PLAYING OFF-KEY: TRANS-ATLANTIC DATA REGULATION IN A DISCORDANT WORLD

I. INTRODUCTION 793
II. BACKGROUND 798
A. *Regional Data Privacy Differences in the United States and the European Union* 799
B. *The Trans-Atlantic Data Transfer Dilemma* 800
1. The Safe Harbor Framework 801
2. The Safe Harbor is Invalidated in *Schrems v. Facebook* 802
3. Interim Business Solutions 804
C. *The Threat of Extraterritorial Jurisdiction* 809
III. ANALYSIS: REGIONAL HARMONIZATION IS NOW A FEASIBLE, LONG-TERM SOLUTION 811
A. *The Lack of a Safe Harbor Encourages Regional Harmonization* 812
B. *U.S. Opinion Demonstrates Interest in Change* 813
1. Growing Recognition that the Notice and Consent System is Flawed 814
2. The Class Action Lawsuit Against Google's Data-Mining of All Gmail Content 816
3. There Are Numerous Proposals for Updating U.S. Law 818
i. Improve Privacy Self-Management 818
ii. Regulate Data Use Rather than Data Collection 819
iii. Establish Clear Due Process Requirements for Digital Transaction Surveillance 821
C. *Shared Economic and Security Imperatives Encourage Regional Harmonization* 824
D. *Harmonization Does Not Require Mirror Image Frameworks* 827
IV. CONCLUSION 828

I. INTRODUCTION

Do you think the Federal Bureau of Investigation ("FBI") should be able to access the data on your iPhone? According to Apple's Chief Executive Officer ("CEO") Tim Cook, there's likely "more information about you on your phone

than there is in your house."[1] From step-tracking apps to banking and social media accounts, a smartphone contains records of all one's calls, text messages, contacts, calendar events and reminders, emails, photos, and internet browsing history.[2] Indeed, smartphones have transformed from audio call devices into "digital repositories for the most intimate details of [one's] life."[3] This is one of the many reasons why Apple's refusal to create a new operating platform through which the FBI can access a terrorist's encrypted iPhone is being hotly debated.[4] The "FBiOS" could then be exploited to hack into anyone's iPhone.[5] Every iPhone user's data would be vulnerable.[6]

The Apple-FBI encryption debate may first appear to be purely domestic in nature, but it has international implications. First, Apple is an international business that sells the same model iPhones worldwide.[7] So any "backdoor"[8] it creates would operate globally. Second, Apple has already faced demands from other countries, like China, to decrypt iPhones on demand.[9] Any concession by

---

1 Chris Strohm, *Your Smartphone Knows Who You Are and What You're Doing*, BNA BLOOMBERG PRIVACY L. WATCH (Feb. 29, 2016, 5:00 AM), http://www.bloomberg.com/news/articles/2016-02-29/your-smartphone-knows-who-you-are-and-what-you-re-doing.

2 *Id.*

3 *Id.*

4 For an overview of the litigation between the FBI and Apple, see *The FBI vs. Apple*, WALL ST. J. (Feb. 19, 2016, 10:17 AM), http://www.wsj.com/articles/the-fbi-vs-apple-1455840721.

5 Julia Angwin, *What's Really at Stake in the Apple Encryption Debate*, PROPUBLICA (Feb. 24, 2016, 4:29 PM), https://www.propublica.org/article/whats-really-at-stake-in-the-apple-encryption-debate ("Apple says the FBiOS would 'be relentlessly attacked by hackers and cybercriminals' hoping to obtain a copy of the golden key."); Brian Barrett, *The Apple-FBI Fight Isn't About Privacy vs. Security. Don't Be Misled*, WIRED (Feb. 24, 2016, 7:00 AM), http://www.wired.com/2016/02/apple-fbi-privacy-security/ ("It would be great if we could make a backdoor that only the FBI could walk through . . . [b]ut that doesn't exist. And literally every single mathematician, cryptographer, and computer scientist who's looked at it has agreed.").

6 Barrett, *supra* note 5 ("[T]he way computer security works means that it has to be absolute. Any precedent that says a company can be compelled to weaken its security will have injurious consequences, full stop. There are no shades of grey, no matter what politicians and law enforcement might suggest.").

7 *See* Benjamin Mayo, *All iPhone 6s and iPhone 6s Plus Models Now Sold Out Worldwide Ahead of Friday Launch*, 9TO5MAC (Sept. 21, 2015), http://9to5mac.com/2015/09/21/iphone-6s-iphone-6s-plus-sold-out-worldwide/.

8 In this case, the "backdoor" the FBI is seeking is an override to the iOS feature in which all local data on an encrypted iPhone is erased after ten incorrect passwords are entered on the device. *The FBI vs. Apple*, *supra* note 4.

9 Danny Yadron et al., *Inside the FBI's Encryption Battle with Apple*, THE GUARDIAN (Feb. 18, 2016, 1:00 AM), http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple ("[Apple CEO] Cook, who has managed threats from China to force decryption of the iPhone, had taken unyielding stances against backdoors, both in the US and overseas, where a host of foreign countries are debating . . . measures to give their security services access to customer data from Apple and other firms.").

Apple to similar U.S. demands threatens their ability to withstand those demands internationally.[10] Finally, the decryption demand follows the recent demise of the U.S.-EU Safe Harbor agreement that governed trans-Atlantic data transfers for the past 15 years.[11] The Safe Harbor was invalidated precisely because the arrangement permitted U.S. government and law enforcement agencies too much freedom in accessing data transferred to U.S. companies.[12] Should Apple create the backdoor that the FBI is demanding—capable of decrypting and providing government access to any iPhone worldwide—then it will likely endanger any hope either region has of reaching an agreement permitting trans-Atlantic data transfers.

For the past 15 years, trans-Atlantic data transfers were conducted via a Safe Harbor agreement between the United States and the EU.[13] The Safe Harbor permitted data transfers to self-certified U.S. companies that provided privacy protections equivalent to European law despite lower U.S. requirements, essentially overriding an EU ban on data transfers to countries with lower data protection.[14] The resulting trans-Atlantic data transfers (which rank as the highest

---

10 *Id.*

11 The Safe Harbor was established in 2009 and was "the primary—and often sole—mechanism under which more than 4,400 companies of all sizes, and across all industries, legally transferred data from Europe to the United States for the past 15 years." *After Safe Harbor: EU-US Privacy Shield*, INFO. TECH. INDUSTRY COUNCIL, http://www.itic.org/safeharbor (last visited Oct. 3, 2016). The Safe Harbor was invalidated by the Court of Justice of the European Union ("CJEU") in October 2015. Natalia Drozdiak & Sam Schechner, *EU Court Says Data-Transfer Pact With U.S. Violates Privacy*, WALL ST. J. (Oct. 6, 2015, 1:42 PM), http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361. The Apple-FBI encryption debate became a publicly-debated issue during February 2016, just as EU authorities began considering a prospective replacement trans-Atlantic data transfer agreement. *The FBI vs. Apple*, *supra* note 4; Stephen Gardner, *Art. 29 Working Party Cautious on Privacy Shield Deal*, BLOOMBERG BNA (Feb. 4, 2016), http://www.bna.com/art-29-working-n57982066965/. That agreement is still dependent on U.S. authorities having only limited, necessary, and proportionate data access. Gardner, *supra*. (emphasizing that the EU regulatory authorities will need to evaluate the prospective deal for four essential guarantees, including government access "governed by the principles of necessity and proportionality"). The Apple-FBI debate threatens the credibility of U.S. claims that this essential guarantee will be honored. *See* Stephanie Bodoni, *Apple's-FBI Clash Risks Piercing EU-US Privacy Shield*, BLOOMBERG BNA ELECTRONIC COM. & L. REP. (Mar. 8, 2016, 5:59 AM), http://www.bloomberg.com/news/articles/2016-03-08/apple-s-clash-with-fbi-risks-piercing-trust-in-eu-privacy-shield.

12 *See infra* notes 56–57 and accompanying text.

13 *After Safe Harbor: EU-US Privacy Shield*, *supra* note 11.

14 The EU prohibits data transfers to countries with protections below their strict requirements. Ivana Kottasova, *Europe's Big Data Bombshell: What You Need to Know*, CNN MONEY (Oct. 6, 2015, 2:41 PM), http://money.cnn.com/2015/10/06/news/companies/safe-harbor-data-privacy-europe/ ("Europe has strict rules to protect data, and doesn't allow it to be transferred to any country that does not adhere to them."). Because the United States did not have a comprehensive data privacy law that provided similar protections to that of the EU, the Safe Harbor framework was

cross-border transfer rate worldwide) support an increasingly interdependent trans-Atlantic digital economy.[15] Seventy-five percent of all products traded and delivered online are attributable to the combined digital economies of the United States and the EU;[16] they are each other's largest trading partners in digitally deliverable services;[17] and the services imported from one region are frequently incorporated into the other's exports.[18] But the Safe Harbor permitting these trans-Atlantic data transfers was invalidated by the Court of Justice of the European Union ("CJEU") in its *Schrems v. Facebook*[19] decision in October 2015, endangering the business practices of over 4,500 U.S. companies[20] and half a trillion dollars of trans-Atlantic trade and other digitally deliverable services.[21]

While there are interim solutions that businesses can use in the absence of the Safe Harbor framework, these are threatened by the United States'

negotiated to permit trans-Atlantic data transfers on the "basis that the transfers [were] done in accordance with privacy principles similar to those contained in the EU Data Protection Directive (95/46/EC)." Jabeen Bhatti, *Commerce Official: U.S.-EU Safe Harbor Vital Because "Huge Economic Interests at Stake"*, BLOOMBERG BNA PRIVACY & DATA SECURITY L. RESOURCE CTR. (May 12, 2015), http://www.bna.com/commerce-official-useu-n17179926398/.

15 JOSHUA P. MELTZER, BROOKINGS INST., THE IMPORTANCE OF THE INTERNET AND TRANSATLANTIC DATA FLOWS FOR U.S. AND EU TRADE AND INVESTMENT 4 (2014), https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf ("The most significant economic relationship for the U.S. and Europe is the one they share; each is the other's largest markets for goods and services."); *see also Remarks for TABC Conference: Perspectives on the EU's Digital Single Market Strategy—The Transatlantic Perspective*, U.S. MISSION TO THE EUROPEAN UNION (Sept. 15, 2015) [hereinafter U.S. MISSION TO THE EUROPEAN UNION], http://useu.usmission.gov/text91715.html.

16 U.S. MISSION TO THE EUROPEAN UNION, *supra* note 15.

17 *Id.*

18 *Id.* ("53 percent of digitally deliverable services imported from the U.S. (including consulting, engineering, design, and financial services) were used in the production of EU exports, and 62 percent of digitally deliverable services imported from the EU were incorporated into U.S. exports.").

19 Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 ECLI 650, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=702383.

20 Drozdiak & Schechner, *supra* note 11.

21 Shannon Taylor, *It's Clear the U.S. and EU Economies Need a Safe Harbor 2.0*, INFO. TECH. INDUSTRY COUNCIL TECHWONK BLOG (Nov. 4, 2015), http://www.itic.org/news-events/techwonk-blog/its-clear-the-us-and-eu-economies-need-a-safe-harbor-20. The trans-Atlantic digital economy has grown substantially, growing from billions to trillions of dollars in just the past three years alone. *See, e.g.*, MELTZER, *supra* note 15, at 1 ("In 2012, the U.S. exported $140.6 billion worth of digitally deliverable services to the EU and imported $86.3 billion worth. U.S. exports of digitally deliverable services to the EU comprise 72 percent of bilateral services exports, compared with 55 percent of exports to Asia and Latin America.").

willingness to use extraterritorial jurisdiction to access data stored overseas.[22] To sustain trans-Atlantic data transfers in the long-term, the United States and EU must harmonize their data privacy frameworks. Right now, the sharp differences between the regional frameworks produce a level of discord similar to the grating sounds of a musical performance without harmony. This striking discord between the United States and the EU was mitigated by the Safe Harbor framework, but its recent demise removed that single harmonizing note and made the regional discord worse.

Legal scholars have historically discarded proposals to harmonize U.S. and EU data privacy regulation as impossible because of the large gap between the frameworks and each region's deep commitment to their approach.[23] But this Note demonstrates that the idea of regional harmonization is much more feasible than it was in the past, and it should no longer be discarded as an inviable option.

This Note argues that regional harmonization is now a much more feasible long-term solution for four reasons: (1) the lack of a Safe Harbor permitting trans-Atlantic data transfers creates an incentive that did not previously exist, (2) the change in U.S. public opinion regarding data privacy demonstrates an interest in changing its framework, (3) the regions share economic and security imperatives that encourage harmonization, and (4) the regions do not need mirror image frameworks to achieve harmonization.

This Note will demonstrate this thesis by first providing a high-level overview of the differences between the U.S. and EU data privacy frameworks and the current trans-Atlantic data transfer dilemma in Part II. Section II.A will provide an overview of the differences between the regional data privacy frameworks. Section II.B will discuss the Safe Harbor framework, its invalidation by the CJEU in *Schrems v. Facebook*, and the interim solutions businesses may use until the regulatory environment is clearly defined. Section

---

22 *See* discussion *infra* Part II.C. Extraterritoriality refers to the "applicability or exercise of a sovereign's laws outside its territory." *Extraterritoriality*, DICTIONARY.COM, http://www.dictionary.com/browse/extraterritoriality (last visited Nov. 1, 2016). For further information on its scope and the various jurisdictional principles it may follow (including the protective principle, universality principle, passive personality principle, and effects jurisdiction), see MARK WESTON JANIS & JOHN E. NOYES, INTERNATIONAL LAW CASES AND COMMENTARY 909–25 (5th ed. 2014).

23 *See* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 881 (2014) (discarding the idea of regional harmonization as a viable solution to the trans-Atlantic dilemma because "[a]ttempts to harmonize U.S. and EU privacy law by turning EU privacy law into a U.S.-style approach, or vice versa, are unlikely to succeed. . . . [as] [b]oth the United States and European Union are deeply committed to their respective approaches"). Professor Daniel Solove is a particularly well respected legal scholar in the area of privacy who has written more than 10 books and 50 articles in the area. *See* DANIEL SOLOVE, https://www.danielsolove.com/bio/ (last visited Nov. 3, 2016). He even founded a company called TeachPrivacy that focuses on privacy and data security training. *Id.* He currently serves as the John Marshall Harlan Research Professor of Law at the George Washington University Law School. *Id.*

II.C will discuss how these interim solutions are threatened by the potential extraterritorial application of U.S. or EU law. Then, Part III will discuss the four reasons why regional harmonization is a much more feasible long-term solution than it was historically regarded.

First, the lack of a Safe Harbor permitting trans-Atlantic data transfers creates an incentive to harmonize that did not previously exist; particularly considering the weight businesses with trans-Atlantic data processes will place on the cost-saving benefits of complying with a streamlined set of harmonized regulations against the costly and duplicative processes required to be compliant with two divergent regional frameworks.

Second, regional harmonization is much more feasible because changing U.S. public opinion regarding data privacy is indicative of a willingness to revise its framework. This willingness to change the current framework is visible in three ways. One, there is a significant push for a more meaningful and nuanced form of consent than the current "notice and consent" or "privacy self-management" framework presents. Two, the growing dissatisfaction with the current framework is evident in the class action lawsuit against Google for its practice of data-mining all Gmail content. Three, there are numerous proposals to update the framework, including proposals to improve privacy self-management, regulate data use rather than data collection, and establish clear due process requirements for digital transaction surveillance. Each of these proposals, combined with the other two indicators of increasing discontent with the current system, demonstrate the United States' growing willingness to revise its current data privacy framework.

Third, the regions share economic and security imperatives that encourage regional harmonization. Fourth, regional harmonization does not require that the United States and the EU have frameworks that mirror each other exactly. Part IV will conclude.

II. BACKGROUND

To understand why regional harmonization should now be considered a viable long-term solution, one must first understand why trans-Atlantic data transfers are at risk. This part will provide a high-level overview of regional data privacy differences in the United States and the EU and the current trans-Atlantic data transfer dilemma. Section A will provide an overview of the differences between the regional data privacy frameworks, while Section B will discuss the Safe Harbor framework, its invalidation by the CJEU in *Schrems v. Facebook*, and the interim solutions businesses may use until the regulatory environment is clearly defined. Section C will discuss how the risk of extraterritorial jurisdiction threatens these interim solutions.

A. Regional Data Privacy Differences in the United States and the European Union

The regional differences between data privacy frameworks in the United States and the EU first became apparent when the EU passed the Data Protective Directive in 1995, and has become more distinct over time.[24] The best summary of these differences is perhaps the six variances Professor Ioanna Tourkochoriti identified between data privacy regulation in the United States and the EU:

> (1) Fundamental Presumptions: Personal data cannot be processed in the EU without a legal basis, whereas it is presumed permissible in the United States unless limited by law.[25] U.S. plaintiffs must prove an actual harm to be successful, whereas EU plaintiffs do not.[26]
> (2) Contractual Limits: EU citizens cannot contract their privacy rights away, whereas U.S. law permits individuals to do so via various user and licensing agreements.[27] This is true even if an EU citizen unambiguously consents to such agreements.[28]
> (3) Protective Coverage: U.S. law offers limited data protections through a sector-by-sector regulatory approach, whereas the EU has a comprehensive framework that requires data protections to "be adequate, relevant and not excessive in relation to the purposes for which they are processed" and that those purposes are "specified, explicit and legitimate."[29]
> (4) Weight of Conflicting Values: Privacy is a fundamental right on par to freedom of expression in the EU; whereas it is an interest that is often secondary to more explicit constitutional rights, like freedom of speech, in the United States.[30]
> (5) Definitions: In the EU, personal data includes any information that is identifiable to a person (meaning the

---

24 MARTIN A. WEISS & KRISTIN ARCHICK, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD, CONGRESSIONAL RESEARCH SERVICE 3 (2016).

25 Ioanna Tourkochoriti, *The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection*, 36 U. ARK. LITTLE ROCK L. REV. 161, 164 (2014).

26 *Id.*

27 *Id.* at 164–65.

28 *Id.*

29 *Id.* at 166.

30 *Id.* at 167.

data could be linked to a person even if it is not at the moment), whereas personally identifiable information in the United States is limited to data that is directly linked to an individual.[31]

(6) Enforcement: Each member-state of the EU has an independent authority dedicated to data protection, empowered to investigate violations and also monitor technology and business practices for data privacy impacts to which the EU legal framework must respond; whereas the United States has yet to establish a similarly dedicated agency, although the Federal Trade Commission has increased its role in data protection.[32]

As these six variants indicate, there are significant differences in the breadth, scope, and depth of the data protections offered in the United States and the EU. But it is common for there to be variations in the legal frameworks of different countries; the trans-Atlantic data transfer dilemma is unique because it arose when the EU prohibited transfers to countries that did not offer an equitable level of protection, and the United States was found to offer insufficient data protection.[33]

B. The Trans-Atlantic Data Transfer Dilemma

Personal data can only be transferred from the EU to a third country, such as the United States, when that country's domestic law or international commitments "ensure[] an adequate level of protection."[34] The United States was one of many countries that did not provide sufficient legal protection for personal data,[35] so the EU collaborated with the United States to develop a "Safe Harbor" framework through which data transfers would be permitted.[36] That framework

---

31 *Id.* at 168. *See generally* Schwartz & Solove, *supra* note 23, at 891–904 (discussing these definitional differences in significant detail).

32 Tourkochoriti, *supra* note 25, at 168, 172.

33 *See supra* note 12 and accompanying text.

34 Court of Justice of the European Union Press Release 117/15, The Court of Justice Declares that the Comm'n's US Safe Harbour Decision is Invalid 1 (Oct. 6, 2015) [hereinafter CJEU Declares Safe Harbor Invalid].

35 *See Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited Nov. 1, 2016) (recognizing only the following countries as providing adequate protection: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay).

36 *US-EU Safe Harbor Under Pressure*, IAPP PRIVACY TRACKER (Aug. 2, 2013), https://iapp.org/news/a/us-eu-safe-harbor-under-pressure (noting that the Safe Harbor was negotiated by U.S. and EU officials "who recognized the need for cross-border data transfers

was formally approved in EU Commission Decision 2000/520/EC on July 26, 2000.[37]

1. The Safe Harbor Framework

The Safe Harbor permitted companies to exchange data internationally by self-certifying that they met the privacy standards of the EU, even though they were not required to meet those standards under U.S. regulations.[38] The representations of these self-certifying companies were to be validated, and the parameters of the Safe Harbor enforced, by the Federal Trade Commission.[39] The program came under scrutiny after the Edward Snowden leaks revealed the expansive U.S. surveillance system that encompassed EU citizens.[40]

On November 27, 2013, the EU Commission sent a communication to the United States regarding the "[f]unctioning of the Safe Harbo[]r from the [p]erspective of EU [c]itizens and [c]ompanies [e]stablished in the EU."[41] In that communication, the EU Commission expressed doubts about the enforcement of the Safe Harbor requirements in the United States and mandated that the United States adopt 13 recommendations to increase transparency.[42] Examples of such improvements included requiring public disclosure of the privacy policies of self-certified companies (with links to the Department of Commerce's list of current Safe Harbor members), public disclosure of privacy conditions within subcontractor agreements, and public disclosure of all former Safe Harbor participants with expired self-certifications on the Department of Commerce website.[43]

The EU Commission also demanded greater enforcement by U.S. agencies, including "ex officio investigations of effective [privacy policy] compliance" of self-certified companies after initial or renewed certification, follow-up investigations within one year of compliance violations, notification to the relevant EU data protection authority whenever there is a complaint or

despite the EU's position that the United States does not provide adequate protection for the personal data of EU data subjects").

37 Commission Decision 2000/520/EC of July 26, 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) 7.

38 Bhatti, *supra* note 14.

39 *Id.*

40 *Id.*

41 *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM (2013) 0847 final (Nov. 17, 2013).

42 *Id.* at 18–19.

43 *Id.* at 18.

investigation into a self-certified company, and mandatory investigations of false Safe Harbor membership claims.[44] Finally, the EU Commission demanded that self-certified companies publish the extent to which U.S. authorities could collect and process data transferred under the Safe Harbor and that any such collections for national security purposes be limited to what is strictly necessary or proportionate.[45] The EU Commission emphasized that the Safe Harbor could be suspended if these concerns were not addressed.

The communication was effective: U.S. enforcement agencies showed increased interest in enforcing Safe Harbor certification requirements. The Federal Trade Commission settled charges of Safe Harbor certification status misrepresentations with 13 companies.[46] But it also sparked fears that the Safe Harbor could be suspended.[47] One EU law student, Maximillian Schrems, even filed a lawsuit against the data protection commissioner in Ireland challenging the Safe Harbor Framework.[48]

2. The Safe Harbor is Invalidated in *Schrems v. Facebook*

Mr. Schrems's lawsuit began as a complaint with the Irish Data Protection Commissioner, alleging that his personal data on Facebook was not sufficiently protected under the Safe Harbor framework because Edward

---

[44] *Id.* at 19.

[45] *Id.* The European Court of Human Rights does not consider the term "necessary" synonymous with "indispensable." ELECTRONIC FRONTIER FOUNDATION, NECESSARY & PROPORTIONATE: INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS LAW TO COMMUNICATIONS SURVEILLANCE 20 (2014), http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf. Nor does it consider it "as flexible as the terms 'admissible,' 'ordinary,' 'useful,' 'reasonable,' or 'desirable.'" *Id.* It is instead very similar to the principle of necessity and proportionality used by the UN Human Rights Committee, which has held that:

> it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them. Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; *they must be the least intrusive instruments amongst those, which might achieve the desired result*; and they must be proportionate to the interest to be protected.

Id.

[46] *FTC Reaches Settlement with Thirteen Companies over Safe Harbor Misrepresentations*, HUNTON & WILLIAMS: PRIVACY & INFO. SECURITY L. BLOG (Aug. 19, 2016), https://www.huntonprivacyblog.com/2015/08/19/ftc-reaches-settlement-thirteen-companies-safe-harbor-misrepresentations/.

[47] *Microsoft Warrant Challenge Could Alter U.S.-E.U. Data Pact*, PEPPER HAMILTON LLP (June 8, 2015), http://www.pepperlaw.com/publications/microsoft-warrant-challenge-could-alter-us-eu-data-pact-2015-06-08/.

[48] Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 ECLI 650, http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=244813.

Snowden had revealed how easily intelligence services could access data transferred to the United States under the Safe Harbor framework.[49] The Data Protection Commissioner rejected his complaint on the ground that the EU Commission had already determined that the United States met the requisite privacy standards when it approved the Safe Harbor framework in 2000.[50] When Mr. Schrems appealed to the High Court of Ireland, the High Court asked the Court of Justice of the European Union ("CJEU") whether the EU Commission's decision prevented national supervisory authorities from independently investigating whether a third country provides an adequate level of protection per the Data Protection Directive and potentially suspending data transfers when those standards are not met.[51]

On October 6, 2015, the CJEU held that national supervisory authorities must be able to conduct such independent assessments and therefore declared the Safe Harbor invalid.[52] First and foremost, the CJEU held that national supervisory authorities "must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive."[53] While the national supervisory authority cannot declare the EU Commission's decision invalid—this can only be done by the CJEU—it must be able to conduct an independent investigation and initiate domestic proceedings that may be referred to the CJEU for a final decision.[54]

Second, the CJEU held that the Commission Decision authorizing the Safe Harbor was invalid because U.S. public authorities were not bound by it.[55] It permitted "national security, public interest and law enforcement requirements of the United States [to] prevail over the safe harbo[]r scheme, so that United States [businesses] are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements."[56] Because the Safe Harbor framework did not include a strict necessity limit on government access and it did not include legal remedies for individuals to "have access to personal data relating to him, or to obtain the rectification or erasure of such data," it did not meet the protective standards guaranteed by the Charter and Data

---

49 CJEU Declares Safe Harbor Invalid, *supra* note 34, at 1.

50 *Id.* (citing Commission Decision 2000/520/EC 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. (L215) 7.).

51 *Id.*

52 *Id.* at 3.

53 *Id.* at 2.

54 *Id.*

55 *Id.*

56 *Id.*

Protection Directive and therefore could not be validly decided by the Commission.[57]

3. Interim Business Solutions

The CJEU's decision does not call for the immediate suspension of data transfers conducted under the Safe Harbor, but it does give national regulators the authority to investigate and suspend data transfers that do not meet the protection standards established in the Charter and EU Privacy Directive.[58] It also creates significant legal risks for the 4,500 companies that have conducted business under the Safe Harbor framework for the past 15 years, including Apple, Google, Microsoft, Amazon, and Facebook.[59]

The Article 29 Working Party, which the EU created to encourage consistency amongst its 28 member-state privacy regulators,[60] issued a public statement following the CJEU's decision declaring "transfers that are still taking place under the Safe Harbor decision after the CJEU judgment are unlawful."[61] It encouraged businesses to immediately review their data transfer mechanisms and emphasized that any legal and technical solutions to the CJEU decision must address the "necessary oversight of access by public authorities, on transparency,

---

57 *Id.* at 3.

58 Drozdiak & Schechner, *supra* note 11.

59 *Id.*

60 The Article 29 Working Party is an independent advisory body on data protection and privacy created under Article 29 of the Directive 95/46/EC. STATEMENT OF THE ARTICLE 29 WORKING PARTY 2 (2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf. It is comprised of "representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission," and its tasks are "described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC." *Id.* It has the authority to "examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives" and "carries out this task by issuing recommendations, opinions and working documents." *Id.* According to Article 30 of the Directive, the Working Party shall:

> (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures; (b) give the Commission an opinion on the level of protection in the Community and in third countries; (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; (d) give an opinion on codes of conduct drawn up at Community level.

Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard To the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 48.

61 STATEMENT OF THE ARTICLE 29 WORKING PARTY, *supra* note 60, at 2.

on proportionality, on redress mechanisms and on data protection rights."[62] But the Working Party also recognized the importance of having a "robust, collective and common position on the implementation of the judgment" and stated that it will give companies until January 2016 to find appropriate solutions for complying with the CJEU judgment before regulators initiate enforcement proceedings.[63]

Although there is a possibility that the regions will be able to create another Safe Harbor framework, it would need to receive approval from all 28 member-state regulators to be effective.[64] In the meantime, there are some alternative solutions that businesses may use.[65] Of course, all of these solutions require time and resources to implement. Large businesses like Amazon, Google, and Facebook will likely be able to weather the storm, but there are many other small and medium-sized businesses amongst the 4,500 impacted by the Safe Harbor's invalidation that may not be so lucky.[66] It is for this reason that the loss of the trans-Atlantic agreement is considered a threat to the "world's largest trading relationship" and the global economy.[67]

Some interim solutions to continue trans-Atlantic business operations without the Safe Harbor include model contracts, binding corporate rules, and dedicated data centers within the EU.[68] Model contracts, which are also known as standard contractual clauses ("SCC"), are template contractual clauses that businesses can create and get pre-approved by EU officials for subsequent use.[69] Of course, businesses will need to invest time and money in first creating these template clauses, soliciting pre-approval by the EU, and then re-papering existing agreements so the model contract language covers current business. Amazon's cloud-computing division has already received approval from the EU for standard contracts.[70] These model contracts will need to govern all data transfers, even if the transfer is between entities within the same multinational

---

62 *Id.*

63 *Id.*

64 *See* Press Release IP/16/216, European Comm'n, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016).

65 These include model contracts, binding corporate rules, and dedicated data centers within the EU. *See* Drozdiak & Schechner, *supra* note 11.

66 *Id.*

67 *Id.*

68 *Id.*

69 *See Model Contracts for the Transfer of Personal Data to Third Countries*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last updated Feb. 12, 2015).

70 Drozdiak & Schechner, *supra* note 11.

company, so a separate legal agreement with this standard contract language may need to be created and signed for each individual data transfer.[71]

An alternative to creating these standard contractual clauses and incorporating them into separate legal agreements governing individual data transfers is to create a single set of binding corporate rules ("BCR") that govern all data transfers between entities within a multinational company. These are internal rules that ensure adequate protection under the EU Privacy Directive, regardless of whether or not the receiving entity within the multinational corporation is located in a country that does not ensure adequate protection.[72] To be valid, the BCR must contain privacy principles like transparency, data quality, and data security; implementation tools like periodic audits, employee training, and a complaint handling system; and evidence that the BCRs are binding on all entities within the multinational company.[73] The Article 29 Working Party hinted in its public statement after the CJEU decision that, even though companies can continue to rely on these compliance mechanisms at the moment, it is possible the effectiveness of these mechanisms will be re-evaluated as the Working Party "continue[s] its analysis on the impact of the CJEU judgment on other transfer tools."[74]

Other businesses, including Google, have elected to avoid the issue entirely by establishing dedicated data centers within the EU. Google announced that it is expanding its data center in Belgium and is building another one in the Netherlands.[75] This is in addition to the data centers it already has in Finland and Ireland.[76] However, this solution is unlikely to remain viable in the long-term

---

71 Model contracts may be used for internal or external data transfers between the United States and the EU. *After Safe Harbor: What To Do Next To Remain Compliant?*, PIERSTONE, http://pierstone.com/after-safe-harbor-what-to-do-next-to-remain-compliant-october-2015/ (last visited Nov. 1, 2016) ("The SCC are suitable for intra-company transfers (e.g. for the transfer of employee or vendor personal data between an EU company and its U.S. mother company) as well as transfers between an EU company and its U.S.-based vendor (e.g. a data center)."). But this standard contractual clause solution only works if the language appears in the relevant contract; it may be necessary for a business to repaper multiple contracts to govern transfers between different entities. *See* HOGAN LOVELLS, INTERNATIONAL DATA TRANSFERS: CONSIDERING YOUR OPTIONS 1 (2015), http://www.hldataprotection.com/files/2015/10/HL-International-Data-Transfers-Considering-your-options.pdf (advising that standard contractual clauses are "[s]uitable for one-off transfers," but "[u]nworkable for multiple and evolving transfers").

72 *See Overview on Binding Corporate Rules*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (last updated Oct. 13, 2016).

73 *Id.*

74 STATEMENT OF THE ARTICLE 29 WORKING PARTY, *supra* note 60, at 1.

75 Drozdiak & Schechner, *supra* note 11.

76 *Id.* Google also plans to build data centers in Singapore, Taiwan, and Hong Kong, but has supposedly avoided building one in China "due to the country's policies regarding content filtering." Rich Miller, *Google to Build Three Data Centers in Asia*, DATA CTR. KNOWLEDGE (Sept.

because it ignores the threatening possibility that either set of regional authorities will exercise extraterritoriality to gain access to the personal information. Both the United States and the EU have expressed a willingness to use principles of extraterritoriality to achieve their aims when companies or their data servers are located outside their territory.[77]

There is a possibility that these issues will be resolved in a second bilateral agreement similar to the Safe Harbor. Tentatively titled the "Privacy Shield," the bilateral agreement is supposed to resolve many of the issues raised by the CJEU when it invalidated the original Safe Harbor.[78] The Article 29 Working Party has promised to evaluate it for the four essential guarantees: (1) "precise rules for processing," (2) government access "governed by the principles of necessity and proportionality," (3) "independent oversight mechanisms," and (4) "effective remedies open to individuals."[79] The Working Party will simultaneously re-evaluate the interim businesses solutions of model contract clauses and business corporate rules against these same standards,[80] which may also be found to offer insufficient data protection.[81]

Some, like Director General John Higgins of DIGITALEUROPE (which represents technology companies such as Apple Inc., Cisco Systems Inc., Google Inc., and Microsoft Corp.), welcomed the announced agreement as a move that would "re-establish a sustainable path for data transfers between the EU and

28, 2011), http://www.datacenterknowledge.com/archives/2011/09/28/google-to-build-three-data-centers-in-asia/.

77 *See infra* Part II.C and its discussion of the CJEU case, *Weltimmo v. Nemzetti*, 2015 ECLI 639, and the U.S. case, *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), *reversed and remanded sub nom. Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016).

78 David Meyer, *Looks Like Data Will Keep Flowing From the EU to the U.S. After All*, FORTUNE (Feb. 2, 2016, 10:19 AM), http://fortune.com/2016/02/02/looks-like-data-will-keep-flowing-from-the-eu-to-the-u-s-after-all/.

79 Gardner, *supra* note 11.

80 *Id.* ("The Art. 29 Working Party had been due to publish the results of an analysis of the impact of the ECJ's ruling on BCRs and SCCs, which might be vulnerable on similar grounds to Safe Harbor. However, the analysis of BCRs and SCCs would be deferred until the Art. 29 Working Party could properly assess the proposed Privacy Shield arrangement, which would likely be done by the end of March.").

81 *Id.* ("Although the court ruling was specific to Safe Harbor, it brought BCRs and SCCs into question on the same grounds of government access to data and lack of redress."); Sam Pfeifle, *Privacy Shield Faces Skepticism in the Marketplace, But Standard Contractual Clauses Pose the Biggest Risk for Market Upheaval*, THE INT. ASS'N OF PRIVACY PROFS. (Aug. 31, 2016), https://iapp.org/news/a/privacy-shield-faces-skepticism-in-the-marketplace-but-standard-contractual-clauses-pose-the-biggest-risk-for-market-upheaval/.

US."[82] But there were others much more critical of the prospective agreement.[83] German lawmaker Jan Philipp Albrecht, for instance, criticized the deal as "little more than a reheated serving" of the Safe Harbor and called it "a joke."[84] Mr. Albrecht is influential because he helped steer the new EU General Data Protection Regulation ("GDPR") through the European Parliament.[85] The GDPR is a significant update to the EU data protection framework that has already been approved but gives businesses two years to become compliant before it becomes active law in 2018.[86] Albrecht criticized the provision prohibiting mass surveillance by the American government as "vague," the creation of an ombudsman to accept European complaints as insufficient, and stated that the proposal is unlikely to withstand CJEU scrutiny.[87]

The Privacy Shield agreement was technically adopted by the European Commission on July 12, 2016.[88] But, it was approved despite the European Data Protection Supervisor advising that "progress compared to the earlier Safe Harbo[]r Decision is not in itself sufficient" and that the "Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court."[89] The Article 29 Working Party expressed similar concerns but agreed not to

---

82 Stephen Gardner, *Safe Harbor Resurrected as EU-U.S. Privacy Shield*, BNA BLOOMBERG PRIVACY & DATA SECURITY L. REP. (Feb. 3, 2016) [hereinafter Gardner, *Safe Harbor Resurrected*], http://www.bna.com/safe-harbor-resurrected-n57982066887/.

83 *See, e.g.*, David Gilbert, *Safe Harbor 2.0: Max Schrems Calls 'Privacy Shield' National Security Loopholes 'Lipstick On A Pig'*, INT'L BUS. TIMES (Feb. 29, 2016, 1:30 PM), http://www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277; Jeff Stone, *Safe Harbor 2.0: Critics Slam US, EU 'Privacy Shield' Data Transfer Deal's Lack Of Details*, INT'L BUS. TIMES (Feb. 3, 2016, 12:17 PM), http://www.ibtimes.com/safe-harbor-20-critics-slam-us-eu-privacy-shield-data-transfer-deals-lack-details-2292287.

84 Gardner, *Safe Harbor Resurrected*, *supra* note 82.

85 *Id.*

86 JAN PHILIPP ALBRECHT, EUR. PARLIAMENT LIBE COMMITTEE, EU GENERAL DATA PROTECTION REGULATION STATE OF PLAY AND 10 IMPORTANT ISSUES 1 (2015), https://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_issues_061115.pdf.

87 *Id.*

88 *The EU-U.S. Privacy Shield*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm (last updated Oct. 13, 2016).

89 EMMA L. FLETT & SHANNON K. YAVORSKY, WORLD DATA PROT. REPORT, MORE ARMOUR REQUIRED BEFORE PUTTING DOWN OUR GUARD? EUROPEAN DATA PROTECTION SUPERVISOR ISSUES OPINION ON PRIVACY SHIELD 2 (2016), https://www.kirkland.com/siteFiles/Publications/World%20Data%20Protection%20Report%20(Privacy%20Shield_%20Flett,%20Yavorsky)%20June%202016.pdf; *see also* Jamie Davies, *EU Moves Forward with Privacy Shield Despite EDPS Warning*, BUS. CLOUD NEWS (July 8, 2016), http://www.businesscloudnews.com/2016/07/08/eu-moves-forward-with-privacy-shield-despite-edps-warning/.

challenge its adequacy during the first year.[90] Unfortunately, it could not prevent third parties from filing such legal challenges: Digital Rights Ireland filed a complaint against the agreement within two months of it coming into force.[91] Because this bilateral agreement has yet to be approved by the CJEU, it cannot yet be viewed as a viable long-term solution and does not mitigate the rationales for regional harmonization.

C. The Threat of Extraterritorial Jurisdiction

The CJEU believes that member-state regulators have the authority to enforce provisions of the EU Privacy Directive regardless of whether the relevant company is physically located within their territories. It recently decided a case, *Weltimmo v. Nemzeti*, in which the company facing enforcement action by the member-state regulator was located outside the member-state but offered a service to individuals within its borders.[92] The company argued that the regulator did not have authority to enforce the EU Privacy Directive provisions because the business could only be held liable by the regulator of the member-state in which it has its headquarters.[93] But the CJEU disagreed.[94] It instead held that member-states could enforce provisions of the EU Privacy Directive against companies outside the member-state in which they are "registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity—even a minimal one—in the context of which that processing is carried out."[95]

The greatest danger, however, may be hidden in an otherwise mundane procedural case within the United States titled *In re Warrant to Search a Certain*

---

90 Stephen Gardner, *EU Privacy Regulators Set Moratorium on Challenges to Data Transfer Pact*, BLOOMBERG BNA (July 26, 2016), https://bol.bna.com/eu-privacy-regulators-set-moratorium-on-challenges-to-data-transfer-pact/.

91 Julie Fioretti & Dustin Volz, *Privacy Group Launches Legal Challenge Against EU-U.S. Data Pact*, REUTERS (Oct. 27, 2016, 11:15 AM), http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK.

92 Case C−230/14, Weltimmo v. Nemzeti, 2015 ECLI 639, http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=93833.

93 *Id.*

94 *Id.*

95 *Id.*; *see also* Natasha Lomas, *Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S.*, TE CRUNCH NETWORK (Oct. 6, 2015), http://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/ ("The Weltimmo ruling effectively means that if a company operates a service in a country it can be held accountable by that country's national data protection agency—despite not being headquartered there.").

E-Mail Account Controlled and Maintained by Microsoft Corp.,[96] which raises the possibility that the United States will exercise extraterritorial authority over data held on an overseas server within the territory of an EU member-state. The warrant being debated was issued under the Stored Communications Act ("SCA") of the U.S. federal law Electronic Communications Privacy Act ("ECPA").[97] Microsoft contends that the warrant should have been obtained through the Mutual Legal Assistance Treaty rather than being issued under a domestic law.[98] Whereas the United States contends that the "emails should be treated as the business records of the company hosting them, by which definition only a search warrant would be needed in order to compel the provision of access to them no matter where they are stored."[99] The danger, as Daniel Solove aptly points out, is that other countries may reciprocate by using their own domestic statutes to obtain data housed within the United States.[100] The result would be a dangerous precedent permitting "governments around the world to seize information held in the cloud."[101]

More importantly, execution of this warrant would eliminate dedicated EU-based data centers as a viable interim solution. Up until now, transnational businesses and the EU alike assumed that the ability of the U.S. government to obtain data would be curtailed if the data was housed on a server outside U.S. territory. But this will no longer be true if the warrant is executed and Microsoft loses its appeal. As of the date of this writing, the warrant was upheld by the court, Microsoft was seeking to appeal, and the U.S. government won a revocation of a stay of the warrant's execution pending appeal.[102]

---

96 15 F. Supp. 3d 466 (S.D.N.Y. 2014), *reversed and remanded sub nom.*, Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

97 Daniel Solove, *Should the U.S. Play by Different Rules in Cyberspace?*, LINKEDIN (Sept. 24, 2015) [hereinafter Solove, *Should the U.S. Play by Different Rules?*], https://www.linkedin.com/pulse/should-us-play-different-rules-cyberspace-daniel-solove. The ECPA has three titles, one of which is the Stored Communications Act. *Federal Statutes: ECPA*, U.S. DEPT. OF JUST. OFF. OF JUST. PROGRAMS, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last revised July 30, 2013).

98 Solove, *Should the U.S. Play by Different Rules?*, *supra* note 97.

99 Sam Thielman, *Microsoft Case: DoJ Says It Can Demand Every Email from Any US-Based Provider*, THE GUARDIAN (Sept. 9, 2015, 4:06 PM), http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant.

100 Solove, *Should the U.S. Play by Different Rules?*, *supra* note 97.

101 Thielman, *supra* note 99.

102 *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., Nos. M9–150, 13–MJ–2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (granting government's motion to lift a stay on the warrant's execution); *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (permitting execution of the warrant), *reversed and remanded sub nom.* Matter

III. ANALYSIS: REGIONAL HARMONIZATION IS NOW A FEASIBLE, LONG-TERM SOLUTION

Although regional harmonization of U.S. and EU data privacy was historically considered impossible because of how committed each region was to its individual frameworks,[103] it is now a much more feasible solution for four reasons. First, the lack of a Safe Harbor permitting trans-Atlantic data transfers between the frameworks creates an incentive to harmonize that did not previously exist.[104] This is particularly true when one considers the practical business impact of being compliant with two distinct frameworks, which creates a cumbersome duplication of processes for any business with trans-Atlantic data operations, against the cost-saving benefits of complying with a streamlined set of harmonized regulations established via bilateral agreement. Second, public opinion regarding data privacy is changing in the United States, indicative of a willingness to change its framework.[105] There is a significant push for a more meaningful and nuanced form of consent than the current "notice and consent" or "privacy self-management" framework presents.[106] This is evident in the class action lawsuit against Google for its practice of data-mining all Gmail content and the numerous proposals on how to update U.S. law for the age of big data.[107] Third, there are shared economic and security imperatives that may make the call

---

of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

103 Schwartz & Solove, *supra* note 23, at 881 ("Attempts to harmonize U.S. and EU privacy law by turning EU privacy law into a U.S.-style approach, or vice versa, are unlikely to succeed. Both the United States and European Union are deeply committed to their respective approaches.").

104 *See* discussion *infra* Part III.A.

105 *See* discussion *infra* Part III.B.

106 *See* discussion *infra* Part III.B.1.

107 *See* discussion *infra* Parts III.B.2, III.B.3. The term "big data" refers to the collection and analysis of large, complex data sets. Dennis D. Hirsch, *That's Unfair! Or is it? Big Data, Discrimination and the FTC's Authority*, 103 KY. L. J. 345, 349 (2014). A full discussion of "big data" and its scope, including its uses and accompanying risks, is outside the scope of this Note. But it is important to understand the concept on a general level because it directly impacts why data transfers are important and why they are being regulated. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (Jack M. Balkin & Beth Simone Noveck eds., 2004) ("There are hundreds of companies that are constructing gigantic databases of psychological profiles, amassing data about an individual's race, gender, income, hobbies, and purchases. Shards of data from our daily existence are now being assembled and analyzed—to investigate backgrounds, check credit, market products, and make a wide variety of decisions affecting our lives."). *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013) (discussing the positive and negative ways in which big data affects us and changes the way in which we live, work, and think). Data-mining is the process in which companies analyze raw data to produce useful information, such as learning more about their customers or developing effective marketing strategies. *Data Mining*, INVESTOPEDIA, http://www.investopedia.com/terms/d/datamining.asp (last visited Nov. 3, 2016).

for regional harmonization a far more feasible solution than it was historically regarded.[108] Finally, regional harmonization does not require that the United States and EU have frameworks that mirror each other exactly.[109]

A. The Lack of a Safe Harbor Encourages Regional Harmonization

One reason why previous proposals for regional harmonization may have been considered unfeasible is because it was not a business necessity. Trans-Atlantic data transfers were already permissible under the Safe Harbor framework,[110] which did not require the United States overhaul or even revise its legal framework.[111] Companies interested in conducting trans-Atlantic data transfers only needed to self-certify that they would provide a level of privacy equivalent to that of the EU framework despite having lower legal requirements in the United States.[112] Thus, harmonization was unnecessary.

But the CJEU's invalidation of the Safe Harbor creates an incentive for regional harmonization that did not previously exist, and was in significant part based on the very fact that the United States did not adjust its legal framework to ensure an equivalent level of data protection.[113] Even if the participating companies delivered all the protections they promised in their self-certification, and these promised protections were found to be equivalent to EU protections (a question of fact that the CJEU did not consider in *Schrems v. Facebook*), the U.S. government was not bound by the Safe Harbor and could access EU data that was otherwise protected by self-certified Safe Harbor participants via contradictory federal laws.[114] This is precisely why the tentative Privacy Shield agreement, which is designed to replace the Safe Harbor but has yet to receive approval from the Article 29 Working Party or the 28 EU member states,[115] is said to only be viable if it meets four "essential guarantees": (1) "precise rules for processing," (2) government access "governed by the principles of necessity and proportionality," (3) "independent oversight mechanisms," and (4) "effective remedies open to individuals."[116]

---

108 *See* discussion *infra* Part III.C.

109 *See* discussion *infra* Part III.D.

110 *See* discussion *supra* Part II.B.1

111 *See* discussion *supra* Part II.B.1.

112 Bhatti, *supra* note 14.

113 *See* discussion *supra* note 56 and accompanying text.

114 *See* discussion *supra* note 31 and accompanying text.

115 Sheila A. Millar et al., *Safe Harbor 2.0 Arrives as EU-U.S. Privacy Shield; Approvals Still Necessary*, NAT'L L. REV. (Feb. 3, 2016), http://www.natlawreview.com/article/safe-harbor-20-arrives-eu-us-privacy-shield-approvals-still-necessary.

116 Gardner, *supra* note 11.

The demand that these EU privacy standards are met before any bilateral agreement is finalized means the EU will not abandon or water-down those principles to do business with the United States. But transnational business transactions are commonplace in today's globalized digital economy, and many U.S. businesses rely heavily on the 15-year-old Safe Harbor framework when conducting their business and establishing their infrastructure.[117] Both are endangered by the inability to reconcile the regional frameworks, thereby creating a strong incentive to harmonize the regional frameworks that did not exist before the Safe Harbor was invalidated.

Regional harmonization offers the additional benefit of potentially streamlining the regulations a business may need to follow to conduct compliant trans-Atlantic data transfers. Right now, companies need to abide by both the EU and the U.S. data privacy frameworks. Those frameworks, as discussed above in Part II.A, are fundamentally different. The United States, for example, permits data processing unless it is specifically limited by law, whereas the EU prohibits it unless it is expressly permitted by law.[118] EU citizens cannot contract their privacy rights away in end user agreements, whereas U.S. citizens can.[119] This creates a cumbersome duplication of processes for any business that offers services to both, as the business must be compliant with the stricter, broader EU rules while also abiding by U.S. law. This means businesses with trans-Atlantic data operations are creating and maintaining two different end user agreements, two different sets of procedures for storing and managing customer data, and two different processes for splicing and analyzing such data. Regional harmonization might eliminate some of that duplicative effort, streamline business requirements, and perhaps even identify a set of common standards or principles that better serve both regions.

B. U.S. Opinion Demonstrates Interest in Change

Another reason why proposals to harmonize the two regional data privacy frameworks may have historically failed is that there was little interest in change in the United States. But U.S. public opinion regarding data privacy is now changing, indicating a willingness to change its framework. This change is evident in three ways. One, there is a growing recognition that the notice and consent system is flawed, and a significant push for a more meaningful and nuanced form of consent than the current notice and consent or "privacy self-management" framework presents.[120] Two, the growing dissatisfaction with the current Framework is evident in the class action lawsuit brought against Google for its practice of data-mining all Gmail content. Three, there are numerous

---

117 *See* Drozdiak & Schechner, *supra* note 11.

118 *See supra* notes 8–9 and accompanying text.

119 *See supra* notes 27–28 and accompanying text.

120 *See* discussion *infra* Part III.B.1.

proposals on how to update U.S. law for the age of big data.[121] Each of these indicators demonstrates a growing interest in changing the current U.S. data privacy framework; making regional harmonization much more feasible than it was historically regarded.

1. Growing Recognition that the Notice and Consent System is Flawed

The U.S. public is becoming increasingly interested in changing data privacy within the United States. More of the public believes that the notice and consent system is not effective, and there has been a recent push for more meaningful forms of consent.[122] The term "privacy self-management" was coined by Professor Daniel J. Solove to represent the idea that individuals can consent to the "collection, use, or disclosure" of their personal data.[123] Under this type of framework, individuals are given a bundle of certain legal rights such as "rights to notice, access, and consent regarding the collection, use, and disclosure of personal data" that the individual can then choose to exercise after "weigh[ing] the costs and benefits of the collection, use, or disclosure of their information."[124]

That may sound great in theory, but Solove also identified some key cognitive and structural flaws within privacy self-management that prevent it from providing individuals with meaningful control over their data.[125] These hurdles include:

> (1) People do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decision[-]making difficulties.[126]

These challenges are compounded by the structural difficulties embedded in the current system, such as the fact that people are asked to make decisions at the point of collection, but the "true consequences of information use for individuals cannot be known when they make these decisions. Furthermore, the

121 *See* discussion *infra* Parts III.B.2, III.B.3.

122 *See* discussion *infra* Part III.B.1.

123 Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013).

124 *Id.* at 1880.

125 *Id.* at 1880–81.

126 *Id.* at 1888.

consequences are cumulative, and they cannot be adequately assessed in a series of isolated transactions."[127]

But at least privacy self-management recognizes that data is not "inherently good or bad," but dependent on the context of the data use.[128] There are many societal benefits that such data collection and use can offer, including the ability to track flu trends in live time and conduct medical research.[129] In 2009, for instance, Google was able to predict the spread of the H1N1 virus in the United States, "not just nationally, but down to specific regions and even states."[130] They did this by identifying a correlation between official Centers for Disease Control and Prevention ("CDC") figures and a mathematical model they combined with 45 search terms.[131] It was a significant achievement: "Like the CDC, they could tell where the flu had spread, but unlike the CDC they could tell it in near real time, not a week or two after the fact."[132] Healthcare researchers at Kaiser Permanente were able to similarly use the medical records of 3.2 million individuals to determine that a child's risk of autism doubled if the mother used antidepressants during her pregnancy.[133] The researchers only made the link because they had access to a large number of medical records that were retained after being collected for some other purpose; they "almost certainly [would] not have made the discovery if they had . . . conduct[ed] only a smaller, 'opt-in' study that required people to actively consent to providing the particular information the researchers were looking for."[134]

The issue is not that individuals are not interested in contributing to such beneficial projects, it is that they wish to provide a more nuanced form of consent regarding how their data may be used.[135] For instance, many may be willing to donate their data to medical researchers dedicated to curing cancer or otherwise conducting broad medical research beneficial to society as a whole, but they would simultaneously wish to prohibit that data from ever being accessible by insurance companies interested in health-based premium rate adjustments. Others may be comfortable with in-app targeted advertising (such as

---

127 *Id.* at 1893.

128 *Id.* at 1898.

129 MAYER-SCHÖNBERGER & CUKIER, *supra* note 107, at 1–2 (noting that Google can track the H1N1 virus in live time); Craig Mundie, *Privacy Pragmatism*, FOREIGN AFFAIRS, (March/April 2014), https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism ("[I]n 2011, researchers at the health-care giant Kaiser Permanente used the medical records of 3.2 million individuals to find a link between autism spectrum disorders in children and their mothers' use of antidepressant drugs.").

130 *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 107, at 2.

131 *Id.*

132 *Id.*

133 Mundie, *supra* note 129.

134 *Id.*

135 *See, e.g.*, *id.*

personalized advertising within a user's email service) but not with that data being directly sold or otherwise shared with those advertisers or other third parties. In that case, the individual wishes to decide whether or not to purchase the product or express further interest by signing up for the company newsletter or exploring the website himself. He does not want to end up on a mailing list because his email provider identified interest in a product during in-app targeted advertising and then sold that potential interest to that third party, without any action on his part. The current notice and consent and privacy self-management framework within the United States does not allow for such a nuanced form of consent.

Although the current form of privacy self-management is imperfect, it nevertheless forms an important part of the foundation of most data privacy frameworks.[136] The below case study regarding Google's data-mining of Gmail content provides a practical example of how the privacy self-management or notice and consent framework is flawed, and how U.S. public opinion regarding data privacy is changing.

2. The Class Action Lawsuit Against Google's Data-Mining of All Gmail Content

The U.S. public's growing dissatisfaction with the current data privacy framework is evident in the class action lawsuit against Google for its data-mining of all Gmail content. When Google announced that its new terms of service permit it to mine the content of all emails within its system, the public was outraged.[137] The company's terms state it is entitled to open, read, and retain the content of any emails sent from—or delivered to—a Gmail user.[138] This includes emails delivered from non-Gmail users who never agreed to its terms of service, and may have actually rejected those terms by choosing to use a different email service.[139] Numerous lawsuits have been filed against the company, particularly in California, alleging that the practice violates California privacy laws and federal wiretapping statutes.[140] In one class action lawsuit, filed on behalf of all those non-Gmail users who send email messages to Gmail users, the

---

136 See *supra* Part II.A.2, which includes a discussion of how the United States and EU handle consent differently by establishing different limits on contractual freedom.

137 Martha Mendoza, *Google Pleads Its Case For Scanning Your Emails to Help Sell Ads*, HUFFINGTON POST (Sept. 5, 2013, 4:39 AM) [hereinafter *Google Pleads*], https://web.archive.org/web/20130908164440/http://www.huffingtonpost.com/2013/09/05/gmail-ads-email-scanning_n_3871246.html; *see also* Martha Mendoza, *Google Argues for Rights to Continue Scanning Email*, U.S. NEWS (Sept. 5, 2013, 6:46 PM) [hereinafter *Google Argues*], http://www.usnews.com/news/technology/articles/2013/09/05/google-argues-for-right-to-continue-scanning-gmail.

138 *Google Pleads*, *supra* note 137; *Google Argues*, *supra* note 137.

139 *Google Pleads*, *supra* note 137; *Google Argues*, *supra* note 137.

140 *Google Pleads*, *supra* note 137; *Google Argues*, *supra* note 137.

practice was described as the "twenty-first-century equivalent of AT&T eavesdropping on each of its customers' phone conversations, or of the postal service taking information from private correspondence—acts that uniformly would be condemned as egregious and illegal invasions of privacy under any circumstance."[141]

Google argues that the data-mining is necessary because it generates revenue from an otherwise free email service through improved targeted advertising.[142] But opponents argue that the company's actions invade its users' privacy and takes their "property because they can get it for free as opposed to paying for it."[143] It is certainly true that there is a commonly held philosophy in the United States that private data can be treated as a commodity when an individual cedes his or her privacy in exchange for an otherwise free, tailored, or convenient service.[144] But it is certainly not true that data-mining and targeted advertising are the only mechanisms through which Google can generate revenue from its email service. In fact, the public outrage over the practice is a persuasive indicator that users would rather pay an annual membership for the email service than have the contents and associated metadata of that correspondence "scanned, analyzed, and catalogued indefinitely."[145]

The practice of data-mining and targeted advertising is partially based on the premise that an individual's personal data is more valuable when combined with the personal data of others within a similar age group or characteristic because it can reveal larger trends (of which even the individuals themselves may be unaware) that will generate more revenue when sold (either outright or via advertising services) to a third party business than the company may be able to generate through individual membership subscriptions. But this makes it incredibly profitable—and indeed preferable—for companies to coerce

---

141 Kat Greene, *Google Faces New Privacy Class Claims Over Email Scanning*, LAW360, (Sept. 8, 2015, 9:25 PM), http://www.law360.com/articles/699961/google-faces-new-privacy-class-claims-over-email-scanning (quoting Plaintiff's complaint).

142 *See id.*; Heather Kelly, *Why Gmail and Other E-mail Services Aren't Really Free*, CNN (April 1, 2014, 4:31 PM), http://www.cnn.com/2014/03/31/tech/web/gmail-privacy-problems/; *Google Argues*, *supra* note 137.

143 *Google Argues*, *supra* note 137.

144 Julia Angwin, *Has Privacy Become a Luxury Good?*, N.Y. TIMES (Mar. 3, 2014), http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html?_r=0 ("In our data-saturated economy, privacy is becoming a luxury good. After all, as the saying goes, if you aren't paying for the product, you *are* the product. And currently, we aren't paying for very much of our technology.").

145 Greene, *supra* note 141. Indeed, the idea that people are "willing to pay a modest upfront price to join social networks that guarantee the integrity of their personal data" has produced the concept of the "privacy economy." DJ Pangburn, *How App Companies are Turning Privacy into a Commodity*, MOTHERBOARD (Mar. 10, 2014, 3:56 PM), http://motherboard.vice.com/blog/how-app-companies-are-turning-privacy-into-a-commodity. It is supported by a recent study by several economists at the University of Colorado-Boulder that found that "people would pay $5.06 for the sweet nectar of privacy." *Id.*

users into ceding their private, personal data to use a service rather than pay for it outright. Indeed, businesses are now "conditioning products, services, or access on opting in" and it is now common for "agreeing to . . . end-user license agreements . . . [to be] a prerequisite for obtaining access to a website or to use a product or service."[146] The user has no bargaining power.[147] The U.S. public is becoming increasingly dissatisfied with this status quo and there is a significant push for a more nuanced form of consent than the current privacy self-management framework presents, as evidenced by the above class action lawsuit against Google's data-mining of all its Gmail content and the numerous proposals for updating U.S. law that are discussed below.

3. There Are Numerous Proposals for Updating U.S. Law

Historical proposals for regional harmonization may have been discarded because of insufficient U.S. interest in changing existing data privacy protections, but discontent is often identified through proposals for change. In this case, the sheer volume and scope of the proposals for updating data privacy law in the United States indicate the level of change in U.S. public opinion. As the President's Council of Advisors on Science and Technology ("PCAST") effectively stated in its 2014 presidential report, "new collisions between technologies and privacy have become evident, as new technological capabilities have emerged at a rapid pace. It is no longer clear that . . . [the current data privacy framework is] sufficient in the court of public opinion."[148] The recommendations for changing this insufficient framework include creating a more meaningful form of consent in an improved privacy self-management framework, using metadata "wrappers" to regulate data use rather than data collection, and establishing clear due process requirements for digital transaction surveillance. Each of these proposals indicates that the U.S. public is interested in changing its data privacy framework and it is this desire for change that makes regional harmonization a more feasible long-term solution than it was historically regarded.

i. Improve Privacy Self-Management

One way those dissatisfied with the current U.S. data privacy framework recommend changing it is to improve privacy self-management so it provides a more meaningful form of consent. The limitations of privacy self-management are apparent to any mobile device user that has accepted an end user agreement

146 Solove, *supra* note 123, at 1898.

147 *Id.*

148 PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 5 (2014) [hereinafter PCAST PRESIDENTIAL REPORT].

in the past. As PCAST summarized in its 2014 presidential report, "[i]n some fantasy world, users actually read these notices, understand their legal implications (consulting their attorneys if necessary), negotiate with other providers of similar services to get better privacy treatment, and only then click to indicate their consent. Reality is different."[149] In reality, people do not read privacy policies.[150] Even if they did, Solove points out that they do not know enough to understand them or make an informed choice.[151] Moreover, it is impossible to exercise meaningful control in such a manner (even if one did read and understand every privacy policy) because the very benefit big data provides in creating "new, non-obvious, unexpectedly powerful uses of data" defeats notice and consent as an effective policy tool: "[i]t is simply too complicated for the individual to make fine-grained choices for every new situation or app."[152]

Solove proposed resolving these difficulties by "recognizing that people can engage in privacy self-management only selectively," "adjusting privacy law's timing to focus on downstream uses," and "developing a coherent approach to consent . . . that accounts for the social science discoveries about how people make decisions about personal data."[153] But PCAST provided an even more concrete solution. It proposed that a third party or agency be created that would be responsible for vetting apps and other digital services against user privacy preferences.[154] Thus, users could create a privacy profile that provides a more nuanced form of consent and the agency would be responsible for comparing those preferences against each company's privacy notice to advise whether or not they align.[155] This would create a "marketplace for the negotiation of community standards of privacy" and encourage businesses to close any gaps between user preferences and current practices.[156]

ii. Regulate Data Use Rather than Data Collection

Another proposed means of improving the current U.S. data privacy framework is to change the focus of regulation from data collection to data use. Craig Mundie discusses this proposal at length in his *Foreign Affairs* article, *Privacy Pragmatism*, and the PCAST cited and adopted his work in its presidential report.[157] Just as Solove suggested in his critique of privacy self-

149 *Id.* at 38.

150 Solove, *supra* note 123, at 1888.

151 *Id.*

152 PCAST PRESIDENTIAL REPORT, *supra* note 148, at 38.

153 Solove, *supra* note 123, at 1903.

154 PCAST PRESIDENTIAL REPORT, *supra* note 148, at 40–41.

155 *Id.* at 41.

156 *Id.*

157 *Id.*

management that "people can engage in privacy self-management only selectively,"[158] Mundie suggests that "there is simply so much data being collected, in so many ways, that it is practically impossible to give people a meaningful way to keep track of all the information about them that exists out there, much less to consent to its collection in the first place."[159] The solution is to shift the regulatory focus from the point of collection to the point of use.[160]

Mundie suggests that the fears users experience regarding privacy violations are not based on the actual data collection, but the fact that "people do not know who possesses data related to them and have no way to know whether the information is being used in acceptable ways."[161] After all, the simple fact that the data is available does not mean it has been abused (yet).[162] But the practice of providing consent at the point of collection (by clicking yes to an endless number of end user agreements) is worthless because those agreements never give sufficient specifics about how that collected data will be used.[163] And if the agreement permits the data being sold to third parties, then that original notice and consent does nothing to limit the downstream uses of that data. In the end, Mundie points out:

> When people are asked to give a practical example of how their privacy might be violated, they rarely talk about the information that is being collected. Instead, they talk about what might be done with that information, and the consequences: identity theft or impersonation, personal embarrassment, or companies making uncomfortable and unwelcome inferences about their preferences or behavior. When it comes to privacy, the data rarely matters, but the use always does.[164]

To be effective, data privacy regulation must shift from requiring consent at the point of data collection to creating a consent framework around data use.

One mechanism for accomplishing this, according to Mundie, is creating data "wrappers" that describe the type of material it contained without revealing content.[165] These wrappers would be created at the moment the data is created and contain rules around how and when that data can be accessed and used, essentially acting as a virtual "lock" against unauthorized use.[166] Thus, anyone

158 Solove, *supra* note 123, at 1903.

159 Mundie, *supra* note 129.

160 *Id.*

161 *Id.*

162 *Id.*

163 *Id.*

164 *Id.*

165 *Id.*

166 *Id.*

seeking to unlock the wrapper would need to get approval from the requisite authorities[167] and perhaps be subject to compliance audits by data regulators.[168] Mundie compares these "wrappers" to the encryption the entertainment industry added to reduce video piracy and maintains that these digital rights management systems would only need to be revised slightly to accommodate such an application to data.[169] Because such a system would require significant details about the types of uses and processing that users would be willing to agree to, and must necessarily and constantly evolve with the technology industry, Mundie suggests that users delegate these rights to a newly created agency that would be responsible for establishing and enforcing such standards on a large scale.[170]

When PCAST incorporated Mundie's proposal into its presidential report on big data and privacy, it suggested that individuals should be able to create a personal privacy profile with nuanced instructions regarding how their data can be used after collection.[171] These instructions would then be translated into code, rendered tamper-proof, and attached to all data associated with that person.[172] The code must be "sticky" so that it remains even if the data is copied or moved.[173] According to PCAST, such use-driven management systems already exist within the U.S. intelligence community and are being increasingly implemented as part of custom builds for large commercial companies, so it is likely that the government could "help motivate the creation of an off-the-shelf standard software."[174]

iii. Establish Clear Due Process Requirements for Digital Transaction Surveillance

A third proposal for improving the current U.S. data privacy framework—and the final one that will be discussed in this Note as evidence of how changing U.S. opinion makes regional harmonization much more feasible than it was historically considered—is to clarify and establish clear due process requirements for digital transaction surveillance. There are numerous types of digital surveillance and intelligence methods that government agencies can

167 *Id.*

168 *Id.*

169 *Id.*

170 *Id.*

171 PCAST Presidential Report, *supra* note 148, at 41.

172 *Id.*

173 *Id.*

174 *Id.* at 42.

pursue in today's big data environment.[175] Of those, transaction surveillance is the act of "accessing *already-existing* records, either physically or through computer databanks. . . . [and] accessing, in real-time or otherwise, the *identifying signals* of a transaction (such as the address of an email recipient)."[176] This is in addition to the more traditional forms of real-time physical and communications surveillance that authorities could use in conjunction.[177]

But unlike the more traditional forms of surveillance, for which there is a fair amount of jurisprudence regarding the relevant due process requirements for surveillance activity (e.g. needing a warrant based on probable cause issued by an independent judge),[178] there is a great deal of confusion regarding the certainty level and authorization required for these more modern forms of transactional surveillance.[179] Professor Christopher Slobogin consolidated the various authorization levels currently required for transactional surveillance in a table that is reproduced in full below.

175 *See* Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 139–41 (2005).

176 *Id.* at 140.

177 *Id.*

178 *Id.* at 152–54.

179 *Id.* at 166.

Table 1: Current Law of Transaction Surveillance[180]

Transaction	Auth'zation Req'd	Certainty Level
———-	Warrant	Probable cause
———-	*Terry* Order	Reasonable suspicion
Medical, financial & tax records; stored email	Subpoena	Relevance, challengeable by target
Financial records and stored email if notification poses risks	Delayed-notice Subpoena	Relevance, challengeable by target only after records obtained
Billing records and logs of phone companies & ISPs; most customer records	Ex Parte Subpoena	Relevance, challengeable only by third party record-holder
Interception of catalogic information re calls & email; tangible items re terrorism	Certification Order	Relevance (determined by government), issued by court, challengeable only by third party record-holder
Federal public records; financial records re terrorism	Extrajudicial Certification	Relevance (determined by government), not challengeable by any party (?)
State public records not protected by law or that are acquired by a CDB	None	None

The sheer volume and variety of authorization levels and due process requirements causes confusion. Professor Slobogin suggested eliminating this confusion by streamlining all the current authorizations levels into three: a warrant, *Terry* Order, or subpoena.[181] Should the United States implement this proposal to clarify existing law by establishing clear due process requirements for digital transaction surveillance, it will have alleviated significant EU concerns surrounding trans-Atlantic data transfers[182] and potentially contributed to the identification of common due process principles that could serve as part of a future bilateral agreement for regional harmonization.

180 *Id.* at 166–67.

181 *Id.* at 169.

182 Namely, limited government access per the principle of necessity and proportionality, as discussed in notes 11, 56, and their accompanying text.

C. Shared Economic and Security Imperatives Encourage Regional Harmonization

Regional harmonization is a much more feasible, long-term solution than it was historically regarded because, in addition to the various proposals discussed above that indicate significant U.S. interest in changing the prevailing framework, the United States and the EU share economic and security imperatives that drive harmonization.

First, regional harmonization is economically imperative to both regions. The EU and the United States are two of the world's largest economies[183] (representing 75% of all products traded and delivered online)[184] and they are each other's largest trading partner in digitally deliverable services.[185] The inability to find sufficient regional harmony to permit trans-Atlantic data transfers endangers billions of dollars of trade[186] and over 4,500 U.S. companies.[187] Nearly all multinational businesses move customer and employee data between regions, including General Electric and Pfizer.[188] And this does not take into account the non-U.S. businesses that may be impacted because of data processing or storage subcontract agreements with U.S. companies that rely on trans-Atlantic data transfers.[189] Regional harmonization would preserve the existing economic activity and encourage increased activity within the trans-

---

183 Mark Scott, *Europe's Top Digital-Privacy Watchdog Zeros in on U.S. Tech Giants*, N.Y. TIMES (Jan. 24, 2016), http://nytimes.com/2016/01/25/technology/europes-top-digital-privacy-watchdog-zeros-in-on-us-tech-giants.html.

184 U.S. MISSION TO THE EUROPEAN UNION, *supra* note 15 ("And demonstrating the interconnectedness of U.S. and European industries, 53 percent of digitally deliverable services imported from the U.S. (including consulting, engineering, design, and financial services) were used in the production of EU exports, and 62 percent of digitally deliverable services imported from the EU were incorporated into U.S. exports.").

185 *Id.*

186 Scott, *supra* note 183.

187 Drozdiak & Schechner, *supra* note 11.

188 Scott, *supra* note 183.

189 The Safe Harbor was commonly used for "data transfers needed to support intra-group operations (for example to assist a U.S. parent in managing EU-based activities) and outsourced services involving a U.S. cloud or software-as-a-service provider." DLA PIPER, US SAFE HARBOR FRAMEWORK DECLARED INVALID 2 (2015), https://www.dlapiper.com/~/media/Files/Insights/Publications/2015/10/Safe_Harbor_Client_Flier.pdf. Its invalidation affects "more than US tech companies," including any company that relied on the Safe Harbor "as a legal basis for transferring user, customer, employee or any other personal data to the United States, either intra-group or through the supply chain." *Id.* at 2. Thus, it is often recommended that every company "verify whether [their] vendors process EU personal data in the United States, or process EU personal data in the EU but have a contractually stipulated right to relocate the data (e.g., in a cloud context)." *Id.* at 4. Should the vendor employ a subcontractor, then these data transfers must also provide "the same rights and must also ensure an adequate level of protection." *Id.*

Atlantic digital economy. Establishing common data protection principles that could streamline the demanding and duplicative regulations to which many multinational businesses are subject in the United States and the EU could actually cut costs and encourage more trans-Atlantic trade.

Second, the United States and the EU share similarly imperative national security interests in harmonizing their data privacy frameworks.[190] Data mining is becoming an increasingly important tool in anti-terrorism efforts,[191] and terrorism remains a critical and substantial threat to both regions. Europol advises that the Islamic State has "expand[ed] its activities to a global level, with a focus on the European Union" and that the EU should "prepare for more frequent acts of terror similar to the recent Paris attacks."[192] This is particularly troubling when 201 terrorist attacks were carried out in EU member-states during 2014 alone.[193] According to one source, there were only 11 terrorist attacks within the United States during 2014,[194] but there were 91 homegrown and 380 international terrorist attacks in the United States between 2001 and 2009.[195]

United States counterterrorism efforts have evolved to include means for accessing data on both national and foreign citizens. The 702 program,[196] for

---

190 The United States and the EU recognized this security interest when it created the Terror Finance Tracking Program (TFTP) in 2010, which permits "bank and credit card transaction information to the U.S. treasury in an effort to trace funding to terrorist groups." *NSA Spy Scandal May Scuttle EU-US Anti-Terrorist Agreement – EU Commissioner*, RT.COM (Sept. 26, 2013), https://www.rt.com/news/nsa-eu-snowden-terrorism-financial-321/. But the EU has threatened to suspend this data-sharing deal after the Snowden leaks revealed that the NSA was "tapping into the SWIFT databases to gain access to the private data of Europeans on their financial dealings" and that officials relied on "broad administrative subpoenas for millions of records" rather than seeking "individual court-approved warrants or subpoenas to examine specific transactions." *Id.*

191 BHAVANI THURAISINGHAM, DATA MINING FOR COUNTER-TERRORISM 191, https://www.utdallas.edu/~jxr061100/paper-for-website/%5B18%5DMining-Terrorism-NGDM04.pdf ("Data mining is becoming a useful tool for detecting and preventing Terrorism."). Indeed, it is one reason why the FBI is so adamant about getting access to the encrypted data on the iPhone of the terrorist who committed the attacks in San Bernardino, California. *See* discussion *supra* Part I.

192 *ISIS Focusing on EU, Threat of Imminent Terror Attack – Europol*, RT.COM (Jan. 26, 2016), https://www.rt.com/news/330151-isis-europe-terror-europol/.

193 EUROPOL, EUROPEAN UNION TERRORISM SITUATION & TREND REPORT 2015, at 8 (2015), https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015.

194 Wm. Robert Johnson, *Terrorist Attacks and Related Incidents in the United States*, JOHNSTON'S ARCHIVE, http://www.johnstonsarchive.net/terrorism/wrjp255a.html (last visited Nov. 11, 2016).

195 David B. Muhlhausen & Jena Baker McNeill, *Terror Trends: 40 Years' Data on International and Domestic Terrorism*, HERITAGE (May 20, 2011), http://www.heritage.org/research/reports/2011/05/terror-trends-40-years-data-on-international-and-domestic-terrorism.

196 The 702 program is one of two intelligence collection programs used by the NSA, authorized under Section 702 of the Foreign Intelligence Surveillance Act. PRIVACY AND CIVIL

instance, permits the U.S. government to "serve orders on social media, webmail, and electronic service providers who store their global customers' data in the United States."[197] The United States has even shared this intelligence with the EU to prevent or solve terrorist attacks. Indeed, the United States shared large amounts of intelligence with France after the Paris attacks and it even helped Germany "thwart [several] planned suicide bombings in Munich over the New Year holiday."[198] But the invalidation of the Safe Harbor threatens the source of much of this information. The 702 program relies on accessing global data held in the United States by multinational companies. Although the U.S. government can still serve court orders on those companies and demand access to their data, the results will no longer be the global data that assisted Germany in thwarting the New Year holiday suicide bombings in Munich or helped France after the Paris attacks. It will no longer include the EU data that was traditionally incorporated via trans-Atlantic data transfers under the Safe Harbor framework.

Regional harmonization, however, could solve this issue. It is one more reason why regional harmonization is a much more feasible, long-term solution than it was historically regarded. It cannot be resolved without first discussing differences between the regional frameworks, of course, and then discussing the common principles that should govern government surveillance and the level of due process required before such surveillance could be performed. These aspects do differ across the regional frameworks; consider, for example, the complicated U.S. due process requirements earlier critiqued by Slobogin and the essential guarantee in the EU that "any government access to data should be governed by the principles of necessity and proportionality."[199] But the very fact that there are varying levels of due process on both sides of the Atlantic means that success is just a matter of finding common ground. This may be difficult, but it is not impossible; both regions have significant national security interests in ensuring that their intelligence agencies are able to gather sufficient data that their counterterrorism efforts are effective. The regions share similar economic incentives to harmonize their data privacy frameworks, as doing so will preserve billions of dollars in trans-Atlantic trade and encourage further economic growth.

LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), http://www.wired.com/wp-content/uploads/2014/07/PCLOB-Section-702-Report-PRE-RELEASE.pdf. It permits the U.S. government to collect "the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person located outside the United States." *Id.* at 1.

197 Stewart Baker, *Time To Get Serious About Europe's Sabotage of US Terror Intelligence Programs*, WASHINGTON POST (Jan. 5, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/05/time-to-get-serious-about-europes-sabotage-of-us-terror-intelligence-programs/.

198 *Id.*

199 Gardner, *supra* note 11.

D. Harmonization Does Not Require Mirror Image Frameworks

Regional harmonization may have been historically discarded as unlikely to succeed because it was difficult to imagine how to bridge the significant gaps between the regional frameworks without requiring one region to adopt a mirror image of the other's framework. As two highly respected legal privacy scholars, Paul M. Schwartz and Daniel J. Solove, theorized, "[a]ttempts to harmonize U.S. and EU privacy law by turning EU privacy law into a U.S.-style approach, or vice versa, are unlikely to succeed. Both the United States and EU are deeply committed to their respective approaches."[200]

But regional harmonization amongst the United States and the EU does not require that either region abandon its framework and adopt mirror images of the other's to be successful. Consider the harmony involved in a musical piece; envision a piano chord. Each note within that chord represents a particular key without which the chord itself could not exist.[201] In this case, the United States and the EU are represented by two separate and distinct notes that create a discordant sound when played together. The idea of regional harmonization is that one can find a single point at which the two regional frameworks agree, perhaps by identifying some key principles that are met in both frameworks, and that third note of commonality can create a chord that is much more pleasing to the ear. The resulting harmony does not require mirror images of a particular framework, so much as an agreement among the regions as to a common set of principles that both regional frameworks would honor.

So long as the United States and EU could agree on a core set of common principles, it remains possible for the regions to maintain their distinct frameworks and enforcement mechanisms while still creating trans-Atlantic harmony in data privacy regulation.[202] This Note does not presume to propose what those common principles should be, as that is a topic whose analysis best deserves a separate Note. But it does not make it impossible. The move would

---

200 Schwartz & Solove, *supra* note 23, at 881.

201 *See* Duane Shinn, *Piano Chords: How Many Are There?*, PLAYPIANO.COM, http://www.playpiano.com/Articles/29-howmanychords.htm (last visited Nov. 3, 2016) ("[A] 3 note chord has 3 positions.").

202 Consider the fact that the EU data privacy framework is actually based on "the Fair Information Practice Principles, which were initially developed in the U.S. in the 1960s and 1970s. . . . Even the EU regulatory structure, which requires an independent regulatory agency, was borrowed from the United States." Abraham Newman, *After Safe Harbor: Bridging the EU-U.S. Data-Privacy Divide*, WORLD POL. REV. (Feb. 9, 2016), http://www.worldpoliticsreview.com/articles/17898/after-safe-harbor-bridging-the-eu-u-s-data-privacy-divide. The U.S. and EU data privacy frameworks may differ significantly, as discussed in Part II.A, but the very fact the EU framework was inspired by U.S. practices means that it is likely that the regional frameworks are supported by a common set of principles. These common principles merely need to be identified and expanded upon to create a new bilateral agreement whose procedures and principles could then govern future trans-Atlantic data transfers.

require significant negotiation and buy-in by political parties and businesses, but it could provide a stronger, long-term solution if carefully crafted. Indeed, the final agreement could take the form of a treaty and might even be nicknamed the new "Safe Harbor 2.0," permitting trans-Atlantic data transactions provided they meet the common principles included in the agreement and are guaranteed to be enforced by the relevant domestic enforcement authority in each region.

IV. CONCLUSION

To sustain trans-Atlantic data transfers in the long-term, the United States and the EU must harmonize their data privacy frameworks. Right now, the sharp differences between the regional frameworks produce a level of discord similar to the grating sounds of a musical performance without harmony. This striking discord between the United States and the EU was formerly mitigated by the Safe Harbor framework, but its recent demise made the regional discord worse by removing that single harmonizing note.

Legal scholars have historically discarded proposals to harmonize U.S. and EU data privacy regulation as impossible because of the large gap between the frameworks and each region's deep commitment to their approach.[203] But this Note demonstrates that the idea of regional harmonization is much more feasible than it was in the past, and it should no longer be discarded as an inviable option. As this Note argued, regional harmonization is now a much more feasible long-term solution for four reasons: (1) the lack of a Safe Harbor permitting trans-Atlantic data transfers creates an incentive that did not exist previously, (2) the change in U.S. public opinion regarding data privacy demonstrates an interest in changing its framework, (3) the regions share economic and security imperatives for harmonization, and (4) the regions do not need mirror image frameworks to achieve harmonization.

What form that harmonization should take, and the common principles that it should be comprised of, is the subject of another Note. But the idea of harmonization is certainly much more feasible than it was historically regarded, and it should no longer be discarded as an inviable option.

*Jennifer L. Bauer**

---

[203] Schwartz & Solove, *supra* note 23, at 881 (discarding "[a]ttempts to harmonize U.S. and EU privacy law by turning EU privacy law into a U.S.-style approach, or vice versa, [is] unlikely to succeed. . . . [because] [b]oth the United States and European Union are deeply committed to their respective approaches").

* J.D. Candidate, West Virginia University College of Law, 2017; B.A., William Paterson University, 2010. The Author expresses her sincere gratitude to Professor Jena Martin, Associate Dean for Innovation and Global Development, for her invaluable guidance and support throughout this process. The Author would also like to thank her friends on the *West Virginia Law Review* for all their hard work, as well as her family for their unwavering support. All errors contained herein are the Author's alone.