is not met, the Directive prohibits personal data transfers from the EU to a third-party country unless the country meets one of the exceptions listed under Article 26;[42] the exceptions fall into three categories. First, Article 26 provides six derogations for transfer where it is completed pursuant to the data subject's consent, is necessary for the performance of a contract, required on grounds of public importance, or legally required.[43] These derogations are fact-based and are to be interpreted strictly.[44] Second, an EU member state may authorize transfer to a country where the data controller "adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals."[45] If the member state decides to grant such permission to a third-party country, the state

37. *Id.* art. 25(2).

38. *Id.* art. 25(4)–(6). The European Commission is the Executive of the European Union and is responsible for developing and implementing EU strategies. *Organisational Structure*, EURO. COMMISSION, https://ec.europa.eu/info/about-european-commission/organisational-structure_en (last visited Feb. 7, 2018).

39. Case C-362/14, *Schrems I*, 2014 E.C.R. 6, ¶ 73.

40. An adequacy decision is a finding of "whether a third country ensures an adequate level of protection by reason of its domestic law or the of the international commitments it has entered into." *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EURO. COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited Feb. 7, 2018) [hereinafter *Commission Decisions*].

41. Directive, *supra* note 31, art. 25.

42. *Id.* recital 57.

43. *Id.* art. 26, ¶ 1.

44. Case C-119/12, Probst v. mr.nexnet GmbH, ¶ 23 (Nov. 22, 2012), http://curia.europa.eu/juris/liste.jsf?num=C-119/12&language=EN#.

45. Directive, *supra* note 31, art. 26, ¶ 2.

must inform the Commission and other member states.[46] Third, transfers may also be conducted pursuant to contractual clauses referred to as SCCs. The European Commission approves these clauses and they are integrated into data transfer agreements between EU and U.S. data controllers.[47]

Additionally, the Directive and GDPR provide two important clauses regarding law enforcement access to user data. First, both the Directive and GDPR allow for member states to adopt laws and regulations restricting rights and obligations when such restriction is necessary for national security, defense, or public safety.[48] This exception allows for the member states to change how data is collected, processed, and transferred whenever the member state is able to justify such behavior for national security purposes.[49] Second, the GDPR changes the methodology for U.S. law enforcement to access user data stored in EU nations by requiring that production of user data be requested pursuant to an international agreement, such as a Mutual Legal Assistance Treaty (MLAT).[50] When the data is controlled by an EU entity, this reflects the standard process that U.S. law enforcement must comply with to obtain EU user data. However, this raises questions as to whether the GDPR is memorializing the Second Circuit's decision in *Microsoft Ireland*, discussed in Section III.B, such that the Supreme Court's holding in that case will be rendered irrelevant.

2. U.S. data privacy

The United States takes a different approach to data privacy laws and regulations. Whereas the European Union employs a comprehensive approach, the United States uses a sectoral approach, consisting of different laws and regulations per commercial sector.[51] This approach

46. *Id.* art. 26, ¶ 3.

47. SCCs are also often referred to as Model Contract Clauses (MCCs). *Model Contracts for the Transfer of Personal Data to Third Countries*, EURO. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (last visited Feb. 7, 2018) [hereinafter *Model Contracts*].

48. Directive, *supra* note 31, art. 13; GDPR, *supra* note 33, art. 23.

49. *See* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems, 18 German L.J. 881, 895–99 (2017).

50. GDPR, *supra* note 33, art. 48.

51. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 505–06 (1995) (addressing the American anti-comprehensive model sentiment and analyzing the U.S. privacy law by sector).

has resulted in fragmented privacy protections and regulations.[52] Thus, when assessing the adequacy of U.S. privacy protections, it is critical to review U.S. law holistically because different protections and remedies derive from different areas.[53] Key to the cases described below in Sections IV.A and IV.B are a myriad of surveillance laws and the Electronic Communications Privacy Act (ECPA).

a. Challenged surveillance laws and programs

In June 2013, former National Security Agency (NSA) contractor Edward Snowden leaked thousands of documents from the agency and exposed section 702 of the Foreign Intelligence Surveillance Act (FISA), which allowed the NSA to target, for intelligence purposes, the communications of non-U.S. citizens reasonably believed to be outside of the United States.[54]

FISA was enacted by Congress in 1975 "to curb the problem of unchecked domestic surveillance and intelligence-gathering abuses undertaken by the executive branch in the post-World War II era."[55] Since passing the law, Congress has amended it several times, most recently through the FISA Amendment Act of 2008 (FAA). The FAA was "designed to provide wholesale authorization for a particular kind of warrantless electronic surveillance that had become . . . unduly cumbersome to pursue on a case-by-case, warrant-driven basis."[56] Mr. Snowden's leaks exposed section 702 of FISA,[57] which, though requiring

52. *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended at 15 U.S.C. § 6801 (2012)) (creating an "affirmative and continuing obligation" for financial institutions "to respect the privacy of its customers and protect the security and confidentiality of those customers' nonpublic information"); The Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 112-278, 126 Stat. 2480 (codified as amended at 20 U.S.C. § 1232g (2012)) (providing a framework to protect the privacy of student records); Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012) (regulating the interception and collection of consumer by private corporations and law enforcement); Health Information Privacy and Accountability Act (HIPAA) 45 C.F.R. § 164.502 (2017) (creating general rules for the use and disclosure of patient health information health care providers).

53. Written Legal Submission on Behalf of the United States of America as Amicus Curiae at 3, *Schrems II*, [2016] IEHC 414 (Hi. Ct.) (Ir.) (No. 4809P), https://www.justice.gov/civil/page/file/947821/download.

54. *Id.*

55. Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090, 1104 (N.D. Cal. 2013).

56. Affidavit of Stephen I. Vladeck, *supra* note 9, ¶ 38.

57. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE

annual certifications authorizing collection of foreign intelligence information, does not require the U.S. government to make a probable cause showing that the target is a foreign agent prior to collection.[58]

Under section 702, the NSA may conduct what is known as PRISM collection.[59] In PRISM collection, the U.S. government sends selectors, such as an e-mail address, to a U.S. electronic communications service provider, such as Google or Yahoo, and compels the service provider to share this information.[60] The NSA may receive all data collected through PRISM, and the Central Intelligence Agency or Federal Bureau of Investigation (FBI) may receive a select portion of the collection.[61] Each agency has minimization procedures limiting how the agency can search and analyze collected data, how long it can be maintained, and how it is to be destroyed.[62] The procedure is also subject to extensive oversight by the Department of Justice (DOJ), the Office of the Director of National Intelligence, and the FISA court.[63]

Following Snowden's revelations of this and other collection programs, the U.S. government took several steps to reform its surveillance programs. President Obama commissioned a review group to provide recommendations to balance U.S. national security with its foreign policy interests and its commitment to privacy and civil liberties.[64] Based on those recommendations, the Obama administration released Presidential Policy Directive 28 ("PPD-28"), which expands surveillance collection principles usually applied to U.S. citizens to foreign nationals.[65] PPD-28 limits the situations in

---

SURVEILLANCE ACT 6 (2014) [hereinafter SURVEILLANCE REPORT], https://www.pclob.gov/library/702-Report.pdf.

58. *Id.*

59. *Id.* Mr. Snowden leaked information of the PRISM collection program in addition to a number of other surveillance pertaining to both U.S. and non-U.S. citizens, including upstream collection, collection of bulk telephony metadata, and surveillance of foreign government leaders. *Snowden Revelations*, LAWFARE, https://www.lawfareblog.com/snowden-revelations (last visited Feb. 7, 2018) (providing a timeline of Edward Snowden's disclosure of NSA classified information).

60. SURVEILLANCE REPORT, *supra* note 57, at 7.

61. *Id.*

62. *Id.*

63. *Id.* at 8.

64. RICHARD A. CLARK ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY 1 (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

65. Directive on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 1 (Jan. 17, 2014).

which bulk collection of information may be conducted and outlines minimization, retention, and dissemination restrictions on the U.S. intelligence community.[66]

b. Electronic Communications Privacy Act (ECPA)

Under the ECPA, U.S. law enforcement is also able to access domestic and foreign user data, including the content of communications.[67] Title II of the ECPA is known as the Stored Communications Act (SCA), and it governs the disclosure of user data, content, and non-content to law enforcement.[68] Section 2703 details the requirements for disclosure of user information using search warrants, subpoenas, or § 2703(d) court orders.[69] While the SCA initially allowed law enforcement to obtain user content via a subpoena if the data had been stored for over 180 days, it is widely recognized that law enforcement is required to obtain a warrant to compel user content.

Two relevant aspects of the SCA are user notice and the use of national security letters ("NSLs"). The SCA, which requires that notice of the law enforcement request be provided to the user at some point, permits courts to issue an order barring service providers from notifying the user of the law enforcement request.[70] Often these orders are frequently renewed or forgotten about such that they become permanent and the user is never notified.[71] Additionally, the ECPA also expands law enforcement's use of NSLs, which allow the FBI to compel

66. *Id.*; *see* Affidavit of Stephen I. Vladeck, *supra* note 9, ¶¶ 62–64.

67. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012).

68. Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). Content is generally considered to include information, such as e-mail messages, while non-content information includes transactional or subscriber information. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) 5 (2015), https://fas.org/sgp/crs/misc/R44036.pdf. Transactional information generally includes more detailed logging information or email headers. *Id.* Subscriber information may include subscriber name, address, phone number, length of service, or means of payment. *Id.*

69. 18 U.S.C. § 2703 (2012).

70. A 2703(d) order is a combination between a warrant and a subpoena that allows law enforcement to obtain transactional information, such as user sign-in logs, but not email content. THOMPSON & COLE, *supra* note 68, at 5.

71. 18 U.S.C. § 2705. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 325–26 (2012).

records from third-party service providers.[72] NSLs are accompanied by an indefinite gag order[73] and prohibit the receiving party from disclosing the existence of the NSL unless certain requirements are met.[74]

c. Redress mechanisms

The final and arguably most important change to U.S. privacy and surveillance law following the Snowden revelations is the ability of foreign nationals to seek redress within U.S. domestic courts for alleged privacy violations caused by U.S. surveillance.[75] This ability highlights basic legal differences in the U.S. and EU legal systems. While these differences include concepts such as remedies[76] and sovereign immunity,[77] the most critical distinction is standing.[78] Though the European Union does not require that the protections afforded to EU residents in the United States be identical to the European Union's, it does require that the protections be commensurate.[79] This requirement creates a problem because the differing attitudes toward standing may lead the European Union to find that U.S. protections are insufficient.[80]

---

72. Law enforcement may use four distinct statutes to obtain information from providers. ECPA (electronic communication service providers); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified at 12 U.S.C. §§ 3401–3422) (financial institutions); National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (codified as amended 50 U.S.C. § 3001–3234) (government institutions); Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 111-2 (codified as amended at 15 U.S.C. § 1681).

73. CHARLES DOYLE, CONG. RESEARCH SERV., RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND 9 (2015), https://fas.org/sgp/crs/intel/RL33320.pdf.

74. 18 U.S.C. § 2709(c).

75. Draft Decision of the Data Protection Commissioner ¶ 62, *Schrems II*, [2016] IEHC 414 (Hi. Ct.) (Ir.) (No. 4809P) [hereinafter DPC Draft Decision] (emphasizing the lack of redress mechanisms in the United States as a key reason for finding SCCs invalid).

76. *See id.* ¶ 51; Affidavit of Stephen I. Vladeck, *supra* note 9, ¶ 88; *see also* Fed. Aviation Admin. v. Cooper, 566 U.S. 284, 298 (2012) (finding that under the Privacy Act the plaintiff must show pecuniary harm and is limited to damages of $1000 for violations of the Act).

77. *See* DPC Draft Decision, *supra* note 75, ¶¶ 47, 59; Affidavit of Peter Swire, at 7-4, *Schrems II*, [2016] IEHC 414 (Hi. Ct.) (Ir.) (No. 4809P), https://iapp.org/media/pdf/resource_center/Schrems-testimony-Swire.pdf; Affidavit of Stephen I. Vladeck, *supra* note 9, ¶ 84–85.

78. *See* DPC Draft Decision, *supra* note 75, ¶ 52.

79. EUROPEAN COMM'N, GUIDE TO THE EU-U.S. PRIVACY SHIELD 11 (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.

80. *Id.* at 13.

The primary civil redress mechanism available to U.S. citizens is the Privacy Act, which allows plaintiffs to challenge the validity of federal agency data collection, prohibits government disclosure to third parties, and requires agencies to be transparent about leveraged collection systems.[81] The Judicial Redress Act of 2015 (JRA) expanded these protections to foreign nationals.[82] While the JRA creates a legal cause of action, a key challenge that each foreign plaintiff will face is standing.[83] U.S. case law has interpreted standing to require that plaintiffs show (1) an injury-in-fact that is concrete and particularized, and actual or imminent; (2) that there is a causal connection between the injury and the alleged conduct; and (3) that the injury will be redressed by the court's decision.[84] Thus, a party that is unable to make this showing, whether a U.S. citizen or foreign national, will be precluded from seeking relief.

Two cases—*Clapper v. Amnesty International*[85] and *Spokeo v. Robins*[86]—are key to analyzing the ability of foreign nationals to bring claims. In *Clapper*, respondents sought a declaratory judgment that foreign collection under FISA was unconstitutional and requested injunction against such collection.[87] The Supreme Court rejected the respondents' claim that there was an objective likelihood of harm and instead found that the respondents could not show that surveillance of their communications was actual or imminent.[88] Additionally, the Court also rejected the respondents' claim that the organizations must have standing to challenge the constitutionality of surveillance programs because otherwise surveillance would be insulated from meaningful judicial review.[89] *Clapper* thus raises questions of how a

81. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (to be codified at 5 U.S.C. § 552a).

82. Judicial Redress Act of 2015, Pub. L. 114-126, 130 Stat. 282 (to be codified at 5 U.S.C. § 552a note). Outside of the JRA, foreign nationals may seek redress under the Administrative Procedure Act (APA), Privacy Shield, Foreign Intelligence Surveillance Act (FISA), or ECPA. *See* Affidavit of Peter Swire, *supra* note 77, at 1-20–1-24.

83. *See* DPC Draft Decision, *supra* note 75, ¶ 52; Irish High Court Referral to European Court of Justice ¶ 222, *Schrems II*, [2016] IEHC 414 (Hi. Ct.) (Ir.) (No. 4809P) [hereinafter ECJ Referral], https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf.

84. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

85. 568 U.S. 398 (2013).

86. 136 S. Ct. 1540 (2016).

87. *Clapper*, 568 U.S. at 401.

88. *Id.* at 422.

89. *Id.* at 420–21.

party is able to challenge U.S. surveillance when plaintiffs do not know whether they have been surveilled.[90]

A corollary case to *Clapper* is *Spokeo v. Robins*, in which the respondent alleged that a website operator published inaccurate information about him in violation of the Fair Credit Reporting Act.[91] The Supreme Court found that even when there is an alleged violation of a statutory right, the plaintiff still has the burden of showing the elements of Article III standing.[92] In this case, Mr. Robins merely alleged a procedural violation but did not adequately show a sufficiently concrete injury.[93] Thus, a party solely alleging the violation of a statutory right without a showing of tangible, actual, and imminent harm is precluded from seeking redress in U.S. courts.[94]

European courts have taken a different approach to standing when it comes to alleged violations of the EU Charter. EU residents need not allege "an adverse consequence" resulting from an interference with certain articles within the Charter "to secure redress of a violation" of the Charter.[95] In the context of surveillance, the European Court of Human Rights has also found that EU residents can challenge surveillance programs, despite their covert nature, because to preclude such a challenge would allow surveillance to remain "unchallengeable."[96] The European standard for accessing the courts is thus lower than in American courts. While some have suggested that U.S. courts have lowered the bar for standing in the United States due to data breach litigation[97] or that the bar may be easier for foreign

90. Timothy Egar, *Standing, Grandstanding and NSA Surveillance*, LAWFARE (Oct. 21, 2015, 12:22 PM), https://www.lawfareblog.com/standing-grandstanding-and-nsa-surveillance.

91. *Spokeo*, 136 S. Ct. at 1544.

92. *Id.* at 1549.

93. *Id.* at 1550 (commenting that "[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm").

94. *Id.*

95. *See* DPC Draft Decision, *supra* note 75, ¶ 54.

96. Klass v. Germany, App. No. 5028/71, 2 Eur. Comm'n H.R. Rep. 214, ¶¶ 30–38 (1978) (finding that an individual may "claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him").

97. Professors Vladeck and Swire, among others, have also suggested that the recent pull-back in standing requirements for data breach litigation indicates that the ruling in *Clapper* is not a *per se* ban on cases involving U.S. foreign intelligence. *See* Affidavit of Stephen I. Vladeck, *supra* note 9, ¶¶ 89–98; Affidavit of Peter Swire, *supra* note 76, at 7-38.

nationals in the context of foreign surveillance,[98] EU officials have still expressed concerns regarding the availability of redress mechanisms because of the standing requirement.[99]

II. CROSS-BORDER DATA TRANSFER MECHANISMS

The law governing cross-border data transfers can be divided into two groups: (1) commercial transfers and (2) law enforcement transfers. As noted, the validity of a commercial transfer from the European Union to the United States is dependent upon the adequacy of the safeguards surrounding the transfer. In the case of EU-U.S. commercial data transfers, this adequacy was first challenged in *Data Protection Commissioner v. Schrems* (*Schrems I*).[100] In contrast, law enforcement access to user information stored in foreign jurisdictions is governed by MLATs. Ultimately, it is the failure of both of these mechanisms to ensure safe, effective, and efficient transfer of user information that will ultimately cause de facto localization.

A. Commercial Data Transfers

To date only ten countries have received an adequacy decision from the European Commission based upon the country's domestic laws.[101] Unsurprisingly, the United States is not one of these countries. Thus, U.S. companies processing EU users' personal information must transfer data under an international commitment to use adequate safeguards, contractual clauses, or one of the derogations listed in Article 26 of the Directive.

Prior to the *Schrems I* decision, U.S. entities under the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT)[102] could transfer EU user data to and from the

---

98. Timothy Edgar, *More on Standing as a Barrier to Surveillance Challenges: Bug or Feature?*, LAWFARE (Oct. 28, 2015, 4:14 PM), https://www.lawfareblog.com/more-standing-barrier-surveillance-challenges-bug-or-feature.

99. *See* DPC Draft Decision, *supra* note 75, ¶ 54; *see also* ECJ Referral, *supra* note 83, ¶ 222.

100. Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), 2014 E.C.R. 6.

101. *See Commission Decisions*, *supra* note 40 (listing Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, and New Zealand as nations that provide adequate safeguards for personal data).

102. Generally, the FTC has jurisdiction over "acts or practices in or affecting commerce by any 'person, partnership, or corporation.'" Int'l Trade Admin., U.S. Dep't of Commerce, *How to Join Privacy Shield Part I*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 (last visited Feb. 7, 2018) [hereinafter *How to Join Privacy Shield*]. However, this is limited, and the FTC does not have jurisdiction "over most depository institutions . . . ,

European Union under the Safe Harbor Framework. Adopted in 2000, the Safe Harbor Framework was a direct response to the passage of the Directive and was designed to limit the negative impact of the inherent differences between the EU and U.S. approaches to privacy, international trade, and investment.[103] The Safe Harbor Framework is an example of an Article 25 international commitment, negotiated by EU-U.S. officials, whereby the United States ensures that the transfers are conducted with an adequate level of protection.[104] These protections are reflected in the Safe Harbor Framework principles, which mirrored key concepts in the Directive, such as notice, choice, and security.[105] U.S. companies processing EU user data were then able to certify compliance with the principles and transfer data under the Framework.

In 2014, Maximillian Schrems, an Austrian privacy advocate, filed a case before the Irish Data Protection Agency (DPA) against Facebook's Irish subsidiary arguing that, under EU legal standards, U.S. law failed to provide adequate protections against U.S. mass surveillance.[106] Mr. Schrems's claim was a direct response to the Snowden revelations,[107] and he argued that Facebook's alleged cooperation with the NSA's PRISM program and involvement in continued mass surveillance was a breach of the principles reflected in the Data Protection Acts of 1988 and 2003[108] and the conditions of the Safe Harbor Decision.[109]

---

telecommunications and interstate transportation common carrier activities, air carriers, labor associations, most non-profit organizations, and most packer and stockyard activities." *Id.* The DOT has jurisdiction over U.S. and foreign air carriers. *Id.*

103. *See* WEISS & ARCHICK, *supra* note 32, at 5.

104. Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 390–91 (2011).

105. *Id.* at 391.

106. *See* Written Observations of Applicant ¶¶ 21–23, Case C-362/14, *Schrems I*, 2014 E.C.R. 6, [hereinafter Written Observations] http://www.europe-v-facebook.org/CJEU_subs.pdf.

107. *See* Outline Written Submissions at 2–3, Case C-362/14, *Schrems I*, 2014 E.C.R. 6 (claiming that in "light of the then recent revelations of . . . Edward Snowden and admissions by USA authorities that the so-called 'PRISM' program existed, it was clear that, despite the 'self-certification' by Facebook Inc. under the Safe Harbour system an 'adequate protection' was factually not provided").

108. The Data Protection Acts of 1988 and 2003 are two pieces of Irish implementing legislation that give effect to the Directive. DATA PROT. COMM'R, DATA PROTECTION ACTS 1988 AND 2003: INFORMATION CONSOLIDATION 3 (2009), https://www.dataprotection.ie/documents/legal/DPAConsolMay09.pdf.

109. Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215), 25/08/2000 p. 0007-00047.

After losing in the lower court,[110] Mr. Schrems appealed this decision to the Irish High Court of Judicial Review, which found that Mr. Snowden's revelations were credible and that, once personal data was transferred to the United States, the NSA and FBI were able to access the personal information through mass and indiscriminate surveillance and collection of data.[111] While the High Court recognized this behavior as a violation of Irish constitutional and data protection law, it also recognized that the issue ultimately involved the interpretation and application of EU law and thus referred the case to the CJEU.[112]

In analyzing Mr. Schrems's claim, the CJEU reviewed the Safe Harbor Framework holistically and in conjunction with the Directive. It determined that U.S. laws did not provide an adequate level of protection essentially equivalent to EU laws because the U.S. government permitted generalized access to electronic information and failed to provide redress mechanisms.[113] Ultimately, the CJEU struck down the Safe Harbor as a valid mechanism for transfers from the European Union to the United States.[114]

Following the invalidation of the Framework in *Schrems I*, the decision had several impacts on EU-U.S. relations. The immediate consequence of the CJEU's decision was that all data transfers from the United States to the European Union under the Safe Harbor regime were now in violation of the Directive.[115] However, the Directive still allowed companies to use SCCs or other derogations (e.g., consent) as an alternative transfer mechanisms.[116]

Companies were able to use these alternatives until the European Union and United States successfully negotiated the Privacy Shield.[117]

---

110. Written Observations, *supra* note 106, ¶ 1 (explaining that existing safe harbor laws protect data transferred from the EU to the United States).

111. Opinion of Advocate General Bot ¶ 36, Case C-362/14, *Schrems I*, 2014 E.C.R. 6.

112. *Id.* ¶ 40.

113. *Schrems I*, 2014 E.C.R. ¶¶ 81–82, 93, 95; Charter of Rights, *supra* note 26, art. 7.

114. McCann Fitzgerald, *Commercial Court Affirms Legal Principles on Admission of an Amicus Curiae*, LEXOLOGY (Aug. 3, 2016), https://www.lexology.com/library/detail.aspx?g=8be84b34-c0b7-4a66-9542-fdde0db0e269.

115. *See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of American Under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, at 4 COM (2015) 566 final (Nov. 6, 2015).

116. *Id.*

117. *See supra* notes 49–101.

Known as the EU-U.S. Privacy Shield,[118] this agreement sought to remedy the problems illuminated in *Schrems I* and allow individual companies to self-certify their commitment to the Privacy Shield Principles.[119] Similar to the Safe Harbor Framework, the Privacy Shield requires that certified parties implement and maintain adequate safeguards for transfer.[120] These requirements are outlined in the Privacy Shield Principles and include concepts such as notice, choice, accountability for onward transfer, security, data integrity, purpose limitation, access, recourse, enforcement, and liability.[121]

The Privacy Shield also specifically sought to address gaps noted in *Schrems I* by requiring specific measures for the maintenance of data transfers and storage, providing access to dispute resolution mechanisms, and ensuring accountability of data providers.[122] More specifically, the Privacy Shield requires strict user notice requirements, provides user data access rights, and extends guarantees under the Privacy Act to EU citizens.[123] The Privacy Shield also created five redress mechanisms, which have since been implemented in the

---

118. *See* INT'L TRADE ADMIN., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE 1, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg (last visited Feb. 7, 2018) (discussing the general principles of Privacy Shield).

119. Int'l Trade Admin., U.S. Dep't of Commerce, *Privacy Shield Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Feb. 7, 2018).

120. *Id.*

121. Int'l Trade Admin., U.S. Dep't of Commerce, *Requirements of Participation*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Requirements-of-Participation (last visited Feb. 7, 2018).

122. *See* Int'l Trade Admin., U.S. Dep't of Commerce, *Key New Requirements: EU-U.S. Privacy Shield Framework Key New Requirements for Participating Companies*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Key-New-Requirements (last visited Feb. 7, 2018).

123. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (to be codified at 5 U.S.C. § 552a) (stating that "[i]t shall be unlawful for any Federal, State[,] or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number"); SHARA MONTELEONE & LAURA PUCCIO, EURO. PARLIAMENTARY RESEARCH SERV., PE 595.892, FROM SAFE HARBOUR TO PRIVACY SHIELD: ADVANCES AND SHORTCOMINGS TO THE NEW EU-US DATA TRANSFER RULES 23–24 (2017) (clarifying that Privacy Shield "transforms this principle into a fully-fledged right of data subjects"); *Privacy Shield: Impact of Trump's Executive Order*, HUNTON & WILLIAMS (Jan. 28, 2017), https://www.huntonprivacyblog.com/2017/01/28/privacy-shield-impact-of-trumps-executive-order.

United States through the JRA.[124] From a national security perspective, as a part of the Privacy Shield negotiations, the United States also declassified minimization procedures under section 702 of FISA[125] and expanded the privacy protections in the PPD-28 to better align American practice with European expectations.[126]

On July 12, 2016, the European Commission issued its adequacy decision regarding the Privacy Shield, finding that the new framework ensured an adequate level of protection for data transfers.[127] While this decision was well received by U.S. and EU businesses, the Privacy Shield has been widely criticized,[128] with EU commentators calling into question the long-term validity of the agreement.[129]

Finally, as a part of the EU-U.S. negotiations, the European Union and the United States also agreed that the Privacy Shield would

---

124. *See* Sheila Miller & Tracy P. Marshall, *Obama Signs Judicial Redress Act—Will It Move EU-U.S. Privacy Shield Forward?*, NAT'L LAW REV. (Feb. 27, 2016) https://www.natlawreview.com/article/obama-signs-judicial-redress-act-will-it-move-eu-us-privacy-shield-forward (noting that the redress mechanisms allow EU citizens to seek redress remedies from the federal government in U.S. courts for alleged privacy violations); *see also* Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (to be codified at 5 U.S.C. § 552a note).

125. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1782 (to be codified at 50 U.S.C. §§ 1801–1885); *see Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, ODNI (last visited Feb. 7, 2018) https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf (discussing the declassification procedures).

126. *See* Directive on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 1 (Jan. 17, 2014).

127. *See* Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of Protection Provided by the EU-U.S. Privacy Shield, art. 1, ¶ 13, C (2016) 4176 final, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf ("Based on the findings developed in recitals (136)–(140), the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.").

128. *See, e.g.*, Jan Philipp Albrecht, *EU-US Privacy Shield: EU Commission Signs Blank Cheque for Data Transfers*, EURO. FREE ALLIANCE (July 12, 2016 https://www.greens-efa.eu/en/article/press/eu-us-privacy-shield (arguing that the Privacy Shield does not address the concerns outlined in the CJEU Safe Harbor decisions); Jedidiah Bradley, *Model Clauses in Jeopardy with Irish DPA Referral to CJEU*, IAPP (May 25, 2016), https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu (commenting on the Article 29 Working Group's criticisms and the inability of an Article 31 group to reach an agreement on the Privacy Shield).

129. *See* MONTELEONE & PUCCIO, *supra* note 123, at 31–32.

undergo an annual review to ensure that it continues to meet adequacy standards.[130] If, through a review, the Commission finds that the Privacy Shield fails to maintain adequate protections, the Commission can use the review as the basis to re-negotiate parts or all of the Privacy Shield.[131] The first review of the Privacy Shield was conducted in September 2017; while all parts of the Privacy Shield were upheld,[132] the Commission commented that there was still room for improvement.[133]

Since the EU Commission's adequacy determination for the Privacy Shield was rendered, its validity has been challenged twice. Digital Rights Ireland[134] brought the first challenge on September 16, 2016, in EU General Court seeking the annulment of the determination on the basis that the Shield failed to provide sufficient substantive changes from the Safe Harbor Framework.[135] This challenge was dismissed on November 22, 2017, for lack of admissibility.[136] However, a French advocacy group, La Quadrature du Net,[137] has also challenged the Commission's decision and is arguing that the Shield not only continues to violate the Charter, but also fails to provide effective

130. Letter from Ken Hyatt, Deputy Under Sec'y for Int'l Trade, Int'l Trade Admin., to Vera Jourová, Comm'r for Justice, Consumers and Gender Equal., European Comm'n (July 7, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v (agreeing to a joint review mechanism as a part of the Privacy Shield's implementation).

131. Tom De Cordier et al., *EU-US Privacy Shield Under High Scrutiny*, LEXOLOGY (Sept. 14, 2017), https://www.lexology.com/library/detail.aspx?g=a7550caf-cfa2-4717-b266-c7dc3c5a9f15.

132. EUROPEAN COMM'N, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FIRST ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD 4 (Oct. 18, 2017), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0611&from=EN.

133. Press Release, European Comm'n, EU-U.S. Privacy Shield: First Review Shows It Works but Implementation Can Be Improved (Oct. 18, 2017), http://europa.eu/rapid/press-release_IP-17-3966_en.htm.

134. Digital Rights Ireland is a non-profit organization dedicated to "[c]ivil, [h]uman and [l]egal rights in a digital age." *About Digital Rights Ireland*, DIGITAL RIGHTS IR, https://www.digitalrights.ie/about (last visited Feb. 7, 2018). The organization actively files constitutional challenges against the Irish government in relation to internet and telephone regulations and policies. *Id.*

135. Action Brought on 16 September 2016—Digital Rights Ir. v. Comm'n (Case T-670/16,), ¶ 8, 2016 O.J. (C 410) 26, 27, http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2016.410.01.0026.01.ENG.

136. Case T-670/16, Digital Rights Ir. v. Comm'r, ¶¶ 45–54 (Nov. 22, 2017), http://curia.europa.eu/juris/document/document.jsf?text=&docid=197141&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=30038.

137. *Who Are We?*, LA QUADRATURE DU NET, https://www.laquadrature.net/en/who-are-we (last visited Feb. 7, 2018).

redress mechanisms.[138] While this case is in its infant stages, it will likely work its way up to the CJEU, and the outcomes of *Schrems II* and *Microsoft Ireland* will certainly impact the CJEU's decision.

While the Privacy Shield provides a mechanism for companies to certify use of adequate safeguards, the Shield only applies to companies under the FTC's or DOT's jurisdiction.[139] Companies not falling under this jurisdiction have generally relied upon SCCs, which provide an adequate basis for transfer under Article 26(2) of the Directive.[140] The European Commission has rendered two sets of clauses adequate, and entities are able to insert these clauses verbatim into their data transfer contracts.[141] However, in *Schrems II*, discussed below in Section IV.A, Mr. Schrems is challenging the adequacy of these clauses.[142]

B. Law Enforcement Access

U.S. local, state, and federal law enforcement entities are able to compel user data maintained in foreign jurisdictions using the MLAT process.[143] MLATs are bilateral and regional treaties governing both U.S. law enforcement's acquisition of user data from foreign jurisdictions and vice-versa.[144] These treaties provide a mechanism for U.S. law enforcement to obtain personal data of foreign individuals held under a foreign jurisdiction's law.[145]

To obtain records via the MLAT process, a domestic prosecutor, whether in the United States or abroad, must first ensure that the request meets local warrant or subpoena standards.[146] Thus, when

---

138. Case T-738/16, Action Brought on 25 October 2016—La Quadrature du Net and Others v. Comm'n (Case T-738/16), ¶ 1–2, 2017 O.J. (C 6) 39, 39, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016TN0738.

139. *How to Join Privacy Shield*, *supra* note 102.

140. *Model Contracts*, *supra* note 47.

141. *Top Ten—EU Data Transfers: Comparing the Proposed Privacy Shield to the Standard Contractual Clauses*, ASS'N OF CORP. COUNSEL (May 24, 2016), http://www.acc.com/legalresources/publications/topten/transferring-personal-data.cfm.

142. *See infra* Section II.B.

143. Virginia M. Kendall & T. Markus Funk, *The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence*, LITIG., Winter 2014, at 59, 60 (2014) (describing MLATs as a "well-worn tool in the prosecutor's toolbox").

144. ANDREW K. WOODS, GLOB. NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE 3 (2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

145. *See id.* (describing a hypothetical where Indian law enforcement officials seek to obtain email records from a U.S. company and use the MLATs to retrieve the data).

146. Yonatan L. Moskowitz, *MLATS and the Trusted Nation Club: The Proper Cost of Membership*, 41 YALE J. INT'L L. ONLINE 1, 3 (2016).

seeking to serve a warrant on the foreign jurisdiction, a U.S. prosecutor must first meet domestic probable cause standards and obtain a warrant before sending the request to the foreign jurisdiction.[147] When foreign entities seek user data held in the United States, foreign requests for user data must first make a probable cause showing and comply with the terms of the relevant MLAT and the ECPA.[148] Whether the request meets these standards is determined by the DOJ's Office of International Affairs, the relevant DOJ field office and district court in the company's jurisdiction, and by the company itself.[149]

While this process ensures constitutional protections for user data in the jurisdiction in which it is maintained, it also creates extensive delays.[150] Requests from the United States to access data held in a foreign jurisdiction, regardless of the type of legal process, can take anywhere from six weeks to ten months or longer.[151] Thus, many critics have argued that the MLAT system is archaic, inefficient, and needs substantial reform.[152]

III. CASES

At the time of writing, two relevant cases are pending before the CJEU and U.S. Supreme Court. In these cases, parties are challenging cross-border data transfers on the basis of privacy concerns and the alleged scope of law enforcement access to data.

---

147. *Id.*

148. *See Foreign Government Access to User Data*, KATE WESTMORELAND, http://www.katewestmoreland.com/new-page-1 (last visited Feb. 7, 2018) (explaining the full process of MLAT requests).

149. MARK A. RUSH & JARED A. KEPHART, K & L GATES, LIFTING THE VEIL ON THE MLAT PROCESS: A GUIDE TO UNDERSTANDING AND RESPONDING TO MLA REQUESTS 4 (2017), http://www.klgates.com/files/Publication/669681d7-12d7-451e-8240-a33cf67c959f/Presentation/PublicationAttachment/ec5fc22d-3e3c-4607-bcb3-f4e99e3f59b4/GE_Alert_01202017.pdf.

150. *Id.* at 8.

151. *See* Mailyn Fidler, *MLAT Reforms: Some Thoughts from Civil Society*, LAWFARE (Sept. 11, 2015, 12:22 PM), https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society (noting that the process is designed to protect rights, but this results in delays that incentivize countries to find faster ways of accessing data).

152. *See id.* (arguing that other countries have difficulty complying with the U.S. standard for MLATs and that the three main issues with such requests are lack of protection for metadata requests, the time delay of processing, and the reduction in the amount of data shared through the response process).

A. Schrems II

After *Schrems I*, Mr. Schrems filed a second complaint with the Irish DPA challenging the validity of the SCCs.[153] Referred to as "*Schrems II*," the case claims that the SCCs do not adequately protect data transfers to the United States because such data can still be surveilled by U.S. intelligence authorities.[154]

Procedurally, this case is unusual.[155] Following Mr. Schrems's application, the Irish Data Protection Commission commenced an investigation into the adequacy standards of U.S. laws under the Directive.[156] To assist in the investigation, the Commissioner sought the opinions from independent experts.[157] The Commissioner determined that while remedies for redress may be available to EU residents, such remedies were fragmented. Additionally, because the SCCs were not binding on U.S. law enforcement, there was no guarantee that they would actually be able to protect EU user data from unbridled law enforcement access.[158] Ultimately, the Commissioner concluded that while she questioned the validity of the clauses under the EU Charter, she was unable to render a final decision until the Irish High Court or the CJEU rendered a decision on the validity of the clauses.[159]

The Irish High Court took up the case and reviewed the Commissioner's draft decision. Ultimately, the High Court concurred with the Commissioner's finding regarding the validity of the SCCs.[160] The High Court, however, also found itself in a jurisdictional bind because a dismissal of the case would be tacit approval of the SCCs.[161] On October 3, 2017, the Irish High Court formally referred *Schrems II* to the CJEU for a preliminary ruling on the validity of the SCCs.[162] While there is no timeline for the completion of this case, given that eighty-eight

153. *See Schrems II*, [2016] IEHC 414, ¶ 2 (Hi. Ct.) (Ir.); *see also* Jedidiah Bracy, *Model Clauses in Jeopardy with Irish DPA Referral to CJEU*, IAPP (May 25, 2016), https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu.

154. *Schrems II*, [2016] IEHC 414, ¶ 3.

155. *See* Judgment of Justice Costello, *Schrems II* [2016] No. 4809 P. (Hi. Ct.) (Ir.).

156. *Id.* ¶¶ 2–3.

157. DPC Draft Decision, *supra* note 75, ¶ 42.

158. *Id.* ¶ 61.

159. *Id.* ¶ 63.

160. ECJ Referral, *supra* note 83, ¶ 333.

161. *Id.* ¶¶ 333–34.

162. *Id.* ¶ 5; *see* Commission Decision 2011/497/EC of June 2001, 2001 O.J. (L 181) 19; Commission Decision 2004/915/EC of 27 December 2004, 2004 O.J. (L 385) 74; Commission Decision 2010/87/EU of 5 February 2010, 2010 O.J. (L 39) 5.

percent of companies use SCCs to transfer personal data from the European Union to the United States, this case will be heavily watched.[163]

B. Microsoft Corp. v. United States *(*Microsoft Ireland*)*

The final case impacting cross-border data transfers of user data is the *Microsoft Ireland* case, now before the U.S. Supreme Court.[164] In this case, U.S. law enforcement sought to compel the production of two Microsoft email accounts.[165] While the warrants were properly served upon Microsoft in Washington, the data sought was stored in Microsoft's data center[166] in Dublin, Ireland.[167] Microsoft filed a motion to quash, arguing that the SCA did not authorize federal courts to compel the production of data stored outside of the United States.[168] The Southern District of New York rejected this argument, and Microsoft promptly appealed.[169]

The Second Circuit reversed and held that an SCA warrant could not compel data stored in a foreign jurisdiction.[170] Using basic statutory analysis, the Second Circuit determined that the primary focus of the SCA is the privacy of stored communications, and thus,[171] courts should apply the law of the jurisdiction where the invasion of

---

163. Lee Matheson, *Understanding "Schrems 2.0,"* IAPP (Oct. 3, 2017), https://iapp.org/news/a/understanding-schrems-2-0.

164. Andrew Keane Woods, *A Primer on Microsoft Ireland, the Supreme Court's Extraterritorial Warrant Case*, LAWFARE (Oct. 16, 2017), https://www.lawfareblog.com/primer-microsoft-ireland-supreme-courts-extraterritorial-warrant-case.

165. *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467–68 (S.D.N.Y. 2014) (stating that Microsoft "move[d] to quash a search warrant to the extent that it direct[ed] Microsoft to produce the contents of one of its customer's e-mails where that information is stored on a server located in Dublin, Ireland"), *rev'd*, 829 F.3d 197 (2d Cir. 2016), *petition for cert. granted sub nom.* United States v. Microsoft Corp., No. 17-2 (U.S. Oct. 16, 2017).

166. A data center is a location where computer servers, containing any form of computerized information, are kept. *How a Data Center Works*, SAP, http://www.sapdatacenter.com/article/data_center_functionality (last visited Feb. 7, 2018). A corporation may have a server room or use a data center, depending upon the size of the company and the number of servers in the enterprise. *Id.* Key characteristics of data centers include redundant power supplies, cooling systems, and controlled access. *Id.*

167. *Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d at 468.

168. *Id.* at 470.

169. *Id.* at 476.

170. *Id.* at 222.

171. *Id.* at 216–17.

privacy occurred.[172] According to the Second Circuit, because the actual intrusion into the user's privacy occurred in the Irish data center, the court ruled that Irish law would apply instead of the SCA.[173] Consequently, U.S. law enforcement must obtain a MLAT to the foreign jurisdiction in order to obtain user data held by U.S. companies abroad.[174]

Since the Second Circuit's holding, nine magistrate and district court judges across the United States have considered and rejected the Second Circuit's conclusion.[175] In these cases, the courts found that the SCA did not apply extraterritorially and that the invasion of the user's privacy occurred in the United States, where the disclosure of the information occurred, rather than in the foreign jurisdiction.[176]

In response to the Second Circuit's decision, the U.S. Solicitor General filed a petition for writ of certiorari in the Supreme Court.[177]

---

172. *Id.* at 217–20 (determining the focus of the SCA after reviewing the plain text, procedural provisions, and legislative history of the statute).

173. *Id.* at 220.

174. *Id.*

175. *See In re* Search Warrant Issued to Google, Inc., No. 5:17-mj-532-HNJ, 2017 WL 4022806, at *9 (N.D. Ala. Sept. 1, 2017); *In re* Search Warrant No. 16-960-M-1 to Google, No. 16-960, 2017 WL 3535037, at *6, 11 (E.D. Pa. Aug. 17, 2017); *In re* Search of Content Stored at Premises Controlled by Google, Inc., No. 16-mc-80263-RS, 2017 WL 3478809, at *2, 5 (N.D. Cal. Aug. 14, 2017); *In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *1, 27 (D.D.C. July 31, 2017); *In re* Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, No. 2:16-mj-02197-DUTY-1, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 2017); *In re* Search Warrant to Google, Inc., No 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *3–4 (E.D. Wis. June 30, 2017); *In re* Search of Premises Located at [redacted]@yahoo.com, No. 6:17-mj-1238 (M.D. Fla. Apr. 7, 2017), slip op. 3; *In re* Info. Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo, No. 17-M-1234, 2017 WL 706307, at *2–3 (E.D. Wis. Feb. 21, 2017).

176. *Search Warrant Issued to Google, Inc.*, No. 5:17-mj-532-HNJ, 2017 WL 4022806, at *3, 9; *Search Warrant No. 16-960-M-1 to Google*, No. 16-960, 2017 WL 3535037, at *10; *Search of Content Stored at Premises Controlled by Google, Inc.*, No. 16-mc-80263-RS, 2017 WL 3478809, at *5; *Search of Info. Associated with [redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-00757 (BAH), 2017 WL 3445634, at *5, 25; *Search Warrant to Google, Inc.*, No 16-4116, 2017 WL 2985391, at *9, 11; *Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156, at *4; *Search of Info. Associated with Accounts Identified as [redacted]@gmail.com*, No. 2:16-mj-02197-DUTY-1, 2017 WL 3263351, at *8–9; *Info. Associated with One Yahoo Email Address that Is Stored at Premises Controlled by Yahoo*, No. 17-M-1234, 2017 WL 706307, at *3.

177. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d. Cir. 2016), *petition for cert. granted sub nom.* United States v. Microsoft Corp., No. 17-2 (U.S. Oct. 16, 2017).

Similar to the lower courts, the Solicitor General argued that the Second Circuit's logic is incorrect because the focus of the SCA is on the disclosure by the company, not the privacy of the stored communications.[178] Thus, according to the Solicitor General, the court should have used the law of the jurisdiction where the company disclosed the communication to U.S. law enforcement, rather than the law where the privacy violation occurred.[179]

On October 16, 2017, the Supreme Court granted certiorari for this case.[180] While commentators tend to believe that the Court will side with the U.S. government, there are troubling implications for either side's success.[181] If the Court sides with Microsoft, law enforcement will be required to use MLATs to compel data held by U.S. companies in foreign jurisdictions.[182] Alternatively, a decision for the U.S. government may undermine the success of U.S. interests in *Schrems II* because the U.S. government will be applying U.S. law to EU residents rather than EU law, thus increasing the optics that U.S. law enforcement has unrestrained access to EU user data.[183]

Whereas the CJEU data privacy cases limit the cross-border movement of user data for commercial purposes, the *Microsoft Ireland* case could limit law enforcement access to user data held by U.S. corporations in foreign jurisdictions. However, the cases are linked in two key ways. First, for a company to comply with a domestic court order for data held in a

178. *Id.* at 12.

179. *Id.* at 14.

180. United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (mem.) (granting certiorari).

181. Jennifer Daskal, *There's No Good Decision in the Next Big Data Privacy Case*, N.Y. TIMES (Oct. 18, 2017), https://www.nytimes.com/2017/10/18/opinion/data-abroad-privacy-court.html (outlining the immediate consequences of the Court's decision).

182. *See* Press Release, Sen. Orrin Hatch, Second Circuit Ruling Gives Data Privacy Bill Momentum in Congress (July 14, 2016), https://www.hatch.senate.gov/public/index.cfm/2016/7/second-circuit-ruling-gives-data-privacy-bill-momentum-in-congress (praising the Second Circuit decision because it will encourage the use of MLATs in obtaining information stored abroad).

183. *See* Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Party at 1–4, United States v. Microsoft, 138 S. Ct. 356 (2017) (mem.) (No. 17-2), 2017 WL 6383224, at *14 [hereinafter Brief of the European Commission] (describing the European Union's interest in the case and the relevant EU laws relevant to the Court's decision); Lee Matheson, *European Commission Weighs in on Microsoft Ireland Case*, IAPP (Dec. 17, 2017), https://iapp.org/news/a/european-commission-weighs-in-on-microsoft-ireland-case (commenting that while the EU amici appear not to support either side before the Supreme Court, there is a strong implication that the European Union would like the Supreme Court to force U.S. law enforcement to rely upon the existing MLAT system).

foreign jurisdiction, the company must transfer the data from the foreign jurisdiction to the United States in order to disclose the information to U.S. law enforcement. If the data is stored in the European Union, this transfer automatically implicates either the use of the Privacy Shield, SCCs, or other tools for transfers. Second, because the *Microsoft Ireland* case also impacts the scope of law enforcement's access to user data, the decision will be considered in the CJEU's decision in *Schrems II* and other challenges to the Privacy Shield.[184]

IV. THE UNINTENDED CONSEQUENCES

A holding for Mr. Schrems and Microsoft in *Schrems II* and *Microsoft Ireland*, respectively, and a successful challenge to the Privacy Shield will ultimately require companies to localize data to ensure compliance with de facto localization regimes. This localization will ultimately undermine user data privacy and security by removing Fourth Amendment protections from user data and limiting the ability of companies to effectively implement scalable security tools.

A. Impact of Localization

If the respective high courts affirm *Schrems II* and *Microsoft Ireland*, those decisions will advance data localization in two ways: (1) by removing legal cross-border data transfer mechanisms for commercial data transfers and (2) by assigning territoriality to data for law enforcement purposes. On their own, the CJEU cases facilitate localization by highlighting the fundamental differences in EU and U.S. approaches to privacy by explicitly calling the U.S. approach inadequate—not once, but twice. Further, because the SCCs and Privacy Shield are based on the same adequacy standard, the invalidation of the SCCs would also bolster any challenge to the Privacy Shield and make it very difficult for the CJEU to uphold the latter framework. Thus, despite the changes made by the United States following the invalidation of the Safe Harbor regime, a further invalidation of the SCCs and the Privacy Shield would suggest that the privacy differences between the United States and the European Union are irreconcilable. The *Microsoft Ireland* case furthers the trend toward data localization by ensuring that the law of the territory where

184. Brief of the European Commission, *supra* note 183, at *14 (noting that under the GDPR, compliance with a foreign court order does not make the transfer lawful).

data is held controls law enforcement access to this data.[185] For practical purposes, U.S. companies must retain data in one country once the data is created because each cross-border transfer would require a new MLAT.[186] While the cases individually restrict the flow of data across borders, taken together, the cases effectively erect territorial boundaries and limit the ability of companies and law enforcement agencies to move and access data.

1. The CJEU data privacy cases and data localization

If the CJEU finds that the SCCs and the Privacy Shield are invalid, the United States has two options: (1) legislate greater privacy protections to meet EU standards or (2) localize data.[187] Given the extent of the changes already made, it seems unlikely that Congress would legislate in favor of greater privacy protections.[188] As a part of the EU-U.S. Privacy Shield negotiations, the United States revised numerous laws and implemented various protections to increase the privacy protections for EU citizens' data.[189] Additionally, as reflected in the Irish Data Protection Commissioner's draft decision in

185. *See supra* notes 165–72 and accompanying text (discussing how the court in the *Microsoft Ireland* case found that the place where the intrusion of privacy occurred is the jurisdiction that should control the matter, so American law enforcement must follow the appropriate jurisdiction's laws to obtain user information held by U.S. companies operating overseas).

186. *See* Jennifer Daskal, *The Microsoft Warrant Case: The Policy Issues*, JUST SECURITY (Sept. 8, 2015, 12:48 PM), https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues (commenting on the unstable nature of data, which makes it difficult for law enforcement to obtain it from any party outside of the United States).

187. *See* EUROPEAN COMM'N, ARTICLE 29 WORKING PARTY STATEMENT ON THE DECISION OF THE EUROPEAN COMMISSION ON THE EU-U.S. PRIVACY SHIELD 1 (2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (criticizing the Privacy Shield for not providing stricter guarantees); *see also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1149 (4th ed. 2011) (commenting on the compromises made by the European Union in drafting the Safe Harbor Agreement because of a recognition that the United States would not pass comprehensive privacy laws).

188. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 151, 178, 173 (1998) (explaining that it is clear to Europeans that the United States will not pass comprehensive data privacy laws); *see also* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 737–38 (2001) (arguing that the Directive will create a bifurcated system of privacy in the United States, where EU citizens are provided with greater privacy than American citizens under U.S. law).

189. *See supra* notes 122–26 and accompanying text.

Schrems II,[190] several issues of contention turn on key constitutional differences, such as Article III standing.[191] While the Commissioner may have misinterpreted some of these doctrines,[192] by targeting these long-standing principles of U.S. jurisprudence, the European Union has given the United States an ultimatum to either adjust basic tenants of U.S. law or refrain from transferring data. It is thus questionable whether the United States is able to give anything more at the negotiating table without overturning decades of legal precedents.

Additionally, from a national security perspective, any further U.S. concessions would subject the United States to greater restrictions than its EU counterparts.[193] For example, following *Schrems I*, the United States amended FISA, declassified the minimization procedures of § 702, and expanded the limitations principles of PPD-28 to non-U.S. citizens, limiting both the practice and appearance of unrestrained government access to user information and content.[194] These protections are commensurate or exceed those provided by the European Union's Directive and GDPR, which allow member states to adopt legislation restricting the scope of privacy rights when necessary to protect national security.[195] However, because it is unlikely that the United States can or will make any further changes to its laws that will satisfy EU authorities, including the European Commission and member state

---

190. Following Mr. Schrems's initial complaint, the Data Protection Commissioner launched an investigation into the allegations. The results of this investigation were circulated in a draft with the parties. *See* McCann FitzGerald, *Commercial Court Affirms Legal Principles on Admission of an Amicus Curiae*, LEXOLOGY (Aug. 3, 2016), https://www.lexology.com/library/detail.aspx?g=8be84b34-c0b7-4a66-9542-fdde0db0e269.

191. *Id.* ¶¶ 56, 79, 84 (stating how some U.S. companies have gotten around Fourth Amendment issues through exceptions to the warrant clause, such as the foreign intelligence surveillance exception and the third-party doctrine).

192. *Id.* ¶ 79.

193. *See* Christopher Wolf & Winston Maxwell, *Why the U.S. Is Held to a Higher Data Protection Standard than France*, IAPP (Nov. 2, 2015), https://iapp.org/news/a/why-the-u-s-is-held-to-a-higher-data-protection-standard-than-france (discussing how the French Patriot Act would fail the adequacy test applied to U.S. laws in *Schrems*); Timothy Edgar, *Schrems v. Data Protection Commissioner: Some Inconvenient Truths the European Court of Justice Ignores*, LAWFARE (Oct. 6, 2015, 8:08 PM), https://www.lawfareblog.com/schrems-v-data-protection-commissioner-some-inconvenient-truths-european-court-justice-ignores (arguing that the European Union should review the surveillance laws of its own member states before passing judgment on the laws of others).

194. *See supra* notes 122–26 and accompanying text.

195. *See* Kuner, *supra* note 49, at 896–97.

governments, companies will likely be forced to localize data because there is simply no longer a valid scalable mechanism for transfer.[196]

2. Microsoft Ireland *and data localization*

Although the CJEU data privacy cases impact the movement of user data for commercial purposes, *Microsoft Ireland* restricts the movement of user data for law enforcement purposes. By finding that the privacy violation occurs at the data center rather than from where disclosure occurs, the Second Circuit's decision links data to the territory where the data is held.[197] This decision creates practical problems for U.S. law enforcement seeking to access data through valid legal processes and incentivizes foreign governments to implement localization regimes. First, the holding requires U.S. law enforcement to obtain an MLAT prior to getting data from U.S. entities storing data abroad, and each MLAT is specific to a country.[198] That means that if a company transfers the data across borders prior to the execution of the MLAT,[199] the MLAT is no longer valid and law enforcement must comply with an entirely new set of laws. Practically, this gap allows companies to continually move data across borders in real time and effectively evade compliance by consistently pointing law enforcement to an alternative jurisdiction. Thus, if the data does not stop moving across jurisdictions,

196. *Id.* at 917–18 (noting that the United States wants the European Union "to make it easier to transfer personal data internationally . . . . This has produced resentment in the EU about the extent of US lobbying on data protection, and in the US about pressure from the EU to change its law").

197. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 390 (2015) (discussing the conflict in the case that "pits the location for data against the location of access, requiring an answer as to which controls").

198. *See supra* Section II.B.

199. *See* ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW LAW ENFORCEMENT SHOULD ACCESS DATA ACROSS BORDERS 13 (2017), http://www2.itif.org/2017-law-enforcement-data-borders.pdf?_ga=2.185940128.821711203.1515263369-2004149087.1515263369 (noting how modern data storage often causes data to be split amongst multiple locations, so using the physical location in which data is stored to determine access forces law enforcement to initiate a separate MLAT request to view the data in each physical location); Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE (May 22, 2017, 7:00 AM), https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization (suggesting that since it is practically impossible for users to know where their data is stored, it will also be extremely difficult for law enforcement to know where necessary data is located such that an MLAT could be served).

law enforcement will be significantly hindered from acquiring data essential to criminal and national security investigations.[200]

Second, because the foreign jurisdiction's law now controls law enforcement's access to the information, countries may be incentivized to formalize the Second Circuit's ruling by mandating that data be held within territorial boundaries of the state. This would allow the foreign state to not only centralize the information but also change the laws and standards regulating access.[201] Thus, because the Second Circuit's holding elevates the position of foreign law and puts the foreign government in greater control of law enforcement's ability to access data within its territorial borders, the *Microsoft Ireland* holding provides a platform on which foreign governments can build more restrictive data localization laws and regulations.

B. Privacy Impact

Data localization undermines user privacy by granting foreign governments greater access to user data, limiting the ability of U.S. companies to defend fundamental rights abroad, and monopolizing the competitive market for privacy controls. Confining data within a territorial jurisdiction brings information directly under the control of a government such that the government can arbitrarily change the rules of access.[202] Then, because of the foreign government's access, corporations have less ability to protect users globally.[203] Data localization also reduces the market power of user choice by reducing the number of companies in any one particular market.[204] Thus, there are several ways that localization benefits foreign governments at the cost of user privacy.

---

200. MCQUINN & CASTRO, *supra* note 199, at 13 (explaining that if a company wanted to impede investigation of data, it could continue splitting the data into hundreds of pieces, "creating a labyrinthine environment for law enforcement agencies" trying to get data).

201. *See infra* note 202 and accompanying text (noting how limiting data geographically allows local governments to control the regulation of the data).

202. *See* Chander & Lê, *supra* note 3, at 735 (commenting that "[t]he end result of data localization is to bring information increasingly under the control of the local authorities, regardless of whether that was originally intended").

203. *See* Daskal, *supra* note 17, at 478 (arguing that data localization laws "also facilitate domestic surveillance by authorizing law enforcement to compel production of data wherever located, based on the requesting country's own laws"); Woods, *supra* note 23, at 753 (explaining the pros and cons of state direct access to companies by discussing an incident where South Korean authorities raided Google's South Korea offices).

204. *See infra* notes 212–15.

First, the current MLAT system exports Fourth Amendment protections worldwide.[205] When seeking information through the MLAT process, foreign law enforcement must show that the legal process is in compliance with the U.S. Constitution, the ECPA, and the controlling MLAT.[206] This level of privacy protection is higher than the standards used in many other liberal and authoritarian nations.[207] However, once domestic law of the foreign nation controls production of user data from U.S. companies, these countries can reduce the level of protection required for law enforcement to obtain the information, a standard that could be changed based upon a shift in political winds.[208] This is especially dangerous when considered in the national security context, such as the Charlie Hebdo attacks.[209] Following the

---

205. Jennifer Daskal, Professor, American Univ., Panelist at the American Enterprise Institute Conference on Domestic Surveillance on Foreign Shores: The Case of Microsoft's Servers in Ireland 10 (Oct. 6, 2015) (transcript available at https://www.aei.org/wp-content/uploads/2015/09/Transcript.pdf).

206. *See* Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L.J. 617, 623 (2017) (stating that foreign governments have to meet the standards of the ECPA and other U.S. laws to gain access to electronic evidence held by U.S. companies); RUSH & KEPHART, *supra* note 149, at 4 (discussing how U.S. district courts are responsible for ensuring MLAT requests are valid under the both the treaty and the U.S. Constitution before granting the requests); *see also Foreign Government Access to User Data*, *supra* note 148.

207. *See* Klass v. Germany, 2 Eur. Ct. H.R. 214, ¶ 75 (1978) (finding that judicial review is not required prior to intercepting communications); Swire & Kennedy-Mayo, *supra* note 206, at 644–45 (commenting on the strength of the probable cause and probable cause "plus" standards required for search warrants and wiretaps in the United States in comparison to other countries); Jennifer Granick, *The* Microsoft Ireland *Case and the Future of Digital Privacy*, JUST SECURITY (July 18, 2016, 12:46 PM), https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy (noting that the United States' "warrant requirement and . . . wiretapping procedures . . . are generally comparatively stringent," as compared to EU counterparts); *see also* WINSTON MAXWELL & CHRISTOPHER WOLF, A GLOBAL REALITY: GOVERNMENTAL ACCESS TO DATA IN THE CLOUD 8–9 (2012) (discussing the German system in which German prosecutors can request certain data from telecommunications services providers if the information would be helpful to public safety, which can be done upon demand without a court order).

208. *See* Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the VISA Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 710 (2016); *see* Daskal, *supra* note 17, at 490 (emphasizing two likely scenarios: one is that nations could "race to the bottom" by ignoring foreign citizens' data privacy rights, and the other is that foreign governments could enact blocking statutes in order to protect their citizen's data).

209. *See generally Charlie Hebdo Attack: Three Days of Terror*, BBC (Jan. 14, 2015), http://www.bbc.com/news/world-europe-30708237 (describing the incident on

attacks, France passed a sweeping surveillance law, referred to as the French Patriot Act, that enables "intelligence agencies to tap phones and emails without seeking permission from a judge."[210] While the French Patriot Act may be unique because of the context in which it was created, it is not extraordinary in what it attempts to do. Liberal and authoritarian governments have used national security events to alter the level required for law enforcement access to information. This legal malleability invariably threatens user privacy more once the data is centralized under the government's control.[211]

Finally, data localization regulations will limit the number of service providers within a jurisdiction and create a monopoly on privacy controls within a country.[212] Currently, users have the ability to choose which service providers to use.[213] This has created a market where corporations must compete for users, and their key currency is user trust.[214] As such, companies that fail to maintain user trust by not

---

January 7, 2015, in which the headquarters of a controversial French magazine were attacked by two Islamist shooters).

210. Angelique Chrisafis, *France Passes New Surveillance Law in Wake of Charlie Hebdo Attack*, GUARDIAN (May 5, 2015, 12:11 PM), https://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack (describing how the legislation "will allow authorities to spy on the digital and mobile phone communications of anyone linked to a 'terrorist' inquiry without prior authorisation"); *see* Nathan Sales, *French Surveillance Law Compared to US Surveillance*, JUST SECURITY (July 31, 2016, 3:04 PM), https://www.justsecurity.org/25143/snapshot-french-surveillance-law-compared-surveillance-law (stating that the legislation gives the French government "sweeping new powers," including the authority to wiretap without a warrant); *see also* Khaled A. Beydoun, *Beyond the Paris Attacks: Unveiling the War Within French Counterterror Policy*, 65 AM. U. L. REV. 1273, 1313–14 (2016) (commenting on the disproportionate impact of the "French Patriot Act" on Muslim populations).

211. Chander & Lê, *supra* note 3, at 737–38.

212. INST. FOR HUMAN RIGHTS & BUS., NO TRADE OFF: HOW THE FREE FLOW OF DATA ENHANCES TRADE AND HUMAN RIGHTS 12 (2016) (describing how regulations restricting market access to data companies in some African countries have made it difficult for these companies to obtain licenses, thus "limiting the number of service providers and creating a de facto monopoly").

213. *See* Daskal, *supra* note 186 (commenting that "customers may increasingly flee from U.S. providers in an effort to shield their data from the U.S. government's reach").

214. *See* Jennifer Baker, *EU Commission Aims to Ban Forced Data Localization*, IAPP (Oct. 24, 2016), https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization (noting that EU Commission Vice President Andrus Ansip has declared that "trust is everything" in regulating data privacy); *see also* WORLD ECONOMIC FORUM, RETHINKING PERSONAL DATA: TRUST AND CONTEXT IN USER-CENTRED DATA ECOSYSTEMS 3 (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (describing how companies are losing individuals' trust

ensuring proper privacy and security measures can be pushed out of a market.[215] By allowing users to choose between rival providers, the market hypothetically incentivizes providers to employ better privacy protocols. However, in order for this market to exist, data must be able to move across borders.[216] The implementation of data localization regulations will likely result in companies exiting or foregoing entrance into markets.[217] Thus, choices for users will be limited, and they will be unable to change providers if they are uncomfortable or disagree with certain privacy controls.[218] If the number of corporations within a territory is limited, the user must either not use the technology or acquiesce to the privacy controls used by the company.[219] This distinction may be insignificant if the corporation employs adequate protections, but substantial if the corporation provides backdoor access to the local government.[220]

---

regarding data protection and how they must adapt their practices to respect their customers' privacy expectations in order to survive).

215. *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMM. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (discussing the impact of decreased user trust on corporations and finding that forty-five percent of households surveyed about their online activity reported refraining from conducting financial transactions online due to a lack of trust in internet privacy).

216. Baker, *supra* note 214.

217. *See* JAMES M. KAPLAN & KAYVAUN ROWSHANKISH, GLOB. COMM'N ON INTERNET GOVERNANCE, ADDRESSING THE IMPACT OF DATA LOCATION REGULATION IN FINANCIAL SERVICES 2 (2015) (commenting on inefficiency costs of localization causing financial corporations to leave markets); Chander & Lê, *supra* note 3, at 682 (stating that data localization will increase costs for information service providers in such a manner that will render "many of such global services impossible"); Natasha Lomas, *Twitter Is Reviewing Whether to Store Some User Data in Russia*, TECHCRUNCH (Apr. 19, 2017), https://techcrunch.com/2017/04/19/twitter-is-reviewing-whether-to-store-some-user-data-in-russia (commenting on how LinkedIn has been blocked in Russia for refusal to comply with data localization regulations).

218. *See* Chander & Lê, *supra* note 3, at 720 (explaining Microsoft's argument that localizing data could limit customer choice, saying that customers "should have the ability to personally control their [data and records] by choosing to have their [data] held by an entity" outside the country).

219. *See id.* at 716–17 (arguing that because of localization, local companies may choose or be required to utilize companies with weak security measures that have less need to offer stronger security measures to attract customers).

220. Backdoor access allows a government direct access via a purposeful security flaw to user content and information regardless of whether encryption is in place. *See Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, CDT (Mar. 3, 2016), https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-

C. Security Impact

Today, companies employ a series of technical and non-technical controls to identify threats, defend against attacks, and respond to network intrusions.[221] Basic technical controls generally include deploying firewalls and intrusion detection systems and monitoring to identify unauthorized access or data exfiltration.[222] Non-technical controls consist of policies and procedures, such as employment of least privilege,[223] development of an incident response plan, and adherence to a patch management policy.[224] A well-structured information security program will leverage both technical and non-technical controls to ensure the confidentiality, integrity, and availability of information to protect data from bad actors, prevent intentional change, and ensure access.[225]

---

surveillance. Such access allows governments to conduct warrantless and indiscriminate surveillance. *Id.*

221. These concepts are integrated into various U.S. and international cybersecurity frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST Framework) and the International Standards Organization 27001 (ISO 27001) standards.

222. "Firewalls have been a first line of defense in network security for over [twenty-five] years" and are a type of "network security device that monitors incoming and outgoing network traffic." *What Is a Firewall*, CISCO, https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (last visited Feb. 7, 2018). Intrusion detection systems are another type of network security technology that detects "vulnerability exploits against a target application or computer." *What Is an Intrusion Detection System?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids (last visited Feb. 7, 2018).

223. The principle of least privilege is the idea that a user is only granted the amount of access to a system that is required for that user to complete his or her job. Jerome H. Saltzer & Michael D. Schroeder, *The Protection of Information in Computer Systems*, Univ. VA, CS551: Security and Privacy on the Internet Fall 2000 (1974), http://www.cs.virginia.edu/~evans/cs551/saltzer.

224. IT managers use patch management systems to quickly fix emerging vulnerabilities in operating systems and applications. DANIEL VOLDAL, SANS INST., A PRACTICAL METHODOLOGY FOR IMPLEMENTING A PATCH MANAGEMENT PROCESS 1 (2003), https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206 (explaining the importance of patch management and its role in systems configurations).

225. *See* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 7 (Adam Gordan ed., 4th ed., 2015).

Localization will require new servers, people,[226] and tools in each jurisdiction in which the company operates or has users.[227] This replication of systems will create fragmented networks linked to territorial boundaries within an enterprise.[228] By simply stretching and segmenting the enterprise network, data localization reduces the efficacy of security practices and tools to detect and respond to cybersecurity threats.[229] Instead, by centralizing data in several key data centers throughout the world, corporations can implement defense-in-depth practices and reduce redundancies.[230] By doing so, corporations are able to ensure uniform management of the systems, scale prediction and detection technologies to secure a higher quantity of user data, and leverage the distributed architecture of the internet to ensure data availability.[231]

---

226. *See* LEVIATHAN SEC. GRP., ANALYSIS OF CLOUD VS. LOCAL STORAGE: CAPABILITIES, OPPORTUNITIES, CHALLENGES 2 (2015) (outlining the difficulties in cybersecurity hiring domestically and internationally).

227. *See* ALBRIGHT STONEBRIDGE GRP., DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION 7 (2015) (commenting on the lackluster realized employment gains associated with data center constructions); Paul Mozur et al., *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html (discussing the costs of Apple's data center in China).

228. *See* WILLIAM J. DRAKE ET AL., WORLD ECON. FORUM, INTERNET FRAGMENTATION: AN OVERVIEW 45 (2016) (commenting that data localization results in fragmentation at the content, routing, and transactional levels).

229. *See* John Lenhart, *Security for the 21st Century Economy: Borders Hold Less Meaning—and That's a Good Thing*, INFO. TECH. INDUSTRY COUNCIL (Aug. 17, 2016), http://www.itic.org/news-events/techwonk-blog/security-for-the-21st-century-economy-borders-hold-less-meaning-and-thats-a-good-thing (commenting that localization deprives corporations of comprehensive real time monitoring and limits deployment of preventative defenses and security controls).

230. Defense in depth is the concept "that a layered approach to network security makes for a formidable challenge for attackers." SCOTT RASMUSSEN, SANS INST., CENTRALIZED NETWORK SECURITY MANAGEMENT: COMBINING DEFENSE IN DEPTH WITH MANAGEABLE SECURITY 2 (2002), https://www.sans.org/reading-room/whitepapers/bestprac/centralized-network-security-management-combining-defense-in-depth-manageable-security-659 (describing comprehensive cybersecurity as one that plugs diverse methods and technologies into the broadest sampling of the network).

231. *See id.* (describing how the defense in depth approach makes it much more difficult for attackers to compromise a network, while "network security personnel are faced with the same requirement to maintain currency on the diverse architecture as well as vigilance").

This replication of systems is not only expensive to build but also difficult to manage because it creates non-uniform security practices.[232] By decentralizing the governance and response, data localization essentially creates a federated system within the larger enterprise, entrusting each country with autonomy over its own systems.[233] As a result, each jurisdiction is able to choose which types of hardware to use, how to classify incidents, and how to administer privileges.[234]

To better illustrate this, consider hypothetical company A, a multinational company with customers in the United States, European Union, Mexico, Brazil, Singapore, and Malaysia. Before localization, company A has data centers in the United States, Ireland, and India, and it manages all user data from these data centers. In 2020, Mexico, Malaysia, and Singapore all pass data localization laws, mandating that all citizen user data be hosted on servers within the relevant territorial jurisdiction. Prior to localization, company A only needed three sets of servers, firewalls, intrusion detection systems, and security staff to manage cybersecurity risks worldwide. In a post-localization world, company A must maintain six sets of these technical and non-technical controls, with one in each jurisdiction.

By inserting more humans and machines into the enterprise's network, localization not only increases the surface area for attacks, but also allows for new zero-day exploits[235] and alters how each group will detect and respond to attacks.[236] The difference in response can then be the difference between threat mitigation and breach, with the

---

232. *See* SOFTWARE & INFO. INDUS. ASS'N, GUIDE TO CLOUD COMPUTING FOR POLICYMAKERS 5 (2011) (commenting that "uniform security management practices" enable key security practices).

233. *See* Allen C. Johnston & Merrill Warkentin, *IT Security Governance and Centralized Security Controls*, *in* ENTERPRISE INFORMATION SYSTEMS ASSURANCE AND SYSTEM SECURITY: MANAGERIAL AND TECHNICAL ISSUES 24 (Merrill Warkentin & Rayford Vaughn eds., 2006) (stating that an end-user's failure to follow through on security protocols in a decentralized system can potentially compromise the entirety of the network).

234. *See* Rosslin J. Robles et al., *Information Security Control Centralization and IT Governance for Enterprises*, INT'L J. MULTIMEDIA & UBIQUITOUS ENGINEERING, July 2008, at 67, 73 (indicating that in a decentralized system there is "a high level of autonomy for end users in dealing with the security of their respective computing resources").

235. A zero-day exploit is "an unknown exploit . . . that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong." *What Is a Zero-Day Exploit?*, FIREEYE, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html (last visited Feb. 7, 2018).

236. *See* Johnston & Warkentin, *supra* note 233, at 21 (commenting that a lack of "motivation or efficacy for compliance with . . . policies and procedures" can have devastating effects in a decentralized system).

latter resulting in the exposure of personal records, unwanted public attention, and regulatory scrutiny.

Additionally, a centralized security system enables a company to more effectively leverage prediction and detection technologies.[237] A centralized information technology system allows for a company to have broader insights into its environment, and it also enables the company to aggregate information from across the network to determine trends and identify abuse.[238] By employing a "big data" solution to IT security, a corporation can detect incidents more quickly and reduce the time between intrusion and detection.[239]

Finally, data localization limits the ability of companies to ensure system and data availability by leveraging the distributed infrastructure of the internet.[240] Because data can be split, copied, and moved, companies are able to leverage the internet's infrastructure to distribute data to servers in different states, nations, or regions.[241] Companies are able to increase both the efficiency of distribution and security surrounding the information by sharding the data,[242] load balancing it

237. *See* SOFTWARE & INFO. INDUS. ASS'N, *supra* note 232, at 16 (commenting that "[c]loud computing creates the ability to link together millions of security nodes" to better detect threats).

238. RASMUSSEN, *supra* note 230, at 9.

239. Dwell time is the time from the initial intrusion (e.g., patient zero clicks on a phishing link) to the time that the intrusion is detected and removed from the system. ERIC COLE, SANS INST., DETECT, CONTAIN, AND CONTROL CYBERTHREATS 1 (2015), https://www.sans.org/reading-room/whitepapers/analyst/detect-control-cyberthreats-36187; *see, e.g.*, MANDIANT, M-TRENDS 2017: A VIEW FROM THE FRONT LINES 7 (2017) (reporting average dwell times of roughly one hundred days).

240. Richard Bennett, *Surge in Data Localization Laws Spells Trouble for Internet Users*, AEI (May 10, 2016), http://www.aei.org/publication/surge-in-data-localization-laws-spells-trouble-for-internet-users.

241. *See* Reisman, *supra* note 199 (giving the example of an email service that makes a person's email accessible anywhere in the world, stating that the messages "probably exist in multiple copies, which could be located in more than one country").

242. Companies shard data by splitting files into many pieces and spreading the pieces across distributed systems. While this process not only allows for quick recovery, it also means that "[n]o single datacenter has all the information required to reassemble a given document." Patrick S. Ryan et al., *When the Cloud Goes Local: The Global Problem with Data Localization*, COMPUTER, Dec. 2013, at 54, 56.

across servers,[243] and backing it up in multiple areas.[244] This enables companies to more effectively respond to certain threat vectors,[245] such as distributed denial of service attacks, and also mitigate system outages from an attack.[246] Data localization restricts this movement by mandating that a copy of the data remain within the jurisdiction itself.[247] Thus, any balancing or movement of data must occur within the one network, essentially reducing the strength of the network's response.

CONCLUSION

The jury is out on whether Mr. Schrems or Microsoft intended for data localization to occur as a result of their successes. By bringing these cases, these privacy advocates have highlighted the fundamental differences in the EU and U.S. approaches to privacy and have put traditional mechanisms for cross-border data transfers at risk. Thus, these cases encourage data localization by opening the door for increased legislation, prohibiting data transfers from the European Union, and restricting data movement for law enforcement requests. These limitations, whether for commercial or law enforcement

---

243. Load balancing allows companies to re-distribute information or traffic depending upon where information and traffic is concentrated. Load balancing is important for ensuring the availability of data and the reliability of applications. *Load Balancer*, F5 NETWORKS, INC., https://f5.com/glossary/load-balancer (last visited Feb. 7, 2018); *What Is Network Load Balancing?*, MICROSOFT (Mar. 28, 2003), https://technet.microsoft.com/en-us/library/cc779570(v=ws.10).aspx; *see* LEVIATHAN SEC. GRP., *supra* note 226, at 3 (describing how geographic redundancy allows corporations to continue operating despite natural disasters or political disruptions); *see also* BROUGH DAVIS, SANS INST., LEVERAGING THE LOAD BALANCER TO FIGHT DDOS 13 (2010), https://www.sans.org/reading-room/whitepapers/firewalls/leveraging-load-balancer-fight-ddos-33408 (suggesting that global load balancing can be used to mitigate DDoS attacks).

244. *Business Challenge: Backup & Recovery*, SYMANTEC, http://www.symantec.com/computer-backup (last visited Feb. 7, 2018).

245. A threat, or attack, vector describes the manner in which a bad actor attempts to or is successful in compromising the confidentiality, integrity, or availability of a victim's network. *Glossary of Security Terms*, SANS INSTIT. (last visited Feb. 7, 2018) https://www.sans.org/security-resources/glossary-of-terms.

246. During a DDoS attack, an attacker attempts to take down a system or prevent legitimate users from accessing a site by flooding a network with information. *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM (Feb. 6, 2013), https://www.us-cert.gov/ncas/tips/ST04-015.

247. Deven Desai, *Beyond Location: Data Security in the 21st Century*, COMM. ACM, Jan. 2013, at 34, 36 (commenting that "location-based rules falter in a large area such as the EU" and "fail in smaller markets" because the traffic spikes or DDoS attacks cannot be distributed to low traffic servers outside of the territorial jurisdiction).

purposes, undermine user privacy and enterprise data security by placing data under government control and fragmenting corporate information security practices.

Before the courts affirm these cases, they should consider the true state of U.S. and EU law and consider the consequences of each case. Though all litigation has an effect on parties, precedents, and politics, not all consequences are created equally. A key consequence of these cases is the fragmentation, which will restrict families, businesses, and leaders from connecting, profiting, and communicating over the internet. While these consequences were likely unintended, these cases have created a territorial regulatory regime for data privacy—a regime that is antithetical to the free and secure flow of information. Ultimately, these cases will make user data worldwide more vulnerable to privacy and security violations by good and bad actors alike.