International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà Vu

ALYSSA COLEY*

Whether operating globally or simply integrating services on the Internet, many business functions inevitably subject companies to a web of complicated international regulatory and legal requirements. For example, collecting customer information worldwide, working with suppliers abroad, or operating a foreign subsidiary each trigger an obligation to protect the personal data of the individuals involved with those transactions adequately, and in accordance with various jurisdictional specific. Because thousands of American companies are affected by Europe's strict requirements, the Department of Commerce, along with the European Commission, implemented the International Safe Harbor agreement ("Safe Harbor") to assist companies in complying with European data protection laws.

An interesting turn of events ignited significant discourse about whether the Safe Harbor provided satisfactory protection for European data transferred to the United States. One European national's challenge of the Safe Harbor provision led the European Court of Justice to review its adequacy, ultimately leading to the data transfer mechanism's invalidation. Soon thereafter, a new framework, the U.S.-E.U. Privacy Shield ("Privacy Shield") replaced the Safe Harbor. However, this new replacement mechanism has drawn equally harsh criticism.

This Note seeks to understand the disapproval of the two regulatory frameworks governing overseas data transfers, and begins by undertaking a brief analysis of the social forces shaping the vastly different regulatory approaches to privacy protection that exist in the United States and the European Union. The Author suggest that such disapproval stems from different cultural notions in the United States and Europe about privacy that are deeply rooted in those nations' respective histories. The result? Déjà vu for the European Court of Justice as they prepare for another challenge to the validity of the existing international data transfer framework less than one year after its adoption and the date it took effect.

---

* Executive Managing Editor, *Hastings Law Journal*, Volume 68; J.D. Candidate 2017, University of California Hastings College of the Law; B.A. Business Economics 2012, University of California, Irvine. The Author would first like to thank Professors Lothar Determann, Jill Bronfman, and Ahmed Ghappour for their expertise and acumen, ultimately illuminating a career path with inexhaustible opportunities to challenge a fresh legal mind. The Author would also like to extend her gratitude to the Notes and Production Teams as well as recognize the Executive Production Editor, Isabella Langone, and the Editor-in-Chief, Amy Holtz. Not only are they both dear friends, but this Note would not be where it is today without their hard work and dedication. Lastly, the Author would like to thank her father and grandparents for their unyielding support, love, and enthusiasm.

Table of Contents

Introduction

The Edward Snowden revelations, alleging Facebook's involvement in the PRISM mass surveillance program, prompted Austrian Ph.D. student and privacy activist Maximillian Schrems to take action. Schrems considered these revelations "the biggest surveillance scandal in years," and he wanted to write for the fundament rights of millions of users abroad.[1] As such, in June 2013 Schrems filed a complaint against Facebook Ireland with the Irish Data Protection Commissioner. He claimed that indicated a violation of the Safe Harbor participant guarantee of adequate protection. The Irish Data Protection Commissioner rejected the complaint as frivolous, leading Schrems to challenge the decision before Ireland's High Court.[2] The High Court was concerned that the widespread surveillance of personal data by several federal U.S. agencies contradicted Irish privacy laws and called upon the European Court of Justice ("CJEU") to review the case instead.[3] Before the CJEU came to a decision, the European Commission found in an executive decision that U.S. companies provided adequate privacy protection under the Safe Harbor agreement.[4] However, in October

1. Radhika Sanghani, *Facebook 'PRISM' Decision to Be Reviewed by Irish High Court*, Telegraph (Oct. 24, 2013), http://www.telegraph.co.uk/technology/facebook/10401419/Facebook-PRISM-decision-to-be-reviewed-by-Irish-High-Court.html.

2. *Id.*

3. Ruadhán Mac Cormaic, *High Court Refers Facebook Privacy Case to Europe*, Irish Times (last updated June 19, 2014, 1:04 PM).

4. Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC).

2015, the CJEU overturned the European Commission's decision, issuing a judgment that declared the Safe Harbor provision invalid.[5]

After two years of negotiation, the European Commission and the United States finally came to an agreement on a new framework for transatlantic data flows called the U.S.-E.U. Privacy Shield ("Privacy Shield"). The Privacy Shield was meant to ameliorate the insufficiency of the Safe Harbor by ensuring that the United States provided an adequate level of protection for personal data transferred to the United States from outside of the European Economic Area. However, with criticism that the Privacy Shield lacks meaningful change, unsurprising it has already garnered equally harsh criticism from European regulators.[6]

Consider the fable "The Blind Men and the Elephant":

> It was six men of Indostan, [t]o learning much inclined, [w]ho went to see the Elephant (Though all of them were blind), [t]hat each by observation [m]ight satisfy his mind.
>
> The *First* approach'd the Elephant, [a]nd happening to fall [a]gainst his broad and sturdy side, [a]t once began to bawl: "God bless me! but the Elephant [i]s very like a wall!"
>
> The *Second*, feeling of the tusk, [c]ried, -"Ho! What have we here [s]o very round and smooth and sharp? To me 'tis mighty clear, [t]his wonder of an Elephant [i]s very like a spear!"
>
> The *Third* approach'd the animal, [a]nd happening to take [t]he squirming trunk within his hands, [t]hus boldly up and spake: "I see," –quoth he- "the Elephant [i]s very like a snake!"
>
> The *Fourth* reached out an eager hand, [a]nd felt about the knee: "What most this wondrous beast is like [i]s mighty plain," –quoth he,-"'Tis clear enough the Elephant [i]s very like a tree!"
>
> The *Fifth*, who chanced to touch the ear, [s]aid- "E'en the blindest man [c]an tell what this resembles most; Deny the fact who can, [t]his marvel of an Elephant [i]s very like a fan!"
>
> The *Sixth* no sooner had begun [a]bout the beast to grope, [t]hen, seizing on the swinging tail [t]hat fell within his scope, "I see," –quoth he,- "the Elephant [i]s very like a rope!" And so these men of Indostan [d]isputed loud and long, [e]ach in his own opinion [e]xceeding stiff and strong, [t]hough each was partly in the right, [a]nd all were in the wrong![7]

---

5. Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. 627; *see* Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1–112 (EC).

6. Katie Bo Williams, *New Transatlantic Data Deal Draws Fire from Privacy Advocates*, HILL (Feb. 29, 2016, 9:34 AM), http://thehill.com/policy/cybersecurity/271126-new-transatlantic-data-deal-draws-fire-from-privacy-advocates.

7. John Godfrey Saxe, *Blind Men and the Elephant*, http://www.allaboutphilosophy.org/blind-men-and-the-elephant.htm (last visited June 4, 2017).

The moral of this story is that often in theological wars parties differ in their perceptions of the subject matter discussed resulting in ignorant disputes. Each man's opinion of the Elephant was influenced by the particular part of the Elephant they encountered, and each observation was informed by past experiences. Differing perspectives may appear to be in direct conflict, when in reality, each individual's view in context may be technically correct.

Consider a twist: Suppose the Elephant is a Lion, and a great predator and enemy of man, where each man is responsible for keeping the Lion away from their respective villages. While the men continue to argue over what a Lion is in developing their plans of attack, the Lion studies the villages from afar, stalks its prey, and becomes a greater threat. The men who are fooled into arguing over superficialities waste precious time. A wise man would know time is better spent formulating and implementing a plan of attack, rather than ignorantly arguing over defining an indefinite concept. While each man may differ over what threat they think the Lion poses and which aspect of their villages' safety is most valued, all men agree that every village must be protected. No man or village can fight the Lion alone; therefore they are forced to unite as one to conquer the threat.

Here, the United States and the European Union are each like a village and the safety of the villagers is akin to individuals' right to privacy protection. In order for the U.S.-E.U. economy to thrive, each villager, man, or country's interests must be safeguarded. Equal protection of each village's unique interests reinforces the trust necessary to work together to combat threats against the village, or in this case, threats to an individual's privacy rights. Once that trust is broken, the village becomes divided, where neither side is better off and rebuilding trust is a challenge.

This Note takes the position that scrutinizing the new Privacy Shield agreement is repetitive and efficient. Furthermore, implementation of a designated data protection authority in the United States that is sufficiently independent and has adequate resources—similar to those already existing in the European Union—might actually resolve the perceived weaknesses of the old Safe Harbor provision and the new Privacy Shield. This is where any efforts to resolve conflict should instead be focused. However, this Note suggests that until the United States actually devotes adequate resources to improve regulatory and enforcement agencies that could have an actual effect on privacy practices on the ground, Europe will be dissatisfied with whichever agreement is in place.

Part I of this Note will explore the forces behind the divergent cultural notions of privacy. Privacy laws developed to increase the ability of individuals to exercise control over personal information; this is

consistent across all countries.[8] Where the European Union and the United States differ most, however, is on their respective citizens' values and expectations when it comes to privacy. Consequently, the data privacy laws and correlating definitions in each jurisdiction differ as well.[9]

Part II of this Note will introduce the laws governing international data transfers, with which strict compliance is required by the European Union—specifically the Safe Harbor agreement and the Privacy Shield frameworks. There is a stark contrast between each side's regulations governing data processing, transfers, or retention, and authority to obtain foreign court orders or to enforce compliance. This creates tension in a world where both social interaction and business are integrated globally.

Part III of this Note will compare the old Safe Harbor agreement to the framework of the new Privacy Shield. It will discuss how scrutiny over the text of the new Privacy Shield framework is unfounded because upon taking a closer look at the actual implementation of privacy protections, companies effectively implement analogous best practices, regardless of whether they have agreed to abide by the international data transfer mechanisms that are available. Part III then highlights areas of weakness in the new framework that warrant our attention and scrutiny that existed in the previous agreement. This Note takes the position that aside from addressing the European Union's concerns about the ability of its citizens to seek redress for privacy related claims, resources should be devoted to the implementation of sufficiently independent, designated data protection authorities in the United States, similar to those in the European Union.

Finally, Part IV of this Note will analyze the future of privacy in the United States. In the digital age, rapid advances in technology result in increased ease with respect to collecting, storing, sharing, and transferring data across international borders. Reaching an agreement on a formal legal framework that facilitates the free flow of information between countries is only the beginning. This Note argues that before the United States and the European Union are going to be able to agree on a formal legal framework to ensure sufficient protection of personal data, changes must be made to the regulatory and enforcement agencies providing protection of U.S. privacy concerns. Because many U.S. citizens feel strict regulation of personal data will result in a hampering of economic freedom, finding a way to better protect our citizens without unduly restricting the free flow of information is paramount to our continued economic development and success as a nation.

8. LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW: INTERNATIONAL CORPORATE COMPLIANCE XIII (2d ed. 2015).

9. *Id.* at XII.

As a preliminary matter, there are several terms that must be defined, as their technical meanings differ from the manner in which they are often construed. First, "personal data" refers to any information relating to the "data subject," meaning any identifiable person.[10] "Data processing" means any operations performed on personal data, manual or automatic, such as collection, storage, redaction, alteration, use, disclosure, dissemination, erasure, or destruction.[11] A "data controller" is a person or entity that determines the purpose of and means for processing any personal data, whereas a "data processor" is the person or entity that processes personal data on behalf of the data controller.[12] Next, "data privacy" is distinguishable from "data protection" in that data *protection* relates to protecting individuals "from the effects of automated data processing," whereas data *privacy* laws are intended to protect individuals "from intrusion into seclusion and interception of confidential communications."[13] "Data security" laws protect individuals' personal information from harms that were a result of unauthorized access—specifically identity theft—and are meant to supplement data privacy laws.[14] For the purposes of this Note, the term "data privacy" will be used as an umbrella term encompassing data protection, data privacy, and data security.[15]

I. FORCES BEHIND THE DIVERGENT CULTURAL NOTIONS OF PRIVACY

A. THE EUROPEAN UNION

Let us assume that the European Union is like the *Third* man in the fable—threatened and afraid of the Elephant because of a harrowing past with snakes. After the atrocities of World War II, people around the world began to recognize the perils of archiving mass amounts of personal information in databases. This prompted the United Nations General Assembly to adopt the Universal Declaration of Human Rights in 1948.[16] The Declaration's inclusion of explicit protections against intrusions into an individual's privacy sparked further global efforts to define boundaries in privacy rights and implement further protections throughout other nations' laws.[17] Shortly after World War II in 1950 the

10. Council Directive 95/46, art. 2, 1995 O.J. (L 281) 31, 38 (EC).

11. *Id.* at 38.

12. *Id.*

13. DETERMANN, *supra* note 8, at 4–5.

14. *Id.* at 6.

15. *Id.*

16. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2015 262 (2015).

17. Additionally, the Organisation for Economic Cooperation and Development ("OECD") developed privacy guidelines in 1980 establishing eight key principles for the protection of personal information, including: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards; (6) the openness principle; (7) individual participation; and (8) accountability. The OECD

Council of Europe adopted the European Convention on Human Rights.[18] The European Union decided that privacy was a fundamental human right, where "[e]veryone has the right to respect for his or her private and family life, home and communications."[19] Additionally, the European Union included the right to protection of everyone's personal data concerning him or herself.[20]

Nearing the age of "Big Brother," as imagined in George Orwell's *Nineteen Eighty Four*, Germany was particularly cognizant of the dangers posed by an omniscient totalitarian authority in power. The people of Germany feared that the dystopian society forecasted in 1984 was an all-too-real possibility. This bourgeoning apprehension primed the State of Hesse in Germany to enact the first data protection law ever in 1970.[21] The European Data Protection Directive followed in 1995, which bound all European Union member states.[22] Thereafter, the remaining German states and other European countries followed suit, implementing tailored regulatory regimes that also generally prohibited processing of personal data.[23]

B. THE UNITED STATES

Whereas previously the European Union was like the *Third* man in the fable, the United States could be akin to the *Fourth* or *Fifth* men—intrigued and contemplating how to benefit from the encounter. Citizens in the United States took advantage of the promising new developments in technology, viewing the ability to archive mass amounts of information as an overlooked economic opportunity. Contrary to the omnibus European style data protection regime, the U.S. Congress deliberately chose extensive regulation with respect to governmental data processing, while facilitating a market-oriented allowance for data processing in the private sector.[24]

Despite the differences in the two regimes, the clairvoyance of George Orwell's infamous novel also provides insight into the economic-based rationale behind our patchwork data privacy regime. The American preference for deregulation and freedom of information

Guidelines were updated in 2013 to include three additional concepts: (1) national privacy strategies; (2) privacy management programs; and (3) data security breach notification. The OECD governs a group of thirty-four leading industrial countries concerned with global economic and democratic development. *See id.* at 262–64.

18. *See id.* at 266.

19. Charter of Fundamental Rights of the European Union 364/01, art. 7, 2000 O.J. (C 364) 1, 10 (EU).

20. *Id.* art. 8.

21. DETERMANN, *supra* note 8, at 4.

22. Council Directive 95/46, *supra* note 10, art. 2.

23. DETERMANN, *supra* note 8, at 5.

24. Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 179 (1999).

provoked the existing conflict between the United States and the European Union. Where U.S. laws are viewed as inadequate, riddled with too many loopholes and national security exceptions for counter terrorism intelligence, Europe has declared that "the choice for mankind [lies] between freedom and happiness, and that, for the great bulk of mankind, happiness [is] better."[25] In the United States, on the other hand, despite the Declaration of Independence's statement that "Americans were of one mind to protect 'LIFE, LIBERTY, and the PURSUIT of HAPPINESS[,]'"[26] happiness to many U.S. citizens is freedom.

C. A COMPARISON OF THE U.S. AND E.U. APPROACHES

The general rule for the European system of data protection laws is that any processing of personal data is typically "verboten," which is German for forbidden.[27] In Europe, the expectation is that personal data is protected "not only within Europe, but throughout the world if the data originates in a member state."[28] European data protection laws give broader protection, covering all personal data, while the reactive U.S. system limits the definition of "personal data" to the more sensitive categories of data collected.[29] There is more harmonization within the European Union than in the United States. In other words, the European preference as to how the processing of data should be regulated resulted in a blanket ban on any processing of personal data. With a blanket ban, processing of data requires an "opt in" system. From the perspective of a citizen in Europe, the gaps in data coverage create confusion among regulated entities and consumers.[30] The tapestry of specific laws tied to specific technology or business practices devalues the moral weight of privacy and its role in a democratic society.[31]

Conversely, in the United States, the processing of personal data is generally allowed, subject to certain exceptions. There is no data minimization requirement in the United States, contrary to European data protection laws, where minimizing the automated processing of data

25. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 271 (1949); *id.* at 269–84.

26. *"July 4th 1776. When Our Declaration of Independence Was Signed Loyal Americans Were of One Mind to Protect Life, Liberty, and the Pursuit of Happiness,"* NAT'L ARCHIVES: DOCSTEACH, https://www.docsteach.org/documents/document/july-4th-1776-when-our-declaration-of-indepedence-was-signed-loyal-americans-were-of-one-mind-to-protect-life-liberty-and-the-pursuit-of-happiness (last visited June 4, 2017).

27. DETERMANN, *supra* note 8, at 4.

28. Cate, *supra* note 24, at 179.

29. DETERMANN, *supra* note 8, at XII.

30. KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 49 (Sandra Braman & Paul Jaeger series eds., 2015).

31. *Id.*

is paramount, even if the data is already publicly available.[32] This hands-off approach to privacy developed nearly three decades after the data protection field emerged in Europe, mirroring the sentiment favoring economic growth evidenced by many companies restructuring their business models to adapt to massive shifts in technological capacities.[33] Privacy laws enacted in the United States have been reactive, rather than proactive, like those in the European Union. This has resulted in several extraordinarily specific statutes that are only relevant in very narrow circumstances, while many privacy rights remain without a remedy.[34] The United States continues to lack a federal general right to privacy and a designated privacy enforcement authority with adequate resources for enforcement.

Individuals in the United States are generally left unprotected from intrusion and interception of private communications. The United States has constitutional protections in circumstances where there is a "reasonable expectation of privacy,"[35] but redress for privacy torts—such as intrusion into seclusion[36] or defamation—can be obtained only through state-specific common law claims. Privacy protections can also be found in state constitutions, federal and state statutes, and contract law. The Fourth Amendment provides sounder protections for individuals when they are *within* their homes than is provided outside of them. In the digital age, defining when a person is secure in their persons, papers, and effects has become an increasingly difficult task due to the ease of access, storage, and analysis of data—a problem the Framers of the Constitution were unlikely to have anticipated.

Previously, questions regarding which information individuals retain a reasonable expectation of privacy in were fairly straightforward. Recently, however, these inquiries have become increasingly nebulous. For example, Internet Protocol ("IP") addresses may identify an individual in a single person household, but also may only identify one individual in a household with more than one individual. Furthermore, an IP address may be allocated to several individuals if it is owned by a business. Additionally, URLs contain the relevant web address, analogous to a residential address. However, problems arise when a web address also includes identifying information about an individual, unlike a residential

32. DETERMANN, *supra* note 8, at 4.

33. BAMBERGER & MULLIGAN, *supra* note 30, at 220.

34. *See generally* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003) (discussing the evolution of privacy rights in the American legal system).

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

36. The invasion of privacy tort "intrusion into seclusion" is liability for "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, . . . if the intrusion would be highly offensive to a reasonable person." Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668, 678 (Cal. Ct. App. 1986) (quoting RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977) (alternations in original) (emphasis omitted)).

address. Typically identifying information has greater protection. However, search terms entered into a search engine qualify as non-subscriber content, despite the potential for information within the search term to comprise the identity of an individual.[37] Specific data points themselves may not be particularly threatening, but when collected in aggregate and over time, these data points could become very illuminating of the private life of an individual. This concept is integral to a company's use of "big data," Big data, unsurprising, describes a large volume of data. However, this data specifically pertains to the sets of data that inundate companies, gathered through their regular day-to-day operation.[38] Businesses analyze big data to gain "insights that lead to better decisions and strategic business moves."[39] The detail and specificity of these insights are so advanced that the Framers—nor even our own grandparents—could have adequately contemplated the privacy issues they would give rise to.[40]

Lastly, the meaning of "sensitive data" in the United States is starkly different from the meaning of the same term in Europe.[41] For example, social security numbers and credit card information are considered sensitive in the United States. In contrast, the European Union is less concerned with identity theft and more concerned with identification of political opinions, racial or ethnic origin, religious or philosophical beliefs, and sexual orientation. Both regimes consider information regarding medical or health conditions, certain types of criminal records, and likeness to be sensitive as well.[42] Generally speaking, the European regime is considered much stricter, largely on the basis that the United States rarely requires inclusion of most data considered to be sensitive in Europe.[43] In Europe, express consent from the data subject must be obtained before any sensitive data may be transferred out of the European Economic Area, which is not required in the United States.[44]

37. Pouya Bozorgchami, *Googling Away Your Privacy: Protecting Online Search Inquiries from Unwarranted State Intrusion*, 2009 LOY. L. REV. 1, 37, http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1045&context=llr_symposia.

38. *Big Data: What It Is and Why It Matters*, SAS INST. INC., https://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited June 4, 2017).

39. *Id.*

40. *See generally* Kashmir Hill, *How Target Figured out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#63d946bf6668.

41. DETERMANN, *supra* note 8, at 9.

42. *Id.*

43. *Id.* at 9–10.

44. The European Economic Area encompasses the territories of member states of either the European Union or European Free Trade Association. *Id.* at 10.

II. INTERNATIONAL DATA TRANSFERS AND PROCESSING

The European Union strictly prohibits any data transfers unless certain requirements are met. Any company wishing to process personal data of a European data subject must satisfy three "hurdles."[45] First, a company must comply with local requirements regarding collection and processing of data.[46] Second, companies must provide justification for all transfers.[47] Third, companies must ensure that the data recipient's jurisdiction provides adequate levels of data protection.[48] In 2000, the U.S. Department of Commerce and the European Commission negotiated the Safe Harbor agreement as a compliance mechanism to facilitate international transfers of data outside of the European Union. Companies in the European Economic Area are even prohibited from transferring personal data on their own company's employees, contractors, customers, and other contacts if the transfer is to any other jurisdiction not included in the European Economic Area.[49] This poses a problem for multinational companies who may happen to have headquarters outside of Europe with a subsidiary in the European Economic Area, or other similar cross-frontier structures.[50] Additionally, this restriction may also indirectly affect third-parties, such as customers, suppliers, and other business partners.[51] To overcome the "third hurdle" prohibiting international data transfers, several compliance mechanisms exist to ensure the required protection of the data recipient.[52]

Other than the Safe Harbor provision, there are four alternative compliance mechanisms available to any person or entity outside of Europe who wishes to facilitate an international transfer of data.[53] First, companies are able to legitimize data transfers out of necessity under a statutory or contractual obligation.[54] Statutory obligations in European laws are rare; however, they do exist in some circumstances, and may legitimize data transfers.[55] Moreover, a company may transfer data to fulfill a contractual obligation, as long as the contract is made directly between the data controller and the data subject.[56] Second, data may be processed internationally with valid consent from the data subject.[57]

45. *Id.* at 42–48.
46. *Id.* at 41.
47. *Id.* at 42–44.
48. *Id.* at 44–48.
49. *Id.* at 41.
50. *Id.*
51. *Id.*
52. *Id.* at 44–48.
53. *Id.*
54. *Id.* at 44.
55. *Id.*
56. *Id.*
57. *Id.*

Valid consent is consent that is "freely given, specific, informed, and in writing."[58] This mechanism allows data processors to overcome the "third hurdle" as well as any other restrictions on data transfers.[59]

The third mechanism is a Standard Contractual Clause ("SCC"), which is used when one company is in the European Economic Area and wishes to transfer data to another company (or within the same company) outside of the European Economic Area. The European Commission has approved two types of SCCs, which may be used between two data controllers or between a data controller and a data processor.[60] The SCCs create a presumption of adequate protection—however, they are still subject to scrutiny by the relevant Data Protection Authority.[61] The fourth and final compliance mechanism is Binding Corporate Rules ("BCRs"). A BCR is a code or policy statement that reflects and safeguards compliance with European data protection laws throughout a group of companies.[62] BCRs may be used when a company has implemented them uniformly throughout the entire organization, when enforceable by the data subject, and when the BCR indicates a clear duty of cooperation with data protection authorities in the European Union.[63] The relevant Data Protection Authority in the country from which the data is to be transferred must approve each BCR.[64] The Article 29 Working Party ("WP29")[65] decides who the relevant Data Protection Authority is and has published guidelines for which topics to address in a BCR, but the European Commission has not published preapproved templates similar to SCCs.[66]

The Safe Harbor provision is the most popular compliance mechanism to overcome the third hurdle. The Safe Harbor covers data transfers to the United States and onward, either to other U.S. companies or elsewhere in the world.[67] Either the Safe Harbor is a "self-certify" program where participants must be a company that is subject to the jurisdiction of the Federal Trade Commission ("FTC") or they are a U.S. air carrier or ticket agent who is subject to the Department of Transportation.[68] Because the FTC has such broad power with respect to commerce, most companies

58. *Id.* at 45.
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.* at 47.
63. SOLOVE & SCHWARTZ, *supra* note 16, at 278.
64. *Id.*
65. Representatives of each national Data Protection Authority of the European Economic Area form the WP29. The WP29 issues guidance to both companies and legislatures. DETERMANN, *supra* note 8, at 47.
66. SOLOVE & SCHWARTZ, *supra* note 16, at 278.
67. *Id.*
68. *Id.* at 45.

fall under the FTC's authority, including telecommunication and financial service providers.[69] Certification to participate in the Safe Harbor Program is completed through the Department of Commerce, where during the certification process the organization agrees to comply with the seven Safe Harbor principles: (1) notice; (2) choice; (3) onward or third-party transfers; (4) security; (5) data integrity; (6) access; and (7) enforcement.[70] The fundamental right to respect for private life—found in the European Commission on Human Rights as previously mentioned—is founded upon these principles, and adherence was thought to ensure protection of that fundamental right.

III. THE SAFE HARBOR FRAMEWORK VS. THE PRIVACY SHIELD

Long before the Safe Harbor provision was invalidated, tension existed between European and American privacy laws.[71] A previous landmark privacy ruling by a European court allowing "anyone with connections to Europe to request that global search engines remove links to items about themselves from queries," now known as the "Right to be Forgotten," prompted the Commission Nationale de l'Informatique et des Libertés to reject Google's attempt to limit how it may be applied worldwide.[72] The French "privacy watchdog" argued that the decision was not implying that other countries must apply French law extraterritorially, but rather that it simply requests full observance of European legislation by non-European players who offer their services in Europe.[73] Typically the court will agree with the court's advocate general, as occurred in the Safe Harbor decision. However, in the Right to Be Forgotten decision, the court went against the advice of the court's advocate general, a rare occurrence.[74] Tensions continued to grow after the Snowden revelations, eventually leading to the challenge by Schrems and the subsequent invalidation of the Safe Harbor.

The Safe Harbor framework previously enabled thousands of U.S. businesses to self-certify. This certification was, and continues to be, a promise to adhere to the seven principles previously mentioned, along with several additional requirements.[75] It was set in place to assure an

69. *Id.* at 47.

70. SOLOVE & SCHWARTZ, *supra* note 10, at 274.

71. Mark Scott, *France Rejects Google's Efforts to Limit Application of Privacy Ruling*, N.Y. TIMES: BITS (Sept. 21, 2015, 5:29 AM), https://bits.blogs.nytimes.com/2015/09/21/france-rejects-googles-efforts-to-limit-application-of-privacy-ruling/?_r=0.

72. *Id.*

73. *Id.*

74. *Id.*; *see* Press Release, Court of Justice of the E.U., Press Release No. 106/15: Advocate General's Opinion in Case C-362/14, Maximillian Shrems v Data Protection Commissioner (Sept. 23, 2015).

75. *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor (last visited June 4, 2017).

equal level of protection for European citizens' personal data akin to that provided by the E.U. Data Protection Directive 95/46/EC.[76] The FTC commented that they will "continue to expect companies to comply with their ongoing obligations with respect to data previously transferred under the Safe Harbor Framework."[77] Meanwhile, in Europe, the Safe Harbor agreement is as good as dead. Hamburg Data Protection Authorities confirmed they will be "cracking down" on companies that still rely on the provision for their transatlantic data transfers, and that they have been preparing fines and investigating several U.S. multinationals.[78]

The Privacy Shield will remain a "self-certify" program, where the seven principles remain in place. The European Union's new General Data Protection Regulation explicitly endorsed self-certification as a means of securing international data transfers.[79] The most notable changes in the transition from the Safe Harbor to the Privacy Shield are primarily found in the level of detail used to describe the principles and in the implementation of more robust obligations regarding customer notice, training, self-assessment, and auditing practices. These changes were included in an effort to increase the transparency of certified businesses.[80] Due to the scarcity of alternative compliance mechanisms, the increased obligations of the Privacy Shield will likely not deter multinational companies from self-certifying, and in fact, companies will likely find the transition fairly straightforward.[81]

Nevertheless, the apparent lack of meaningful change is precisely the reason the new framework has received so much criticism. The Privacy Shield "places a heavy focus on ramping up the way that companies communicate their compliance rather than making changes to the substantive steps businesses need to take to protect transferred data,"[82] and several influential organizations dedicated to protecting privacy rights and civil liberties have publicly disparaged the new regime. Even social media platforms have received comments about the Shield, such as the following: "[E]veryone knows: it's as bad as the first one,"[83]

76. Council Directive 95/46, *supra* note 10.

77. *U.S.-EU Safe Harbor Framework*, FED. TRADE COMMISSION (last updated July 25, 2016), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

78. David Meyer, *Privacy Shield Legality 'Rather Doubtful,' Says German DPA*, INT'L ASS'N OF PRIVACY PROFS. (Mar. 21, 2016), https://iapp.org/news/a/privacy-shield-legality-rather-doubtful-says-german-dpa/.

79. *Id.*

80. Allison Grande, *Privacy Shield Text Won't Spur Sweeping Data Transfer Fixes*, LAW 360 (Feb. 29, 2016, 9:23 PM), https://www.law360.com/articles/765097/privacy-shield-text-won-t-spur-sweeping-data-transfer-fixes.

81. *Id.*

82. *Id.*

83. European Digital Rights (@edri), TWITTER (Mar. 4, 2016, 1:39 AM), https://twitter.com/edri/status/705689212771823616.

"[i]t's unclear what, if anything, the new Privacy Shield is supposed to be shielding people from,"[84] and it "appears to amount to little more than a remarketed version of the pre-existing Safe Harbour decision, offering little more than cosmetic changes."[85] Such comments are not entirely baseless. No comment so far is as apropos as the tweet by Max Schrems himself stating, "#PrivacyShield: They put ten layers of lipstick on a pig but I doubt the Court and [data protection authority regulators] now suddenly want to cuddle with it."[86]

Before the text of the amended Privacy Shield was finalized, European Data Protection Authorities needed to approve it. One German Data Protection Authority, Johannes Caspar, has already cast doubt on the ability of the Privacy Shield to survive this heightened scrutiny. Whether the agreement will "'meet the high level of the requirements the [CJEU] postulated in the Schrems ruling is rather doubtful[]' . . . . 'This has to be assessed very closely by the [Data Protection Authorities].'"[87] At 130 pages, the Privacy Shield package is "dense, and potentially daunting."[88]

Citizens of the United States identify with the European concerns regarding the ability of U.S. agencies to enforce compliance with the original Safe Harbor principles through audits and monitoring. The Electronic Privacy Information Center ("EPIC") in Washington D.C. is a public interest research group dedicated to bringing awareness to emerging civil liberties issues and protecting privacy.[89] EPIC fears that the Privacy Shield's lack of an effective means of enforcement and redress for privacy violations places an unreasonable burden on consumers seeking reparation.[90] Further, EPIC states that the most significant shortfall (other than the lack of enforcement) is accountability.[91] Without enforcement and clear disincentives, there are no satisfactory guarantees that U.S. companies will not violate their declared privacy practices.[92] Thus, no matter what these companies are self-certifying to, if there is no one to

84. Danny O'Brien & Rainey Reitman, *The Privacy Shield Is Riddled with Surveillance Holes*, ELECTRONIC FRONTIER FOUND. (Mar. 3, 2016), https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes.

85. *See* Press Release, The Greens/EFA in the Euro. Parliament, EU-US Data Protection: New 'Privacy Shield' Data Transfer Framework a Cosmetic Change (Feb. 29, 2016), http://www.greens-efa.eu/eu-us-data-protection-15242.html.

86. Williams, *supra* note 6 (alteration in original).

87. Meyer, *supra* note 78.

88. Gabe Maldoff, *We Read Privacy Shield so You Don't Have to*, INT'L ASS'N OF PRIVACY PROFS. (Mar. 7, 2016), https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to/.

89. *Schrems v. Data Protection Commissioner*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/intl/schrems/ (last visited June 4, 2017).

90. *Id.*

91. *Id.*

92. *Id.*

enforce their promises then text of the agreement may as well be null and void.

In contrast, non-U.S. citizens such as Schrems are largely demonstrating uneasiness with the government's apparent power to compel disclosure of data collected by companies who have self-certified and are in compliance with the Safe Harbor program, or will be in future compliance with the Privacy Shield. United States agencies such as the National Security Association ("NSA"), Central Intelligence Agency ("CIA"), and Federal Bureau of Investigation ("FBI"), that have expansive access and control through mass surveillance programs, continue to exist, and there is little a business can do to prevent government overreach, unless that business is an online service provider. Why is it that people in Europe are outraged at the thought of agencies conducting mass surveillance, such as the U.S. NSA, when European data protection regulations also continue to largely exempt data processing for national security purposes?[93]

The answer lies within two cultures' distinct definitions of a reasonable expectation of privacy. While national security agencies have enormous discretion, the manner in which those agencies exercise that discretion defines the boundaries of their power. In other words, they will define boundaries that address the concerns and values of their own citizens, which may not comport with different views in other jurisdictions. If the NSA in the United States is able to continue to operate in its current clandestine manner, the United States will need an independent agency to keep the NSA in check. Even the NSA equivalent in Europe appointed a Data Protection Authority in February 2014.[94] Since the United States is no stranger to a system of checks and balances, they could implement an analogous structure.

A. A COMPARISON OF THE TWO ENFORCEMENT AUTHORITIES

As explained previously, representatives of each national data protection authority of the European Economic Area form the WP29.[95] The WP29 issues guidance to both companies and legislatures and determine who the relevant Data Protection Authority will be.[96] Additionally, there are locally designated Data Protection Authorities that have significant independence. The role of a designated Data Protection Authority includes serving as a body to be notified before any data processing occurs or to obtain approval from before any transfers outside of the European Economic Area occur.[97] Alternatively, several

93. DETERMANN, *supra* note 8, at 5.
94. *Id.* at 13.
95. *Id.* at 47.
96. *Id.*
97. *Id.*

European countries have allowed companies to appoint a Data Protection Officer, either an internal employee or an external service provider.[98] These Data Protection Officers are not government officials, but they must monitor whether the company is in compliance with applicable data protection laws.[99] They are overseen by local Data Protection Authorities and must report serious offenses. In fact, even some government agencies have appointed Data Protection Officers to monitor internal compliance efforts.[100] The European General Data Protection Regulation provisions discussing Data Protection Officers, where a data controller's employee must fulfill certain requirements as a Data Protection Officer, do not provide much clarity either. They will serve an indefinite term and be protected from dismissal, but at the same time, the Data Protection Officer position could be outsourced.

United States consumer protection agencies like the FTC and other government agencies, such as the U.S. State Attorneys General, the FCC, or the Department of Health, are tasked with responsibilities similar to those handled by European Data Protection Authorities.[101] However, unlike their European counterparts, the FTC was responsible for enforcing these promises from companies who certified that they participate in (and agree to comply with) the Safe Harbor framework.[102] In addition to requiring these companies to follow through on their self-certified obligations, the FTC encourages companies to continue following robust privacy practices, reviewing their privacy policies, and ensuring they describe their privacy practices accurately, including those involving international data transfers.[103]

The narrowly tailored data protection and data privacy laws are not the result of a lack of oversight. By developing laws based on actual and imminent threats in relevant sectors, the United States benefits from the preservation of freedom of information and technological progress.[104] By considering the needs of many business models, the United States has been a leader in innovation and market share for many information driven sectors such as e-commerce, cloud computing, software-as-a-service, and social networking, while European companies by comparison are far off.[105] If the threat of an indefinite ban on international data transfers were to materialize, many companies would suffer economic loss from the inability to continue to do business as usual.

98. *Id.*
99. *Id.*
100. *Id.*
101. *U.S.-EU Safe Harbor Framework*, *supra* note 77.
102. *Id.*
103. *Id.*
104. DETERMANN, *supra* note 8, at 6.
105. *Id.* at 5.

Europe's biggest concern may be the ability of governmental authorities to demand disclosure of personal data from online service providers. In the context of electronic communications, the requirements of the Stored Communications Act ("SCA") are inconsistent with Fourth Amendment requirements. Title I of the Wiretap Act is the only Title under the Electronic Communications Privacy Act ("ECPA") that provides for an exclusionary rule.[106] Neither the SCA nor the Pen Register Act allow for suppression of evidence upon a constitutional violation during the collection of evidence.[107] Additionally, in lieu of a warrant, the SCA also provides the government with an option to obtain a "D-order" to compel contents of communications from online service providers in certain situations. The D-order requires a governmental entity to offer only "specific and articulable facts."[108]

It is important to note that, pursuant to the Fourth Amendment, obtaining a warrant requires probable cause.[109] Here, the specific and articulable facts standard is an easier standard for the government to meet than probable cause, and falls short of the requirements of the Fourth Amendment. The U.S. House of Representatives unanimously passed the Email Privacy Act on April 27, 2016, which requires the government to get a probable cause warrant from a judge before obtaining the contents of communications from online service providers and other documents stored online.[110] The bill is viewed as a victory for user privacy because it codified the Sixth Circuit's ruling in *Warshak v. United States*, which required the government to first obtain a warrant before accessing emails stored with cloud service providers. But, it is also viewed as long overdue—and far from perfect.[111] Proponents of broader civil liberties seek stricter notification requirements from the government when requesting disclosure of information after seeking a warrant, as well as changes requiring the government to obtain a warrant when demanding a person's geolocation data.[112]

106. Wiretap Act, 18 U.S.C. § 2511 (2017); *see* Nardone v. United States, 308 U.S. 338, 340 (1939).

107. Pen Register Act, 18 U.S.C. § 3121 (2017).

108. Stored Communications Act, 18 U.S.C. § 2703(d) (2016).

109. U.S. CONST. amend. IV.

110. Email Privacy Act of 2016, H.R. 699, 114th Cong. (2015).

111. Sophia Cope, *House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform*, ELECTRONIC FRONTIER FOUND. (Apr. 27, 2016), https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform; *see* Warshak v. United States, 532 F.3d 521, 525–27 (6th Cir. 2008) (holding that compelled disclosures of e-mails without a warrant violate the Fourth Amendment and Stored Communications Act).

112. Cope, *supra* note 111.

B. CAUSE AND EFFECT: WHAT IS THE CAUSE OF THESE DIFFERENT VIEWS AND HOW IS IT AFFECTING OUR LAWS?

International data processing requires multinational companies doing business to comply with as many laws as are applicable to territories where they do business. For example, any information made available on the Internet is subject to every jurisdiction possible, over 190 countries, each with different federal and state laws.[113]

Different connotations for different definitions often contribute to the problem.[114] Certain terms may appeal to one audience and completely turn off another. For example, it seems that European attitudes toward privacy hinge specifically on the illusion of greater protection under a sweeping data protection directive with significant restrictions, when in practice, many companies in Europe collect and process equal amounts of personal data as their competitors in other parts of the world.[115] In fact, after much scrutiny over the Safe Harbor provision and the new Privacy Shield, not much has changed other than the illusion of stricter rules.

Due to a principal hostility toward the processing of personal data and maintaining databases, Europeans feel more in control of their information when European companies process personal data only upon consent of the data subject, or through a statutory exemption allowing the processing to occur.[116] However, despite vastly different approaches to data protection, research confirms that there is a rift between regulation on the books and the reality of on-the-ground corporate behavior.[117] For example, the rising number of Chief Privacy Officers in U.S. corporations suggests an increase in corporate attention to privacy in the states.[118] In fact, U.S. and German companies have been shown to have similarly robust privacy practices.[119] This suggests that if U.S. companies need a powerful and relatively autonomous professional privacy officer at the top level, why shouldn't our government as well?

IV. THE FUTURE OF PRIVACY IN THE UNITED STATES

American companies' attitudes towards privacy rights have already begun to transform. Groups like the Electronic Frontier Foundation ("EFF") track which companies "will stand by users, insisting on transparency and strong legal standards around government access to

113. DETERMANN, *supra* note 8, at 6–7.
114. *Id.* at XIII.
115. *Id.* at 5.
116. *Id.*
117. BAMBERGER & MULLIGAN, *supra* note 30, at 241.
118. *Id.*
119. *Id.*

user data[.]"[120] The EFF creates a report to assess company practices and policies using five evaluation criteria, including whether the company in question:

> (1) follows industry-accepted best practices (considering whether the company requires the government to obtain a warrant before handing over content, whether the company publishes a transparency report, and whether the company publishes law enforcement guides explaining how they respond to data demands);
>
> (2) tells users about government data requests;
>
> (3) publicly discloses the company's data retention policies;
>
> (4) discloses the number of government content removal requests and compliance with such requests; and
>
> (5) has pro-user public policies, such as opposing backdoors.[121]

"[N]ine companies earned stars in every category that was available to them: Adobe, Apple, CREDO, Dropbox, Sonic, Wickr, Wikimedia, Wordpress.com, and Yahoo."[122] Other major findings include that: "AT&T, Verizon, and WhatsApp Lag Behind Industry in Standing by Users," and an "Overwhelming Majority of Tech Companies Oppose Government Mandated Backdoors."[123] When this report commenced in 2011, Google was the only company to satisfy three categories, and only six out of thirteen companies satisfied just one of the five categories.[124] However, in 2015, twenty-one out of twenty-five companies satisfy three or more categories.[125] It is important that this progression toward increased transparency continues.

Many intermediaries such as Apple, Google, and Microsoft have already begun to fight government overreach in accessing their users' information after being "[s]tung by Mr. Snowden's revelations about how the National Security Agency had secretly breached company networks—often without the companies' knowledge."[126] In one instance, the Justice Department demanded Apple turn over text messages from suspects' iPhones pursuant to a court order.[127] Apple responded by stating that its iMessage system was encrypted and the company could not comply even if they wanted to.[128] Apple set an example with its

120. NATE CARDOZO ET AL., WHO HAS YOUR BACK? THE ELECTRONIC FRONTIER FOUNDATION'S FIFTH ANNUAL REPORT ON ONLINE SERVICE PROVIDERS' PRIVACY AND TRANSPARENCY PRACTICES REGARDING GOVERNMENT ACCESS TO USER DATA 4 (2015).

121. *Id.* at 5–7.

122. *Id.* at 7.

123. *Id.*

124. *Id.* at 67.

125. *Id.* at 13.

126. Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S. over Data Access*, N.Y. TIMES (Sept. 7, 2015), http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html.

127. *Id.*

128. *Id.*

commitment to user privacy rights through encryption of sensitive data, although they "and other companies had privately expressed willingness to find common ground."[129] Timothy Cook, CEO of Apple, stated that there is "another attack on our civil liberties that we see heating up every day—it's the battle over encryption . . . . We think this is incredibly dangerous."[130] Similarly, Microsoft argued that since its data is stored around the world, U.S. firms should be relieved from turning it over.[131] The government won in a federal district court, arguing that where the data is stored is irrelevant because the company still has control over email records.[132]

Regardless of the amount of discretion American businesses have in disclosing certain types of information, the government may generally compel these providers to disclose information if they are able to obtain a warrant. The amount of personal information intermediaries collect creates a huge responsibility—they must choose how much information to collect and the scope of use they will reserve regarding that information. When companies seek to profit from targeted advertising, data must be retained, thereby opening up potential risk to the users of compelled disclosure by the government, shedding any anonymity maintained by the service provider.

The court decisions in the following cases reflect the circumstances U.S. courts deem to constitute an unreasonable intrusion into an individual's privacy. First, in *In re iPhone Application Litigation*, a Northern District of California court found disclosure of information that included a device identifier number to constitute personal data. The court further found that the disclosure of geolocation information did not constitute "an egregious breach of social norms," even if the information was transmitted without consent.[133] In *United States v. Jones*, the Supreme Court determined that a vehicle was considered a personal effect, therefore, using a GPS to track the location of a car constitutes a search.[134] However, while there is no expectation of privacy on a public thoroughfare, there is a reasonable expectation of privacy in the information created by the aggregate points of data—and, as mentioned previously, attitudes are changing with respect to what society demands that courts recognize as private.[135]

Similarly, in *Smith v. Maryland*, the Court found no legitimate expectation of privacy regarding the collection of numbers dialed on a

129. *Id.*
130. *Id.*
131. *Id.*
132. *Id.*
133. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012).
134. United States v. Jones, 565 U.S. 400, 404 (2012).
135. *Id.*

phone.[136] The Court also found that a search and seizure of the information gathered by a pen register could not qualify as a warrantless search within the meaning of the Fourth Amendment because pen registers only collect call records, not content.[137] Likewise, in *Riley v. California*, the Court held that the police must get a warrant before searching a cell phone seized incident to an arrest because of the enormous dearth of information, such as additional contact information, that is stored in cell phones.[138] Additionally, in *Gonzalez v. Google*, a government request for URL samples was granted, where a request for specific search queries was not.[139]

If the United States would like to be seen as a populace invested in protecting privacy, the current reliance on public pressure created by breach laws or high-profile investigations with only occasional regulatory enforcement action will not suffice.[140] In a post-Snowden era, the visible shift in the landscape of the corporate world reflects much needed changes in the expectations of our government. The FTC's status as a de facto Data Protection Authority in the United States is no longer acceptable. The FTC has broad authority under section 5 of the FTC Act to enforce violations against unfair or deceptive trade practices may give the FTC some authority, but the ability to remedy violations is lacking.[141] Even if the FTC was granted authority to do more than just issue consent decrees and wait for violations of those orders to issue fines, the FTC still lacks resources. The FTC lacks the necessary manpower, and most importantly, the FTC lacks sufficient independence from our government. In any event, the implementation of detailed mechanisms for redress, arbitration, and appeal is one of the most significant changes reflected in the Privacy Shield. American citizens must not become complacent. Americans must petition Congress to take initiative in bolstering our own enforcement authorities.

Even privacy professionals who have been analyzing the future of the Privacy Shield seem to be unclear themselves as to the effect of the textual changes promising enforcement. "One of the big novelties of the Privacy Shield is its intricate system of oversight, enforcement and redress," says European Certified Information Privacy Professional

136. Smith v. Maryland, 442 U.S. 735, 745 (1979); *see Ex parte* Jackson, 96 U.S. 727, 733 (1877) (holding that the outward information on a mail package such as an address or the weight is not subject to any expectation of privacy).

137. *Smith*, 442 U.S. at 746.

138. Riley v. California, 134 S. Ct. 2473, 2493–95 (2014); *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 388 (5th ed. 2014) (discussing the FBI's discontinued use of "Carnivore" software, which was used to intercept e-mail and instant messaging information while scanning headers to identify senders and recipients in order to filter out irrelevant Internet service provider users).

139. Gonzales v. Google, Inc., 234 F.R.D. 674, 678 (N.D. Cal. 2006).

140. BAMBERGER & MULLIGAN, *supra* note 30, at 221.

141. Federal Trade Commission Act, ch. 311, 5 Stat. 719 (current version at 15 U.S.C. § 45(a)).

Eduardo Ustaran, which "reflects the complexities of this issue and shows us a pattern for the future."[142] Ustaran ultimately concludes with the age old adage that only "[t]ime will tell how workable this is," while still remaining confident that efforts in creating a credible system have been made.[143] Despite significant reforms made by the Obama administration post-Snowden, and surviving the adequacy decision of the European Commission Data Protection Authorities continue to question the adequacy of the Privacy Shield. Of particular importance to the Privacy Shield's survival, says one European Commission Spokeswoman, is "Presidential Policy Directive No. 28 (PPD-28) – and Obama era reform which extended privacy protections to foreigners."[144] This indicates that companies may be better off relying on alternative mechanisms to overcome the "third hurdle" in order to ensure legal compliance when processing any transatlantic data. Ultimately, this illustrates how the text of the Privacy Shield agreement may not be the real issue, especially in light of the recent change in administration, "it could take just a single stroke of Trump's pen to bring the entire arrangement toppling down."[145] In reality, the Data Protection Authorities are looking for meaningful reform through action, such as refining the surveillance process to narrow targeting efforts, as was the intent of Presidential Policy Directive 28 and the USA Freedom Act.[146]

CONCLUSION

Although there are many lessons that can be learned from the attempt to resolve differences in cultural expectations through the example of the transition from the Safe Harbor to the Privacy Shield, one thing is particularly clear: As individual data subjects begin to feel a loss of control over their data, they will look to increase regulation. When the loss of control is paired with a general feeling of distrust in one's government, individuals must move toward smarter regulation rather than piling more obligations onto businesses, and focus reform on substance rather than appearance.

142. Eduardo Ustaran, *Privacy Shield: The Bigger Picture*, INT'L ASS'N OF PRIVACY PROFS. (Mar. 10, 2016), https://iapp.org/news/a/privacy-shield-the-bigger-picture/.

143. *Id.*

144. Natasha Lomas, *EU-US Privacy Shield Remains Precariously Placed*, TECH CRUNCH (Apr. 6, 2017), https://techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed/.

145. *Id.*

146. Meyer, *supra* note 78.

***