RETHINKING DATA SECURITY: THE DIFFERENCES BETWEEN THE EUROPEAN UNION AND THE UNITED STATES' APPROACH TO DATA SECURITY AND BUILDING TRANSNATIONAL STANDARDS WITH TRANSPARENCY AND UNIFORMITY

SHELBY L. WALLACE*

* Shelby Wallace received her Juris Doctor from the University of Wisconsin Madison Law School. She also received her Bachelor of Arts degree and a Certificate of European Studies from the University of Wisconsin Madison. After graduation, Shelby hopes to pursue a career in public interest. She would like to thank her family and friends for all of their support and the WILJ editors for their work and guidance during the writing and publication process.

INTRODUCTION

The past decade has marked an immense growth in technology and the way we utilize data. With growth comes change and the need for more protective policies. The personal privacy many have taken for granted for generations, "is being swept away by a variety of forces."[1] These forces include "our heavy reliance on the Internet for work, entertainment and shopping; our addiction to cellphones, data plans and apps; our eagerness to expose the details of our lives on websites like Facebook; and our tolerance of excessive government spy programs."[2] The dependence on technology has brought to light problems such as data security breaches, government surveillance, and international data transfer rights. In general, the populace is becoming less tolerant of collection and sale of personal data by third parties and the government.[3]

While some companies, like Facebook, have responded to this sentiment by providing options for increased privacy settings, some companies lack such options, and some individuals question whether the higher standards are enough.[4] Given the lack of accountability amongst private sector businesses, and the trend in government to collect and monitor the personal data of its citizens, there is a need for a more extensive policy that will encompass international companies and governments alike. The problem for regulators lies in the dichotomy of protecting fundamental rights versus enabling free transnational flow of data for the operative use of the respective companies and governments as well as the convenience and safety of its customers. Interestingly enough, the standards of privacy are changing because young people feel like the they have more control on the web than they do in their own

---

1 Walter Simpson, *The end of privacy? Government and private surveillance pose a growing threat to Americans,* THE BUFFALO NEWS (May 10, 2014), http://www.buffalonews.com/opinion/viewpoints/the-end-of-privacy-government-and-private-surveillance-pose-a-growing-threat-to-americans-20140510.

2 *Id.*

3 *See* Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden,* PEW RESEARCH CENTER (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

4 *See generally* Bobbie Johnson, *Privacy No Longer a Social Norm, says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy; Dan Wilson, *Are high privacy settings on Facebook enough to protect your information?*, METRO (Sep. 25, 2013), http://metro.co.uk/2013/09/25/are-high-privacy-settings-on-facebook-enough-to-protect-your-information-4109736/.

homes, so even despite the loosened standards, young people feel more in control of their digital content.[5]

An adequate standard of protection would need to strike a balance between this dichotomy, while accounting for the continuous changes in technology. A standard like this would come as a massive change to the Facebook, Microsoft, and Googles of the world, as well as those who subscribe to such services and are subjects to a developed government. Perhaps the greatest challenge in the development and implementation of such a standard is feasibility. Is one universal standard feasible for the world we live in today? Is this just too simple and ignorant of government interests and other such externalities?

This paper addresses these issues and others that arise as we further conceptualize the implementation of a new worldwide standard of protection for personal data protection. Accordingly, in Part II, this paper explores the data security regulations in place in the United States and the European Union, and explores a major challenge within the current infrastructure. This part also provides an in depth look into *Schrems v. Data Protection Commissioner*, which illustrates the distinct problem with the American approach to data security, and the effects it has on both citizens and non-citizens. In Part III, this paper proposes that a more stringent approach would protect the public against both governmental and private intrusion. This paper argues that a comprehensive and uniform approach will allow for free flowing trade and individual liberty while still permitting governments to monitor online exchanges for terrorism and other security threats.[6]

II. BACKGROUND

A. HISTORY OF UNITED STATES GOVERNMENTAL REGULATIONS OF CITIZENS' PRIVATE DATA

George Orwell's *1984* provides an eerily accurate foreshadowing of the age of government surveillance.[7] In the real world, questions of privacy and consumer data have been present for decades. While there

---

[5] Bobbie Johnson, *supra* note 4.

[6] The author is aware of the changing and unprecedented political landscape and predicts that both the Trump presidency and the "Brexit" movement will have a chilling effect on future transnational agreements regarding transnational data flow. This paper explores the legal climate as it stands with the status of the TPP, TTIP, and TiSA, which is still largely uncertain.

[7] *See generally* GEORGE ORWELL, 1984 (Signet Classics 1961).

may not be monitors in each room watching every move we make, presently there are legitimate concerns about the way our personal information is collected and shared online.[8] These concerns are exacerbated by a lack of legal protections. For example, in the United States, there is no single, comprehensive federal law regulating the collection and use of personal data. Instead, there exists a patchwork system of federal and state laws.[9]

American's relationship to privacy began when colonists emigrated from Britain to escape persecution,[10] fueled, in part, by a desire to be free of intrusion by the Crown. These desires shaped the drafting of the United States Constitution.[11] Specific to this issue, is the Fourth Amendment, which enumerates the "right to be secure from all unreasonable searches and seizures" and the liberty of personal autonomy guaranteed by the Fourteenth Amendment.[12]

These questions continued on into the nineteenth century, until the advent of the telegraph and the national census changed the conversation.[13] The telegraph was invented in 1844 and was used strategically during the Civil War when the Union and Confederate armies tapped each other's telegraph communications to ascertain battle plans and troop movements.[14] Later in the nineteenth century, rival press organizations tapped each other's wire communications to be the first to report major news items.[15] In 1890, a profound work, "The Right to Privacy," asked questions and proposed thoughts that were unprecedented in scholarship"[16] The media's expansion inspired this article. The authors were concerned that "[t]he press [was] over-stepping in every direction the obvious bounds of propriety and decency."[17] As a

---

[8] *See* Raine & Madden, *supra* note 3.

[9] Arti Sangar, *Data Privacy Protection: A Serious Business for Companies,* 41 INT'L LAW NEWS 1, 2 (Fall 2012).

[10] DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 1 (1972).

[11] Doug Lidner, *The Right of Privacy: Is it Protected by the Constitution?,* UMKC, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (last visited Jan. 10, 2017).

[12] U.S. CONST. amend. IV; U.S. CONST. amend XIV.

[13] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 46, 111 (1995).

[14] *Id.*

[15] *Id.* at 110-11.

[16] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[17] *Id.* at 196.

result, individuals began to challenge their right to privacy in their personal interactions.

Sparked by Warren and Brandeis's the Right to Privacy, the twentieth century, was marked with judicial and executive policy that pushed for individual privacy and freedoms.[18] Many characterize this century by the passage of the first Foreign Intelligence Surveillance Act (FISA). FISA, enacted in 1978, afforded the government more power to "spy" on those engaged in espionage on behalf of a foreign power.[19] Lawmakers seemed to justify this invasion of privacy because when it was originally passed, its purpose was to "allow the government to collect foreign intelligence information involving communications with 'agents of foreign powers.'"[20] At the Federal level, regulation continued through several industry-specific regulations, such as the Cable Communications Policy Act of 1984 and the Right to Financial Privacy Act of 1978.[21] There are also broader laws that impose a duty of self-regulation amongst consumer-based companies. Another consequential act was the Electronic Communications Protection Act (ECPA), which was passed in 1986.[22] "The Act reflects a general approach of providing greater privacy protection for materials where there are greater privacy interests."[23] Moreover, there have been many guidelines developed by governmental agencies and industry groups that are not legally enforceable but are part of self-regulatory efforts and are considered best practices.[24]

At the turn of the twenty-first century, the data and security landscape dramatically changed. After 9/11, individuals were willing to give up their privacy, their freedom, and their liberties in exchange for a sense of security.[25] The ECPA was strengthened by the USA PATRIOT

---

[18] *See e.g.* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); RESTATEMENT (SECOND) OF TORTS §§ 652C and 652E; Simonsen v. Swenson, 177 N.W. 831, 832 (Neb. 1920); Olmstead v. United States, 277 U.S. 438 (1928).

[19] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881(a) (2008).

[20] *The Foreign Intelligence Surveillance Act - News and Resources*, ACLU, https://www.aclu.org/other/foreign-intelligence-surveillance-act-news-and-resources.

[21] *See generally* 47 U.S.C. § 551 (1984); *see also* 15 U.S.C. 1681 (1978).

[22] *See* 18 U.S.C. 2510–22 (1986).

[23] *Id.*

[24] *See* Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising,* (Dec. 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

[25] *See* Langer, *9/11 Anniversary: A Sense of Security Rebounds*, ABC News (Sept. 9, 2011), http://abcnews.go.com/blogs/politics/2011/09/911-anniversary-a-sense-of-security-rebounds/.

Act.[26] The 2008 FISA amendments also expanded this regime to include the infamous NSA PRISM Program.[27] The PRISM program ramped up targeting procedures, including procedures for targeting American citizens, and an "exigent circumstances" provision, which allowed searches prior to approval by the FISA court.[28] Citizens still lack full knowledge of the extent of the application of FISA amendments, the Prism program, and the NSA's ability to collect individual data directly from the servers of companies such as Google and Facebook.[29]

Most recently, concerns about data privacy were brought in the case *USA v. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203,* (Cal. Central Dist. Ct. Feb. 19, 2016).[30] The issue in this case was whether the FBI could order a private company, Apple, to hand over the encryption software that would unlock the phone of an alleged terrorist.[31] Apple has repeatedly argued that private companies cannot be compelled on a whim to assist authorities without limits, and that China and other authoritarian governments point to the warrant as a pretext for their own attempts at forcing access into customer data.[32] The FBI argued in a 35 page brief that Apple's practices are "corrosive of the very institutions that are best able to safeguard our liberty and our rights: the courts, the fourth amendment, longstanding precedent and venerable laws, and the democratically elected branches of government."[33]

No matter the outcome, this case is just another part of a piecemeal fix to a larger issue. It failed to address the questions that go beyond the scope of the facts listed. Questions remain: whether private companies give this information on their own will or if courts can

---

[26] *See* 18 U.S.C. 2510–22, *supra*, note 21.

[27] *See* Timothy B. Lee, *Here's Everything We Know about PRISM to date*, WASHINGTON POST (June 12, 2013), https://www.washingtonpost.com/news/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

[28] *FISA Amendments Act of 2008*, WSJ.COM, (June 19, 2008) *available at* http://www.wsj.com/articles/SB121391360949290049.

[29] *See generally* Rainie & Madden, *supra* note 4.

[30] *See In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 2016 WL 618401 (an unpublished case).

[31] *Id.* at 1.

[32] Danny Yadron & Spencer Ackerman, *Apple accused of trying to make iPhones 'warrant-proof' in FBI case*, THE GUARDIAN (Mar. 10, 2016).

[33] *Id.*

compel private companies to hand over raw information, as opposed to software. These questions are exacerbated by the many other gaps and unsettled law surrounding an individual's right to the private data they generate and the government's role in protecting or exploiting that data.

B. REGULATION OF BIG BUSINESS AND PRIVATE INDUSTRY AGAINST INDIVIDUAL PRIVACY AND SECURITY CONCERNING ELECTRONIC DATA

In recent years, the line has blurred between government and private sector data regulation. Like the government, private businesses are mainly left to self-regulate their inflow of personal data, save for a few industry-specific laws. Some businesses profit by selling personal data back to the government, and sometimes a government demands that personal data be turned over for whatever purpose they are pursuing at the time.[34] Therein lies the issue with the patchwork approach and the deference given to companies for self-regulation. As Paul Schwartz observes, "personal information in the private sector is often unaccompanied by the presence of basic legal protections.[35] Yet, private enterprises now control more powerful resources of information technology than ever before."[36] What many are just beginning to realize is that a great threat to individual privacy is coming from thousands of companies, most have likely never heard of, and the government is not doing anything to stop it. In fact, they are participating in the name of commerce.[37]

One such company is Booz Allen, which works with the government as independent contractors. [38] After Booz Allen was made famous by the recent Edward Snowden information leak, it was revealed almost "500,000 private employees held top-secret clearances in 2012,

---

[34] Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Mar. 9, 2014), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/. [*hereinafter* Data Brokers]. *See also* Alex Hern, *FBI 'could force Apple to hand over private key'* (Mar. 11, 2016), http://www.theguardian.com/technology/2016/mar/11/fbi-could-force-apple-to-hand-over-private-key; *see e.g.* Mark Gordo & Martha Mendoza, *AT&T, Verizon and Sprint Push Back Against the NSA, Too,* ABQ J., (Mar. 3, 2014), https://www.abqjournal.com/362115/telecoms-push-back-on-proposed-nsa-plan.html.

[35] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1633 (1999) (internal citations omitted).

[36] *Id.*

[37] *See* Data Brokers, *supra* note 34.

[38] Norm Ornstein, *Edward Snowden and Booz Allen: How Privatizing Leads to Crony Corruption*, THE ATLANTIC (June 20, 2013), http://www.theatlantic.com/politics/archive/2013/06/edward-snowden-and-booz-allen-how-privatizing-leads-to-crony-corruption/277052/.

giving them access to the most sensitive secrets of the United States, with much of the clearance process itself done by . . . the same private contractors."[39] This issue is compounded by the fact that the government also demands access to private company records from non-contracted companies.[40] Accordingly, among Edward Snowden's revelations was that the government was gathering data directly from the servers of Google, Microsoft, and Facebook.[41]

Data transfer also comes from another vantage point: not from leaks or direct collection by government, but private collection of personal data by "data brokers."[42] For example, the company Epsilon claims to have "'the world's largest cooperative database' including more than 8 billion consumer transactions combined with an extensive network of online sources."[43] While certain government entities have expressed their disdain for companies like Epsilon and even claimed to have proposed legislation curtailing their practices, Epsilon has provided the Senate Commerce Committee with binders full of information but has not taken any steps to utilize the information given.[44] The CEO of Epsilon has called the hearings "political theater" and sees no need for more oversight or regulation of one of the fastest-growing sectors of the economy.[45]

These so-called "Data Brokers," a concept largely brought to light by Snowden, mark a pivotal shift in governmental collection of data in its own regard and about its relationship with private companies.[46] This shift occurred because the public was finally made aware that private companies are not regulated in this arena and are left to police themselves. Phone industry executives have privately told administration officials they do not like the idea of storing phone records gathered by the NSA because they do not want to become the government's data minders.[47] Companies say they are wary of being forced to standardize

---

[39] *Id.*

[40] *Id.*

[41] Allegations about NSA Prism program verified by top secret documents released on Wikileaks. *See* Lee, *supra* note 26.

[42] *See* Data Brokers*, supra* note 33.

[43] *Id.*

[44] *Id.* (The Senate Commerce Committee and its chairman, Jay Rockefeller, have proposed legislation that calls for more oversight and transparency).

[45] *Id.*

[46] *Id. See e.g.*, *supra* note 35.

[47] Gordo & Mendoza, *supra* note 34.

their own data collection to conform to the NSA's needs.[48] Despite being wary, it has been "extremely unusual for telecoms to resist any requests from the government," according to software engineer Zaki Manian of Palo Alto who advocates against mass government surveillance.[49]

The reality is that private companies have been purchasing data from private companies for decades, starting with the telecommunication industry and expanding.[50] Today, companies including AT&T and Verizon have come forward admitting they sold data to the government and to other companies targeting specific consumers.[51] Now these companies are questioning the continuance of these practices.[52] Shockingly, there is little governing these sorts of transactions. Moreover, there is a lack of incentive to enact more law in this arena because it would require the government to jump through hoops to get the data they "need to protect their nation and its citizens."[53]

Apart from the government's attempts to curtail this brokerage of personal data, there is an actual need to reign in the sale of personal data as a commodity. These sales jeopardize the privacy of thousands of individuals each day, and the government has done nothing concrete to assign responsibility. In fact, there is evidence that facets of the government, like the NSA, take part in these unregulated exchanges. Given these problems, it is clear that the United States' current patchwork approach to data security provides no oversight in vulnerable areas. This lack of oversight leaves private information and consumer data free to be hacked or purchased by the highest bidder. The only answer seems to be a comprehensive approach that will apply to all data exchanges.

C. DATA REGULATION IN THE EUROPEAN UNION AND ITS APPROACH DATA TO SECURITY AMONGST ITS CITIZENS AND ABROAD

Digital companies domiciled in the European Union (EU) conduct business inside and outside the EU; and of course, the same is

---

[48] *Id.*

[49] *Id.*

[50] *See* Data Brokers, *supra* note 33.

[51] Gordo & Mendoza, supra note 34.

[52] *Id.*

[53] Dan Roberts and Spencer Ackerman, Anger swells after NSA phone records court order revelations, The Guardian, (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

true for companies in the United States. Yet, the difference is the EU has developed a more comprehensive data protection directive than its counterpart.[54] The established directive sets forth rigorous government oversight and requires compliance by all 27 member states.[55] That is not to say that the EU has it all figured out, as the directive allows for significant variations among the member states and enforcement has not been consistent in practice.[56]

The background and underlying philosophy of the Directive differs in important ways from that of the United States. As noted above, the United States has, in recent years, left the protection of privacy to markets and private regulation rather than law. In contrast, "Europe treats privacy as a political imperative anchored in fundamental human rights."[57] The EU Data Protection Directive also contains restrictions on the flow of personal data outside the borders of EU nations to countries not governed by the Directive.[58] Data can be transferred to a third country if the country "ensures an adequate level of protection."[59] The goal of the Directive is comprehensive reform, "to give citizens back control over of their personal data, and to simplify the regulatory environment for business. "The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised."[60]

Given the differences in approach, when dealing internationally with the United States, the EU has relied upon a Safe Harbour Agreement to increase the level of protection afforded to their citizens by US companies. Moreover, the United States and the EU share the goal of "enhancing privacy protection for their citizens" and allowing free uninhibited international trade, but take varying approaches to achieve this goal. Accordingly, the U.S. Department of Commerce in consultation with the European Commission developed a 'safe harbor' framework in attempt to close the gap between the different approaches when data is exchanged between the two countries.[61] After several rounds

---

[54] *See* Sangar, *supra* note 9.

[55] *Id.*

[56] *Id.*

[57] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* 38 HOUS. L. REV. 717, 730 (2001).

[58] Council Directive 95/46, art. 25, 1995 O.J. (L281/31) 1 (EC).

[59] *Id.*

[60] European Commission, *Protection of Personal Data*, http://ec.europa.eu/justice/data-protection/ (last updated Nov. 24, 2016).

[61] 1-Intellectual Property, (Nov. 1, 2016) https://www.export.gov/article?id=Privacy-Shield-Safe-Harbor.

of negotiation, the Safe Harbour Agreement was enacted as a result of the European Commission's Directive on Data Protection.[62] That directive went into effect in October of 1998, and "would prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) 'adequacy' standard for privacy protection."[63] The Safe Harbour Agreement provides in part:

> All 28 Member States of the European Union will be bound by the European Commission's finding of "adequacy";
>
> Participating organizations will be deemed to provide "adequate" privacy protection;
>
> Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted;
>
> Claims brought by EU citizens against U.S. organizations will be heard, subject to limited exceptions, in the U.S.; and
>
> Compliance requirements are streamlined and cost-effective, which should particularly benefit small and medium enterprises.[64]

In the case of C-362/14 *Schrems v. Data Protection Commissioner,* 2015 E.C.R I- 1, the Court of Justice of The European Union (ECJ), invalidated the Safe Harbour Agreement.[65] In that case, Austrian law student Maximilian Schrems filed a complaint with the Irish Data Protection Commissioner, claiming the Safe Harbor did not adequately protect his Facebook data that was stored in the United States and subject to government surveillance.[66] Though the Irish Data Protection Commissioner rejected Schrems' claim, he appealed to the ECJ, who ruled on the issue.[67] After the ruling, Schrems went on record commenting, "I very much welcome the judgment of the court," calling it a "major blow" for US surveillance and saying it "makes it clear that US businesses cannot simply aid US espionage efforts in violation of

---

[62] *See* Commission Decision 2000/520/EC of 26 July 2000, Safe Harbour Agreement, 2000 O.J. (L 215) 7.

[63] *See* 1-Intellectual Property, *supra* note 61.

[64] U.S.-EU Safe Harbor Overview, http://2016.export.gov/safeharbor/eu/eg_main_018476.asp (last updated Dec. 18, 2013).

[65] Case C-362/14, Schrems v. Data Protection Commissioner, 2015 E.C.R. I-1.

[66] *Id.*

[67] Sharon Shea, *Safe Harbor agreement invalid: Privacy win or enterprise woe?* (Oct. 9, 2015), http://searchsecurity.techtarget.com/news/4500255226/Safe-Harbor-agreement-invalid-Privacy-win-or-enterprise-woe.

European fundamental rights."[68] Schrems also acknowledged, "This case law will be a milestone for constitutional challenges against similar surveillance conducted by EU member states."[69] Schrems insinuates what many others are thinking: there are many other cases to be resolved and greater resolution will be essential to regulate data privacy going forward. No matter his personal thoughts, as a direct result of his suit, companies like Facebook are in flux and unsure of what this means for the transfer of data that is going on in the present without a coherent rule of law to follow.

D. FUTURE INTERNATIONAL AGREEMENTS AND THEIR ANTICIPATED DOWNFALLS

With the world becoming more globalized and the gaps in data privacy standards becoming more evident, this issue must be resolved. It seems, however, that courts and legislatures are struggling to quash citizens' fears and maintain at least a minimal amount of data security because of the acknowledged ease that comes with unfettered access to individual data. One thing is for sure; after the ECJ struck down the Safe Harbor Agreement in the *Schrems* case, something must change.

One step the global community is taking comes in the form of multi-nation partnership agreements. Notably, the Trans Pacific Partnership Agreement (TPP) passed by the United States and eleven other countries aims to create a standard platform for free flowing information, while addressing policy objectives such as private personal information.[70] While this agreement covers a wide range of technological issues, the key paragraph regarding data privacy reads rather vaguely. It states that "TPP Parties commit to ensuring free flow of the global information and data that drive the Internet and the digital economy, subject to legitimate public policy objectives such as personal information protection."[71] Regarding transnational flow, the TPP's only concern is that the host country does not favor national parties over

---

[68] *Id.*

[69] *Id.*

[70] *TPP's electronic commerce chapter: EU trade buff's take note*, BORDERLEX (October 6, 2015) http://www.borderlex.eu/blog-tpps-electronic-commerce-chapter/.

[71] Press Release, Summary of the Trans-Pacific Partnership Agreement, Ministers of the 12 Trans-Pacific Partnership Countries (Oct. 4, 2015) (available at https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership).

international.[72] The pertinent articles necessitate that "the 12 Parties also agree not to require that TPP companies build data centers to store data as a condition for operating in a TPP market, and, in addition, that source code of software is not required to be transferred or accessed."[73] The chapter also prohibits "the imposition of customs duties on electronic transmissions, and prevents TPP Parties from favoring national producers or suppliers of such products through discriminatory measures or outright blocking."[74]

Despite its vague directives, international data experts are taking note.[75] For example, 'Borderlex', a renowned EU trade blog warns that "EU trade buffs need to look very closely at TPP's electronic commerce chapter" because Europe hopes to pass its equivalent of the TPP under the title Trade in Services Agreement (TiSA) with the United States as a party to this agreement as well.[76] The blogger poses the idea that political backing in Washington D.C. will put the United States in a stronger position to negotiate.

This paper calls for a balance between the freedom of flow of information to promote national security and international trade versus individual's rights to keep their data private. The crux of the issue is that privacy concerns will be heightened as the flow globalized trade continues to increase, unless some measures are taken to curb these data transfers. This problem is especially pertinent as experts warn that the United States is emerging "as the global rule maker" in the digital arena.[77]

III. ANALYSIS

A. THE CURRENT US STANDARD WILL NOT SUFFICE TO SERVE AS A MODEL FOR THE INTERNATIONAL COMMUNITY

As previously discussed, privacy is essential to the American way of life. "It permits us to create and maintain private lives from which spring personal identity, self-determination, freedom and, ultimately,

---

[72] *Id.*
[73] *Id.*
[74] *See TPP's electronic commerce chapter*, *supra* note 70.
[75] *See Id.*
[76] *Id.*
[77] *Id.*

happiness."[78] The American government has tried to reconcile the need to collect data, both publicly and privately, with the privacy of individuals with little to no avail. As a result of this struggle, there is no single comprehensive federal law regulating the collection and use of personal data. In the United States, there is a "patchwork system of federal and state laws and regulations that overlap. . . and contradict one another."[79] In addition, "there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices."[80] Of course, the US government has recognized the gaps and contradictions but this exacerbates the issue because more regulation is created and more contradictions are put into force.[81] While it is significant that the Federal Government has recognized this issue and is seeking solutions, the problem is that they are continuing to work toward an unobtainable solution using a desultory patchwork approach. The reason this goal is unobtainable is the ever-singular approaches taken by lawmakers to try to chip away at a widespread problem instead of adopting a proactive comprehensive approach that would secure protection in a variety of instances. Technology is always changing; it is difficult, if not impossible, to catch up to the continual change with a reactive patchwork approach.

In 2014, the White House led a 90-day review of big data and privacy.[82] The group charged with that task found that we live in a world of near-ubiquitous data collection in which that data is being crunched at speeds increasingly approaching real time.[83] They characterized it as a sort of "data revolution."[84]That study also noted some fears stemmed from this data revolution. Former advisor to the President and author of this study, John Podesta noted specifically:

> . . . big data technologies raise serious concerns about how we protect personal privacy and our other values. As more data is collected, analyzed, and stored on both public and private systems, we must be

---

78 Simpson, *supra* note 1.

79 Ieuan Jolly, *Data Protection in the United States: overview*, THOMPSON REUTERS (July 1, 2016), http://us.practicallaw.com/6-502-0467#a57587.

80 *Id.*

81 *Id.*

82 John Podesta, *Big Data and Privacy: 1 Year Out,* THE WHITE HOUSE (Feb. 5, 2015), https://www.whitehouse.gov/blog/2015/02/05/big-data-and-privacy-1-year-out.

83 *Id.*

84 *Id.*

> vigilant in ensuring the balance of power is retained between government and citizens and between businesses and consumers. And one novel finding of the working group report was the potential for big data technologies to circumvent longstanding civil rights protections and enable new forms of discrimination in housing, employment, and access to credit, among other areas.[85]

The big data and privacy report offered as one of its six chief recommendations that the government seek to ensure that data collected on students in school is used only for educational purposes, and that students be protected against their data being shared or used inappropriately.[86] The goal of this policy is to "ensure that students' privacy is protected in the educational context and that their education data is not mined for commercial or marketing purposes." Notably, laws such as the Student Data Privacy Act are well-intended, but like other data privacy laws in the United States, only extend to one particular area and do not address the full scope of ramifications.

Other key federal privacy bills introduced in 2015 include in terms of education: H.R.B. 2092 (Student Digital Privacy and Parental Rights Act) would prohibit operators of websites, applications and other online services from selling students' personal information to third parties and using or disclosing students' personal information to tailor advertising to them. The bill would also give parents access to information held about their children and allow them to correct it, delete information about their children that schools do not need to retain, and to download any material their children have created.[87]Also, in terms of data brokerage, a more direct requirement: S.B. 668 (Data Broker Accountability and Transparency Act) would, among other things: require data brokers to establish procedures to ensure the accuracy of the personal information they collect, assemble, or maintain; and any other information that specifically identifies an individual, (unless the information only identifies an individual's name or address); require data brokers to provide individuals' a cost-free method to review their personal or identifying information; allow individuals to dispute the accuracy of their personal information with a written request that the data broker make a correction.[88]

---

[85] *Id.*

[86] *See generally* Jolly, *supra* note 79.

[87] *See* Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

[88] *See* Data Broker Accountability and Transparency Act of 2015, S. 688, 114th Cong. (2015).

While these examples are plentiful and are well-intended laws, the issues are numerous. For example, what is considered an "educational purpose," and what happens to student records that are transferred abroad? What if international education based companies are required to follow these privacy regulations? Many international companies publish student data to create more comprehensive textbooks or classroom activities; what regulations, or penalties apply to them? What about international students in the US? These issues are not addressed in a domestic and sector specific law such as the Student Data Privacy Act; even education has become globalized to the extent a need for a comprehensive international data privacy framework has become paramount.

The proliferation of security breaches in recent years has led to an expansion of this patchwork system of privacy laws, regulations, and guidelines, which is becoming one of the fastest growing areas of legal regulation.[89] The combination of an increase in interstate and cross-border data flow, together with the increased enactment of data protection related statutes, heightens the risk of privacy violations and creates a significant challenge for a data controller to negotiate the onerous and often inconsistent requirements for each state when operating at a national or international level.[90] Therein lies the issue of transfer of personal data outside the United States, where there are very few restrictions. Several states have enacted laws that limit or discourage state agencies or state contractors from outsourcing data processing beyond US borders. These laws, however, are typically limited to state government agencies and private companies that contract to perform services for state agencies and are not realistic in a capitalistic economy that naturally encourages growth through international operation.[91]

Another issue is the self-regulatory frameworks that have developed in an attempt to establish accountability and create tools for enforcement.[92] Established by regulators like the Federal Trade Commission (FTC), the self-regulatory frameworks aim to close the gaps and flush out the contradictions between laws that span across different sectors not originally intended to span across those sectors. "[T]he position of the FTC and other regulators is that the applicable US laws

---

[89] *See id.*
[90] *Id.*
[91] *See id.*
[92] *Id.*

and regulations still apply to the data after it leaves the United States, and US regulated entities remain liable for [1] data exported out of the United States [2] the processing of data overseas by subcontractors."[93]

Subcontractors use the same protections (such as through the use of security safeguards, protocols, audits, and contractual provisions) for the regulated data when it leaves the country.[94] "There are few express restrictions on storing personal data outside the United States, but some states have restrictions on data access, maintenance, and processing from outside the United States with respect to government contracts and off-shore outsourcing situations. Otherwise, a requirement to store personal data in the United States usually manifests as a contractual requirement where a customer is apprehensive about sensitive data being stored in jurisdictions that are perceived as having a weak personal data protection regime."[95] This problem is sourced in agreements like the Safe Harbour Agreement and remains the primary purpose of international data privacy agreements.

B. IMPLICATION OF SCHREMS AND WHY IT IS NOT FEASIBLE TO CONTINUE TO MAINTAIN THE VARYING AND AMBIGUOUS STANDARDS OF SECURITY BETWEEN DEVELOPED NATIONS

Prior to 2015, countries with different standards of data security managed their differences by conducting business with agreements modeled after the US-EU Safe Harbour Agreement.[96] Since the European Court of Justice' ruling in the *Schrems* case that the EU-US Safe Harbor scheme is now invalid, these agreements have been largely removed. Schrems[97] claimed his privacy had been infringed by the NSA's mass surveillance programs, specifically PRISM. Schrems resides in Australia, but brought the case against Facebook in Ireland because the company's European headquarters are in Dublin.[98] The Data Protection Commissioner, Ireland's data regulator, rejected his case because it was bound by the Safe Harbour Agreement, which *Schrems* subsequently

---

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *See generally* Margaret Rouse, *Safe Harbor*, WhatIs.com, http://searchcio.techtarget.com/definition/Safe-Harbor.

[97] Schrems, 2015 E.C.R. at I-1 (As indicated above, Schrems is a privacy activist who brought a case against Facebook in Ireland).

[98] *Id.*

appealed, resulting in the current European Court of Justice ruling, invalidating the Agreement.[99]

Yet, given the continual necessity of data exchanges for trade and business, companies continue to transfer data with one another, though largely uncertain of the standards they are operating under.[100] In attempts to provide tools for companies to navigate in the interim, the EU published guidelines in which it indicated a need to clarify "under which conditions transfers can continue."[101] Regarding these conditions, it provides the following: (1) "data transfers can no longer be based on the Commission's invalidated Safe Harbour Decision;" (2) "[s]tandard Contractual Clauses (hereafter also: "SCCs") and (3) Binding Corporate Rules (hereafter also: "BCRs") can in the meantime be used as a basis for data transfers."[102] The statement also called on Member States to maintain open discussions with the United States in order to find the best legal and technical solutions for future data transfers.[103]

It is important to note that it is not just the EU and the United States that have been affected, but other countries as well. For example, the Abu Dhabi Global Market (ADGM) provides certain regulations for transfers outside their state.[104] The ADGM Regulations state that "transfers of personal data to recipients located outside ADGM may only take place if an adequate level of protection for such data is ensured by laws applicable to the recipient."[105] Accordingly, the ADGM Registrar has designated a list of jurisdictions to the Regulations that it deems to provide an adequate level of protection for personal data. This list includes "United States of America, subject to compliance with the terms of the applicable US-EU or US-Switzerland Safe Harbours."[106] The full

---

[99] *Id.*

[100] *See* Kelli Clark, *The EU Safe Harbor Agreement Is Dead, Here's What to do about It*, FORBES.COM (Oct. 27, 2015), http://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/#68b4ef567171.

[101] *Commission Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14,* at 5, COM (2015) 566 final (Nov. 11, 2015).

[102] *Id.*

[103] *Id.*

[104] Wilkinson, et al., *Schrems: the global impact – how the ECJ ruling is affecting countries outside the EU and US*, DATA PROTECTION REPORT (Nov. 2, 2015), http://www.dataprotectionreport.com/2015/11/schrems-the-global-impact-how-the-ecj-ruling-is-affecting-countries-outside-the-eu-and-us/.

[105] *Id.*

[106] *Id.*

effects of the *Schrems* decision on this passage have yet to be determined.

Australia has experienced minimal material effects thus far.[107] The Australian government seems to be most concerned about the second prong of the ECJ *Schrems* decision, "namely a lack of mechanisms under which an Australian citizen could enforce privacy protection in the recipient's country."[108] This has caused Australia to operate under alternative mechanisms such as APP 8.1. In practice, APP 8.1 "requires the disclosure to include a detailed privacy provision in its agreement with the recipient."[109] While this mechanism might work for the time being, it is not a permanent solution because it casts a large burden onto the individual, who in turn is responsible for negotiating a stricter privacy agreement if they deem necessary.[110] In comparison, South Africa operates to satisfy the standards of the Protection of Personal Information Act 2013 (POPI). "POPI is largely based on the principles of the EU Data Protection Directive."[111] This includes the requirement that personal information must be adequately protected when transferred cross-border (assuming none of the other grounds apply). To date, "US corporations had attempted to rely on their Safe Harbour certification when demonstrating the adequacy of their data protection capabilities to South African companies."[112] "In light of the *Schrems* case, this is unlikely to be acceptable [as t]he ECJ's ruling [will] have a bearing on the manner" in which many countries conduct business with US corporations and even the Government itself.[113] One of the greatest effects could come in South Africa.[114] "The information regulator (once appointed) [is expected to] enforce the requirement of adequacy in POPI once it is in full force."[115] "In the meantime, South African companies with EU-based operations [are reviewing] their contractual arrangements for data transfer to the US" in efforts to maintain trade while ensuring protections.[116]

---

[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.*

While some implications have been seen abroad, many articles indicate it is too early to classify the repercussions of the ruling in the United States. The ruling allows individual European countries to set their own regulation for US companies' handling of citizens' data, vastly complicating the regulatory environment in Europe.[117] Countries can also choose to suspend the transfer of data to the United States, forcing companies to host user data exclusively within the country.[118] We know what the ruling allows, but since the enforcement of these decisions like *Schrems* are left to individual actors within these foreign nations, we do not yet know the full effect.

It would be a waste of an opportunity to wait to feel the full effect after these respective decisions are made certain. Many countries are demonstrating uncertainty and lacking guidance. It is a crucial time for countries to come together to establish a standard guide or designate a benchmark that each country must meet in order to conduct international business. Such a standard would render enforcement decisions unnecessary and provide a global practice moving forward, allowing all countries to operate on the same page while increasing individual protections, especially in the United States.

The United States, however, would likely take issue with a global standard. The government would either need to establish a law or regulation requiring companies to provide certain privacy standards, or these companies themselves would need to be involved in these international negotiations. Both scenarios pose problems. On one hand, the US government seems to favor its patchwork approach, as it allows businesses to operate "lassiez faire" and requires less actual regulation on the part of the government and its administrative agencies. On the other hand, bringing so many actors to the negotiating table, including big business with deep pockets and influence, would potentially side track the negotiations. It is hard to imagine an instance where the US Congress would be willing to impose a restrictive statute on domestic companies unless there was great influence on an international scale. With the world in flux after the *Schrems* case and potential loss of business in American technology firms, this seems to be the time where that influence would be the greatest, and in following, the best time for that influence to be put to the test.

---

[117] *Id.*
[118] *Id.*

C. SO NOW WHAT? PROPOSED STANDARD: THE IMPLICATIONS, THE REMEDIES IT WILL PROVIDE AND POSSIBLE SHORTCOMINGS

Although the United States and the EU have made strides in personal privacy regulation, governments, regulators, and private companies still struggle to find clarity amidst a sea of contradicting laws that may or may not apply to them, either domestically or in an international context.[119] Several scholars have criticized the applicability of information privacy laws to ever increasing collection of personal information gathered by large globalized corporations.[120]An international standard would mean that regulations adopted by world powers such as the United States, the EU, Russia, and China would transfer by trade to smaller countries, spreading higher protections on a world-wide basis. Achieving this goal would require, in part, a regulatory commission with enforcement power to enact new rules as technology changes and evolves.

Recently, there has been movement to create a commission through the UN Human Rights Council in Geneva.[121] In 2015, the Human Rights Council adopted the establishment of a new UN Special Rapporteur on "The Right to Privacy in the Digital Age."[122] "[T]he mandate of the Special Rapporteur will include special consideration of issues related to the digital age and new technologies, including surveillance. This focus led to many disagreements in drafting sessions, but eventually the Human Rights Council adopted the Resolution without a vote."[123] There is precedence that change can be effectuated through a special rapporteur to the UN Human Rights Council. Experts believe that "if the work of the UN Special Rapporteur on Freedom of Expression is any indication, we can expect this new independent expert to bring some

---

[119] *Id. See also* Gordo & Mendoza, *supra* note 34.

[120] *See, e.g.,* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution,* 86 MINN. L. REV. 1137, 1140 (2002); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 S. CAL. L. REV. 1083, 1084 (2002). Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373 (2000); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internent,* 17 BERKELY TECH. L. J. 1085 (2002); Stan Karas, *Privacy, Identity, Databases,* 52 AM. U. L. REV. 393 (2002).

[121] Nicolas Seidler, *UNHRC Creates New UN Special Rapporteur on "The Right to Privacy in the Digital Age"*, INTERNET SOCIETY (Mar. 26, 2015), http://www.internetsociety.org/blog/public-policy/2015/03/unhrc-creates-new-un-special-rapporteur-"-right-privacy-digital-age".

[122] *Id.*

[123] *Id.*

useful human rights insights into some of the key privacy issues that affect people today, whether online or offline."[124]

Another possibility is the TPP. The TPP is a free trade agreement that was negotiated starting in 2010, by twelve countries of the Pacific realm: Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United States, and Vietnam.[125] The involved countries represent almost 45 percent of the global GDP.[126] Given what we know, the TPP is another agreement that has the potential to create change. The public has been kept in the dark during the TPP negotiation process, which was concluded and passed on October 5, 2015. The TPP negotiations have lacked transparency and multi-stakeholder participation, with the only players involved being the member governments and cleared advisors from large companies.[127] The public at large knows the TPP only through leaks.[128] Even members of public interest groups and federal legislators, after being denied the text for years, are only now being provided limited access to the text.[129] What we do know has been criticized by experts as a threat to the citizens of the member countries.[130] "The draft agreement is composed of twenty-nine chapters, and at least three chapters (the intellectual property chapter, the services chapter, and the e-commerce chapter) could have a negative impact on Internet freedoms and human rights online.[131] The latter two chapters could have a negative impact on information flow, Internet Service Provider liability, and more."[132]

The TPP chapter on intellectual property (IP) aims to impose more stringent copyright norms, including: extraordinarily long copyright terms; the criminalization of small-scale infringement; the

---

[124] *Id.*

[125] Trans-Pacific Partnership Agreement, *supra* note 71.

[126] Office of The U.S. Trade Representative, *Overview of the Trans Pacific Partnership*, https://ustr.gov/tpp/overview-of-the-TPP (last visited Feb. 15, 2017).

[127] Eric Bradner, *How secretive is the Trans-Pacific Partnership?*, CNN, (June 12, 2015) http://www.cnn.com/2015/06/11/politics/trade-deal-secrecy-tpp/index.html.

[128] *Trade in Services Agreement Annex on [Electronic Commerce]*, WIKILEAKS (Sep. 16, 2013), https://wikileaks.org/tisa/ecommerce/05-2015/TiSA-Annex-on-Electronic-Commerce.pdf.

[129] *See TPP: The "Trade" Deal that Could Inflate Your Healthcare Bill*, Public Citizen, (July 2014), http://www.citizen.org/documents/TPP-threats-to-US-healthcare.pdf.

[130] *See Trans-Pacific Partnership (TPP): Expanded Corporate Power, Lower Wages, Unsafe Food Imports*, Public Citizen, http://www.citizen.org/tpp (last visited Feb. 15, 2017).

[131] Richard Warnick, Comment to *Robert Reich: TPP is Part of the Global Race to the Bottom*, ONEUTAH (Feb. 1, 2015, 10:11 PM), http://www.oneutah.org/2015/01/robert-reich-tpp-is-part-of-the-global-race-to-the-bottom/.

[132] *Id.*

restriction over temporary copies; and the prohibition against breaking digital locks for legal purposes.[133] Clearly, these restrictive norms would negatively impact the rights of individuals in all negotiating countries, including the United States.

While an agreement modeled after the format of the TPP would be ideal, the problem is that only eleven countries and the United States are parties to the agreement. Most European countries believe that the negotiations were too private and that the limitations were not conducive to the general public. While countries cannot be forced to participate in any agreement that would limit their ability to transfer data, we need more than 11.2 percent of the population and more key players to force a global movement toward adopting any set of standards, whether based on the TPP or not. Such a movement would require most of the EU, China, Russia, the United States and Canada to participate: each is a major player that accounts for much of the world's online trade. Only then will major companies and other governments be obliged to participate and a new standard will take hold.

To determine the substantive content that would appeal to the EU, regulators should look to their current standards and what they hoped to achieve. Under current EU law, personal data can only be legally gathered under strict conditions and for a legitimate purpose.[134] Persons or organizations that collect and manage personal information must protect it from misuse and must respect certain rights of the data owners, which are guaranteed by EU law.[135] Every day within the EU, businesses, public authorities, and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries disrupt international exchanges of data and leave knowledgeable individuals to worry about the fate of their data. Individuals, like Schrems, may also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries. Therefore, common EU rules have been established to ensure that personal data is afforded a high standard of protection everywhere in the EU.[136] The benefit to the European Directive is that individuals have

---

[133] Trans-Pacific Partnership, chap. 18: Intellectual Property, https://www.mfat.govt.nz/assets/_securedfiles/Trans-Pacific-Partnership/Text/18.-Intellectual-Property.pdf (last visited Feb. 15, 2017).

[134] *See generally* Sangar, *supra* note 9.

[135] *Id.*

[136] *See Id.*

the right to complain and obtain redress if their data is misused.[137] The EU's Data Protection Directive also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of personal data when it is exported abroad. The caveat to the Directive is the United States, which does not abide by this higher level.[138]

Another possible solution is the TiSA. This agreement has the potential to be a single standard worldwide agreement. According to the infamous website Wikileaks and later published by European countries who agreed that publishing the terms is in the best interest of the public, TiSA is a more widespread agreement that is currently in negotiations.[139] TiSA is a trade agreement currently being negotiated by twenty-three members of the World Trade Organization (WTO), including the EU.[140] Together, "the TPP countries are the largest goods and services export market of the United States. U.S. goods exports to TPP countries totaled $698 billion in 2013, representing 44 percent of total U.S. goods exports."[141] TiSA is based on the WTO's General Agreement on Trade in Services (GATS), and includes all WTO members.[142] The key provisions of the GATS—scope, definitions, market access, national treatment, and exemptions—are also found in TiSA.[143] TiSA aims at opening up markets and improving rules in areas such as licensing, financial services, telecoms, e-commerce, maritime transport, and professionals moving abroad temporarily to provide services.[144]

The European Commission negotiates based on a mandate issued by the governments of the EU's twenty-eight member countries.[145] In March 2015, the EU agreed to publish this mandate.[146] TiSA is open to all WTO members who want to open up trade in services. China has

---

[137] European Commission*, supra* note 60.

[138] *Id. See generally* Schrems*,* 2015 E.C.R. at I-1.

[139] *Trade in Services Agreement Annex on [Electronic Commerce]*, WIKILEAKS (Sep. 16, 2013), https://wikileaks.org/tisa/ecommerce/05-2015/TiSA-Annex-on-Electronic-Commerce.pdf.

[140] *Id.* at 1.

[141] Office of The U.S. Trade Representative, *supra* note 126.

[142] *Id.*

[143] General Agreement on Trade in Services, Annex 1B, p. 283, WTO, (Jan. 1995), https://www.wto.org/english/docs_e/legal_e/26-gats.pdf.

[144] Tony Burke, *TiSA – the new trade deal being kept under wraps*, LEFT FOOT FORWARD, (July 27, 2015) https://leftfootforward.org/2015/07/tisa-the-new-trade-deal-being-kept-under-wraps/.

[145] European Commission, Trade in Services Agreement (TiSA), http://ec.europa.eu/trade/policy/in-focus/tisa/.

[146] *Id.*

asked to join the talks. The EU supports China's application because it wants as many countries as possible to join the agreement[147] to increase TiSA's legitimacy and attention while spreading the standard to all corners of the world.

If enough WTO members join, TiSA has the potential to become a comprehensive and enforceable WTO agreement and see its benefits extended beyond the current participants. TiSA negotiations are in the early stages and although the latest report on progress of TiSA negotiations for the 15th round was reported as "very good," negotiations still remain before an agreement can be reached and put into force.[148] The next TiSA negotiation is scheduled to take place during "the first week of February 2016 and will be organized and chaired by the US."[149] The talks are based on proposals made by the participants.[150] Overall, TiSA would be a step in the right direction for data security, however, the public knows too little at this time to deem this strategy a worthwhile solution to the issues at hand. Some basic requirements would need to be fulfilled in order to be a worthwhile solution.

The latest and perhaps the most comprehensive and realistic attempt to fill the gap left by the invalidation of the Safe Harbour agreement has come from the European Commission and the United States. As of February 6, 2016, the European Commission and the US Department of Commerce have agreed on a new framework for transatlantic data flows, and have referred to the new agreement as the EU-US Privacy Shield.[151] The agreement sets forth to accomplish the following:

> The new arrangement will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities. The new arrangement includes commitments by the U.S. that possibilities under U.S. law for public authorities to access personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, preventing generalised access.

---

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

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

> Europeans will have the possibility to raise any enquiry or complaint in this context with a dedicated new Ombudsperson.[152]

Proponents of this agreement hope this will assure people that their personal data is "fully protected."[153] The next steps will be to seek adoption of the agreement by the College after obtaining the advice of the Article 29 Working Party and after consulting a committee composed of representatives of the Member States.[154] In the meantime, the United States must make the necessary preparations to put in place the new framework and monitoring the mechanisms to do such.[155]

The *Schrems* case sparked public awareness on the issue of data privacy and if pending cases are similarly decided, the need for a worldwide standard is necessary. Not any agreement, however, will be substantively sufficient. Ideally, a new strategy, whether it be TiSA or a new agreement altogether, would adopt a more streamlined approach with higher standards. Preferably, an agreement formatted akin to the North American Trade Agreement (NATO)—an agreement between twenty-eight states that would take hold of its member states and govern their data protection schemes for years to come.[156] While such an agreement has its downfalls, it could be looked at as a model, updated as time goes on in order to garner more state participation. In order to garner more state participation, the content of the agreement needs to reflect the ideals of the EU, as the EU is a leader in data privacy and a close trade partners with the United States. With the EU on board, it would also be more likely that a transnational agreement would command the market of transnational data, forcing other world powers to sit up and take note.

IV. CONCLUSION

In conclusion, a more stringent and uniform approach to data protection will allow for free flowing trade and individual liberty while still permitting governments to monitor online exchanges for terrorism and other security threats. With the world becoming more globalized, and the issue of data exchanges becoming more clouded, lawmakers are

---

[152] *Id.*
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] North American Free Trade Agreement, U.S.-Can.-Mex., Dec. 17, 1992, 32 I.L.M. 289 (1993).

struggling to quash the fears of its citizens and maintain at least a minimal amount of data security while acknowledging the ease that comes with unfettered access to individual data.

To date, U.S. corporations have attempted to rely on their Safe Harbor certification when demonstrating the adequacy of their data protection capabilities to outside countries and international companies.[157] In light of the *Schrems* case, this reliance is not satisfactory. To further exacerbate the issue, the EU has developed a more comprehensive data protection directive than the United States. The established Directive sets forth rigorous government oversight and requires compliance by all twenty-seven member states. While the Directive addresses the problem of lack of protection and allows for variation among the member states, enforcement has not been consistent and would need to be improved upon if used as a model for a larger scale standard.[158]

While promising groundwork exists, the problems with existing standards make establishing a needed overarching solution a very difficult and time consuming journey. Despite these difficulties, the European Commission and the United States have agreed on a new framework for transatlantic data flows, the EU-US Privacy Shield;[159] combining the best of the European approach on a larger scale, while accounting for slight differences between domestic laws. The problem is that this agreement exists only between the United States and the EU and lacks certain enforcement mechanisms that are necessary to enforce it on a multinational scale. In a separate attempt to establish a standard of individual protection, the U.S., EU and twenty-two other countries came together to directly address some of the issues highlighted in the *Schrems* case.[160] Although negotiations surrounding TiSA have been kept under wraps, proponents have theorized that TiSA is being drafted to open up markets and improve oversight.[161] Despite its downfalls, this agreement is a good model for what is needed. Given the infrastructure, TiSA has the potential to be the first step to ensure secure transnational data transfers.

The recent changes in the political landscape, most notably, the Trump administration and the United Kingdom backing out of the

---

[157] European Commission, *supra* note 60.

[158] *See* Sangar, *supra* note 9, at 2.

[159] European Commission, *supra* note 60.

[160] *See* Burke, *supra* note 144. *See also Trade in Services Agreement*, WIKILEAKS (Oct. 14, 2016), https://wikileaks.org/tisa/.

[161] *See id.*

European Union could add another wrinkle to the already complicated world of international trade agreements. Most recently, U.S. opponents, have cast the TPP "as a secretive deal that favoured big business and other countries at the expense of American jobs and national sovereignty."[162] While campaigning, Donald Trump called the TPP, a "horrible deal."[163] As of January 23, 2017, Donald Trump used an executive order to pull out of the TPP.[164] Arguably, the United States pulling out renders the agreement "meaningless" to the other signatories.[165] Other signatories say they might go ahead and attempt to forge a deal without the United States.[166] President Trump has not made clear whether United States would be open to negotiate a more satisfactory trade agreement, though it is doubtful given his economic platform.[167]

Negotiations with the TTIP "are at an earlier stage."[168] So while a TTIP agreement is more hopeful, "given President Trump's hostility towards trade deals in general it's unlikely to be plain sailing for that one either."[169] However, since scrapping the TPP, President Trump has called for a "much closer" relationship with Britain though it is unclear whether that close relationship would involve any sort of agreement or change to the EU-US Privacy Shield.[170]

Moving forward, and focusing on the prospect of a multiple party agreement like TiSA or a revised TTP, the likelihood that multiple countries can come together and agree on a solution to a problem like, the of lack of privacy brought to light by individuals like Schrems and Snowden; is slim to none. The questions only begin there. We also must think about how, even if parties manage to come to such an agreement, how will such an agreement be enforced? Could the EU-US Privacy

---

[162] *TPP: What is it and why does it matter?* BBC NEWS, (Jan. 23, 2017) http://www.bbc.com/news/business-32498715.

[163] *Id.*

[164] *Id. See also* Zoe Nauman*, A Don Deal Donald Trump pledges much closer relationship with Britain after scrapping landmark Trans Pacific Partnership agreement,* THE SUN, (Jan. 24, 2017) https://www.thesun.co.uk/news/2689219/donald-trump-pledges-much-closer-relationship-with-britain-after-scrapping-landmark-trans-pacific-partnership-agreement/.

[165] *TPP, supra* note 162.

[166] *Id.*

[167] *TPP, supra* note 162; *see also* Adam Chandler, *Trump Takes Office, Kills TPP*, THE ATLANTIC (Jan. 23, 2017) https://www.theatlantic.com/business/archive/2017/01/trump-tpp-dead/514154/.

[168] *TPP, supra* note 162.

[169] *Id.*

[170] Nauman, *supra* note 164.

Shield be applied on a multi-national level? Perhaps one way to do this is to create a compliance mechanism, with a Special Rapporteur enforcing compliance. This final option might be our best bet, given the circumstances. With such high stakes and no clear solution, it remains to be seen whether a large scale, comprehensive solution is even realistic. If it is not, how will the world manage without a standard on global data transfers in a post *Schrems* environment? Realistically, the issue will continue to be swept under the rug especially in the United States where trade and especially transnational data protection seems to be a low priority within the new administration.