Seattle Journal for Social Justice

Volume 14 | Issue 1 Article 14

4-24-2016

The Great Divide: Recent Trends Could Help Bridge the US EU Data Privacy

Patrick Troy Hatfield

The Great Divide: Recent Trends Could Help Bridge the US/EU Data Privacy Gap

Patrick Troy Hatfield

I. INTRODUCTION

You have heard the word "data" used in the news, on TV, and in numerous other mediums, but what does "data" mean? Tech companies, governments, and computer geeks deal with data, but the word doesn't seem to have much weight to the average person. It should. Google alters its search results to cater to you.[1] Amazon offers different products at different prices to different consumers.[2] The United States government collects phone records by the billions.[3] Blogs, websites, photos, bank statements—all of these involve data. Your data. Your information. Imagine if that information fell into the wrong hands and was used to intimidate you or your family. Imagine if it were being used to cheat you out of your hard-earned money. Now imagine if that same data could prevent a terrorist attack. Data can run the gambit of social concerns from freedom of speech to personal privacy to a nation's struggle to protect its citizens from harm. It has to be regulated, but how?

Answers to that question vary, and data security experts have long feared a clash between the US data privacy regime and that of the European Union

---

[1] Grace Nasri, *Is Google's Search Manipulation Hurting Customers?,* DIGITAL TRENDS (Nov. 5, 2012), http://www.digitaltrends.com/web/bias-and-google-shopping/.

[2] Anita Ramasastry, *Websites change prices based on customers' habits,* CNN.COM (June 24, 2005, 3:14 PM), http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/.

[3] Barton Gellman, *Edward Snowden, after months of NSA revelations, says his mission's accomplished,* WASH. POST (Dec. 23, 2013), https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

(EU).[4] Pending EU legislation could make that fear a reality. In 2012, a new regulatory structure was proposed that would replace the current EU Privacy Directive (Directive).[5] Under the current system, a rift exists between the EU and the United States over the US regime's prioritization of security over privacy.[6] The EU considers personal privacy to be a fundamental right.[7] However, the current Directive allows for exceptions and loopholes that have kept the differences in regimes from being too prohibitive for US business and government interests.[8] The pending legislation will remove many of these exceptions and loopholes, impose harsher restrictions for violations, and include new provisions that would further distance the EU regime from US norms.[9]

Although this may seem like a battle that will only affect big business and government interests, it has far-reaching implications for individual rights and freedoms. The way that these governments and businesses handle data privacy fundamentally affects personal privacy. For instance, Google and Facebook could have to alter the way they store personal data as a result of the EU legislation, which would change how personal information is maintained and accessed and could result in more stringent privacy protections for individuals.[10] Conversely, the EU legislation could restrict the storage of and access to information in such a way that would limit

---

[4] Alessandra Suuberg, *The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law*, 16 TUL. J. TECH. & INTELL. PROP. 267, 268–86 (2013).
[5] *Id.*
[6] *See* DAVID BENDER, WHICH REGIME OFFERS MORE ACTUAL PRIVACY – US OR EU?, (2014), *available at* LexisNexis 7189.
[7] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).
[8] Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L L. REV. 1095, 1110–1111 (2013).
[9] *See id.* at 1129.
[10] *See Fundamental Overhaul of EU Data Protection Regime Unveiled,* TAYLOR WESSING GLOBAL DATA HUB, http://www.taylorwessing.com/globaldatahub/article_eu_dp_regulation.html (last visited Dec. 6, 2014).

freedom of speech and could cause barriers to freely sharing and accessing previously public information.[11] Furthermore, the US government has espoused the idea that personal privacy may be infringed upon if it means that citizens are safe from threats, such as terrorism, while the EU has taken the opposite approach and has provided its citizens with privacy as an "absolute right."[12] These differing approaches have resulted in different means of achieving the same end—protection of the citizenry.

The EU employs an omnibus privacy structure, which means that no sector (or type of data) is left unprotected because all data is treated the same, regardless of what it is used for or what it contains.[13] This structure is largely considered to provide a great deal of privacy protection because of the reliance on uniformity, but detractors argue that it is slow moving and overly bureaucratic.[14] The presence of US businesses in Europe and the transference of data into the United States have been seen as hindrances to these protections because of the difference in the way the US government approaches data privacy.[15]

The United States employs a sectoral privacy structure. This structure allows different rules to pertain to different sectors because data can be more or less sensitive from sector to sector.[16] For instance, in the United States, medical information is treated very differently from other types of

---

[11] *See* Craig Timberg & Sarah Halzach, *Right to be Forgotten vs Free Speech*, WASH. POST (May 14, 2014), http://www.washingtonpost.com/business/technology/right-to-be-forgotten-vs-free-speech/2014/05/14/53c9154c-db9d-11e3-bda1 9b46b2066796_story.html.

[12] Alo, *supra* note 8, at 1102–1105.

[13] *Id.*

[14] BENDER, *supra* note 6.

[15] *See* Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227, 231 (2013).

[16] *See* BENDER, *supra* note 6.

data.[17] Data brokerage has been an area left largely outside of the umbrella of protections because of strong business interests and an emphasis on greater security.[18] This sectoral structure has made EU member states wary of allowing their data to be stored in the United States because they fear that businesses will be able to abuse the data and that US intelligence services will be able to search the data without cause.[19] The resulting rift between the two regimes has meant that data sometimes falls through the gray area in between, and, at times, citizens' rights have been left unprotected.

However, shifts in policy in both the United States and EU could speak to a more cooperative future between the two regimes. Despite the proposed legislation being seen as increasing the gap, there has been pushback among EU member states.[20] Security and anti-terrorism concerns have forced the EU to be more proactive and less reliant on US intelligence. While the EU maintains its focus on privacy within the realm of business and personal data, it has expressed the necessity of safety concerns with regard to the collection and access of data by governments.[21] Similarly, US policy has undergone a recent shift toward the mean by expressing a renewed interest in maintaining personal privacy. A recent White House report on "big data" echoed this sentiment, and there has been cooperation with Canada in protecting Canadian personal data.[22] Likely most compelling, however, are

---

[17] *Health Information Privacy*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html (last visited Dec. 6, 2014).
[18] *See* BENDER, *supra* note 6.
[19] *Id.*
[20] Konrad Lischka & Christian Stocker, *Data Protection: All You Need to Know About the EU Privacy Debate,* SPIEGEL ONLINE INT'L (Jan. 18, 2013), http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html.
[21] KRISTIN ARCHICK, CONG. RESEARCH SERV., U.S.-EU COOPERATION AGAINST TERRORISM 3–4 (2010), *available at* https://www.fas.org/sgp/crs/row/RS22030.pdf.
[22] *See generally* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

recent Supreme Court warrantless cell phone seizure decisions that express the need for data protection by limiting the scope of data seizure during an arrest because of the sensitive nature of that data.[23] Ultimately, both the United States and EU have recognized a need for global interoperability if any data protection regime is to be effective.[24] That interoperability can only occur if both sides are willing to cooperate.

The common perception is that the US data privacy regime cannot adequately address the personal data privacy concerns held by EU member states, and that the pending EU privacy legislation will have a detrimental effect on US business concerns.[25] However, the divide between US security concerns and EU privacy concerns is overstated. The aforementioned shifts in policy by both parties have likely pushed the two regimes closer than ever. The goal of both is to weigh the personal privacy of their citizens against the security of those citizens and the nation and to eventually be part of a globally viable protection scheme that will allow their people to freely use technology without having their rights unjustly infringed upon.[26] A compromise needs to be made before conflict between the regimes is realized and it detrimentally affects those meant to be protected.

This compromise should involve three major aspects. First, "the right to be forgotten" should be removed from the pending legislation. This provision is likely the least workable provision within the framework of US privacy law. Much debate, even within the EU, has centered on this

---

[23] David Bender, *Supreme Court Prohibits Warrantless Cell Phone Searches Incident to Arrest*, LEXISNEXIS GROUP (July 3, 2014), http://www.lexisnexis.com/legalnewsroom/criminal/b/criminal-law-blog/archive/2014/07/22/supreme-court-prohibits-warrantless-cell-phone-searches-incident-arrest-fourth-amendment-invariant-technology-facts-legal-conclusions.aspx.

[24] *See generally* THE WHITE HOUSE, *supra* note 22.

[25] *See* BENDER, *supra* note 6.

[26] Jay Johnson, *Report on Global Data Hints Toward Global Interoperability*, LAW 360 (May 16, 2014), http://www.law360.com/articles/538570/report-on-big-data-hints-toward-global-interoperability.

provision as unfeasible within a globalized structure.[27] At its core, the provision provides a way for interested parties to erase their personal information.[28] Critics from the United States have consistently pointed to freedom of speech concerns and the burdensome nature of drudging through mountains of data to delete every mention of a particular party as reasons that the right to be forgotten cannot coexist with current US law.[29]

Second, the warrantless cell phone seizure cases should be used to drive privacy policy revision in the United States. The largest concern that non-US parties have with the US regime is that the sectoral system, paired with the PATRIOT Act, allows for sensitive personal information to be seized and accessed at will and without cause.[30] The cell phone cases are a step toward assuaging these concerns. In them, the judiciary indicated the importance of having a valid reason for accessing something as sensitive as personal data, and that government officials should not be able to do so without a show of cause.[31] Implementation of these holdings across a broader spectrum (and for non-US citizens) would do much to close the gap.

Third, since both sides have indicated a need and a willingness to cooperate with each other, they should actually do so, and they can look to Canadian action as a guide. Canada's regime is more similar to the EU system than to the US framework.[32] However, practical concerns have

---

[27] Eduardo Ustaran, *The Wider Effect of the "Right to be Forgotten" Case,* 14 PRIVACY & DATA PROTECTION 18 (2014).
[28] *Id.*
[29] *See* DAVID BENDER, INSIGHT INTO SELECTED PROVISIONS OF PROPOSED EU DATA PROTECTION REGULATION (2014), *available at* LexisNexis 7222.
[30] Alex Lakatos, *The Patriot Act and the Cloud: Part 2*, LAW 360 (Jan. 30, 2012), http://www.law360.com/articles/301726/the-patriot-act-and-the-cloud-part-2 [hereinafter Lakatos, *Part 2*].
[31] *See generally* Riley v. California, 134 U.S. 2473 (2014).
[32] *See* Paul A. Meyer, *Achieving Canada-United States Economic Competitiveness Through Regulatory Convergence—A Common Cause Agenda: Divergence and Convergence of Data Privacy Rules–Myth and Reality,* 36 CAN.-U.S. L.J. 77, 112–113 (2011).

necessitated cooperation and interaction between Canada and the United States because of close government, business, and geographic ties. Despite this cooperation, Canada has been able to maintain strong data storage and transfer relationships with EU businesses and member states as well.[33] The discourse between Canada and the United States on the subject should be used as a roadmap for cooperation between the United States and EU.

This article advocates for compromise between the United States and EU on data privacy issues by considering these three points, their impacts, and how they could catalyze the push toward global interoperability. In the first section, this paper will discuss EU privacy law with a focus on the Directive and the proposed changes to the regime. Furthermore, this paper will address how US interests have coexisted within the EU regime, and how American actors will have to adapt when the proposed legislation is enacted. The second section will focus on privacy law in the United States, how the sectoral system is different, how security concerns took the forefront post-9/11, and why the regime has been met with skepticism by the EU. In the third section, this paper will address recent developments that will impact privacy concerns. These developments include the EU's increased security concerns, more weight being placed on privacy concerns in the United States, and interaction between both regimes and Canada. The fourth section will then tie these ideas together into a proposal for compromise and a more uniform system.

II. EU PRIVACY LAW

The EU data privacy Directive currently governs data privacy among EU member states. This Directive provides that

> data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to

[33] *Id.*

> privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals.[34]

This distinction is important because it explicitly notes that the right to privacy is fundamental with regard to data processing, and this right extends to peoples of all nationalities and residences. The proposed legislation will keep this spirit of the Directive while creating more stringent protections for personal data.

A. The Directive

The Directive has an omnibus structure that allows for uniformity across sectors and provides gap-filling when new areas of privacy concerns arise. This gap-filling happens because the provisions of the Directive are applied to every aspect of data privacy.[35] For instance, if a new industry or technology arises that has data privacy implications, an understanding exists that the rules imposed by the Directive will apply to that new concern. Furthermore, the Directive follows the ideal of personal privacy as a fundamental right even in cases where security interests would supersede personal freedoms in the United States.[36]

The Directive does not allow for seizure or access of data without a cause. In fact, the controller of the data must notify the subject if her data is being processed, and the subject has the right to object

> at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.[37]

---

[34] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).
[35] *See* Suuberg, *supra* note 4.
[36] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).
[37] Council Directive 95/46, art. 14, 1995 O.J. (L 281) 42 (EC). Directive 95/46/EC of the European Parliament and of the Council § VII Art. 14.

This provision keeps businesses from using data without a legitimate reason, and prevents governments from seizing data—unless a member state can show cause and a link to national security—without having to deal with objections by the subject of that data because "such interests are overridden by the interests for fundamental rights and freedoms of the data subject."[38]

Data privacy concerns of a national security nature are left to each member state in the EU to handle on their own, with some European Council oversight. Under Article 13, "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided . . . when such a restriction constitutes a necessary measures to safeguard: (a) national security; (b) defence; (c) public security."[39] This provision is a source of contention because it gives a great deal of leeway to the member states, so long as they do not violate the spirit of the Directive.

The EU's Directive-based legislation can get bogged down in bureaucracy because the member states often have competing interests. Proposed reform in the Directive evidences this bureaucratic mire.[40] Data privacy reform was proposed in January of 2012 in the form of this new legislation (now called General Data Protection Regulation), and although the EU has decided that some form of this new legislation will be adopted, there is still wide-ranging debate—more than three years later—as to what exactly it will consist of.[41]

Helene Sjursen (an EU foreign and security policy academic) argues that since national security concerns are not addressed specifically within the provisions of the Directive, but are instead left to each state to handle, immediate action is often difficult to take even in dire situations.[42] As such,

---

[38] Council Directive 95/46, art. 7, 1995 O.J. (L 281) 40 (EC).
[39] Council Directive 95/46, art. 13, 1995 O.J. (L 281) 42 (EC).
[40] *See generally* BENDER, *supra* note 6.
[41] *See id.*
[42] *See generally* HELENE SJURSEN, A COMMON FOREIGN POLICY FOR EUROPE? 95–112 (John Petersen & Helene Sjursen eds., 1998).

enforcement has been tenuous because of the reliance on member state action within a broader regulatory scheme, thus, many of the provisions of the Directive are considered to be without teeth and not a deterrent.[43] US businesses, specifically, have enjoyed a wide array of exemptions under the Directive's provisions.[44]

B. Proposed Legislation

EU member states are pushing the new legislation forward out of a feeling of necessity.[45] This idea of necessity is prevalent despite opposing views on what provisions should be added or altered. Under the current regime, there are multiple loopholes and exemptions, many of which are used and exploited by non-member countries such as the United States, and the member states feel that it is nearly impossible to protect personal privacy without a stronger legislative framework.[46]

To strengthen the privacy framework, the proposed legislation includes harsher penalties for violations and numerous additional provisions (the most controversial being the right to be forgotten).

1. Increased Penalties

The current penalty structure of the Directive is not as deterrent as it could be because of the many exceptions that have allowed for abuses. To address this issue, EU members proposed a new penalty structure as part of the new privacy legislation.

These penalties are bound to have a huge impact on businesses based outside of non-member countries, specifically those from the United States. A single slip-up in data transfer or storage could result in enormous

[43] BENDER, *supra* note 6.
[44] Wolf, *supra* note 15, at 231.
[45] Press Release, European Commission, Progress on EU Data Protection Reform now Irreversible Following European Parliament Vote (Mar. 12, 2014), *available at* http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.
[46] *See generally* Alo, *supra* note 8.

monetary loss for those companies.[47] Data protection authorities will have stronger enforcement powers, and the penalty for breaches of data protection law could reach "€100 million or 5 percent of annual global turnover—depending on which one is the greater."[48] US companies that operate in Europe could get stuck in a no-win situation since many of the exemptions to these penalties under the current structure will be done away with. "Companies such as Google, Facebook and Apple—which have their European headquarters in Ireland—may be forced to seek clearance from data protection authorities before handing over the personal data of their users to security agencies outside Europe."[49] Every company doing business and storing data within the EU will have to follow the EU's rules, but it is foreseeable that many of these companies will also receive data requests from US authorities in the interest of national security. They may have to choose between the penalties imposed by the two regimes. Feasibility is also a concern, as both the impact of these penalties on business concerns and the lack of enforcement of previous data privacy legislation are issues to be dealt with.

2. The Right to be Forgotten

The proposed legislation would mandate that member states adopt procedures for a right to be forgotten. At its core, the right to be forgotten is a way for an individual to have his or her data expunged (or forgotten).[50] The individual would need to formally petition the local judiciary for their data to be removed, and then the court would determine if there is a reasonable basis (such as undue prejudice) for doing so. These requests

---

[47] Dan Rampe, *What's $138,050,000 or 5% of Annual Global Turnover? The Fine Companies Face if the European Parliament Passes Data Protection Measure,* THREATMETRIX (Nov. 19, 2013), http://www.threatmetrix.com/whats-138050000-or-5-of-annual-global-turnover-the-fine-companies-face-if-the-european-parliament-passes-data-protection-measure/.

[48] *Id.*

[49] *Id.*

[50] Ustaran, *supra* note 27.

would be considered on a case-by-case basis to determine whether that information holds some utility that outweighs the concerns of the petitioner.[51]

This type of power has been exercised in limited instances in some EU member states, so there is some precedent for it.[52] However, insertion into the omnibus structure that the EU privacy regime employs would make the provision pervasive, so its use has been controversial. In fact, Google Spain was at the center of one such controversy. In 2010, a Spanish national asked Google Spain to remove links to news articles that detailed the forced sale of properties owned by him.[53] Google Spain refused, so Spain's data protection authority ordered them to honor the request because Spanish law included a right to be forgotten provision.[54] Google Spain fell under Spanish authority for the matter because they could be classified as a "controller" under the EU Directive, and any controller of data within a state is subject to that state's laws.[55] The case provided for very limited circumstances in which such a request could be honored, but explicit inclusion of such a provision in the Directive would open all EU data law up to the provision.

Since the right to be forgotten has to be considered on a case-by-case basis, its adoption could result in an overload on the EU privacy regime, especially when member states that experience much more data traffic than Spain are included. From an efficiency standpoint, the right may be unfeasible as currently constructed, and the expectation is that there will be a flood of petitions seeking to exercise the right.[56] Furthermore, the expense on businesses and data collectors to remove the data could be astronomical.

---

[51] *Id.*
[52] *See, e.g.*, *id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] Craig Newman, *"A Right to be Forgotten" Will Cost Europe,* WASH. POST (May 26, 2014), http://www.washingtonpost.com/opinions/a-right-to-be-forgotten-will-cost-europe/2014/05/26/93bb0e8c-e131-11e3-9743-bb9b59cde7b9_story.html.

"While Google may have the resources to forge on in Europe, tomorrow's Google or Facebook or Tumblr may not. It isn't difficult to imagine start-ups simply forgoing a European presence, given the high cost of doing business there."[57]

Critics consider the right to be forgotten to be unrealistic given the realities of global information sharing, the prevalence of search engines and data caching, and the very real possibility that, despite all best efforts, it may not be possible to completely erase all trace of that data. For instance, after the Google Spain case, Google received "120,000 requests from individuals to remove certain links from the results of searches for their name. These have led to more than 457,000 links to articles, websites, tweets, blogs, photos and Wikipedia entries."[58] Even after removing nearly 500,000 possible hits to their searches, there is no guarantee that Google found every bit of relevant data.

US detractors, specifically, point to First Amendment concerns with regard to this right to be forgotten as it could serve to limit freedom of speech in certain instances.

> The media and the press in particular have the constitutional right to publicize information as long as it is legally available. The notion that privacy would put a limit on the right of the press to reveal the shameful past of an individual has been litigated and rejected in the Supreme Court of the United States. The notion that constitutional rights could be balanced against each other and that the freedom to speak and inform could be balanced against a

---

[57] *Id.*

[58] Juliette Garside, *Right to be Forgotten is a False Right, Spanish Editor Tells Google Panel*, THE GUARDIAN (Sept. 9, 2014), http://www.theguardian.com/technology/2014/sep/09/right-to-be-forgotten-spanish-hearing-google.

> competing constitutional right to one's private life does not seem to be an option under US constitutional law.[59]

C. US Business Interaction with the EU Regime

As discussed previously, much of the perceived problem with the current Directive has revolved around the exemptions and loopholes employed by businesses based outside the EU. US businesses, specifically, have largely been allowed to operate with fewer limitations.[60] The current exemption structure allows for a good deal of gray area for these businesses to operate in.[61] The proposed legislation is, in part, a response to this problem, and it will greatly impact US business concerns.

1. US Exemptions Under the Directive

The current penalty structure is much less restrictive than the proposed legislation would be. As currently constructed, US businesses have been able to escape deterrent punishment even when they have been found to have violated provisions of the Directive because exemptions are allowable under member state law and, for some, the penalties are just a cost of doing business in Europe.[62] The Directive states, "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions . . . either by national law or by decision of the supervisory authority."[63] Using this provision, EU members are able to make deals with outside corporations.[64] The perception is that if a company is large enough and generates enough revenue, paying a few minimal fines

---

[59] Suuberg, *supra* note 4, at 283 (quoting Franz Werro, *The Right To Inform v. The Right To Be Forgotten: A Transatlantic Clash*, *in* LIABILITY IN THE THIRD MILLENNIUM 285–86 (Aurelia C. Ciacchi et al. eds., 2009).
[60] *Id.* at 277.
[61] Council Directive 95/46, art. 3, 1995 O.J. (L 281) 31-50 (EC).
[62] Newman, *supra* note 56.
[63] Council Directive 95/46, art. 3, 1995 O.J. (L 281) 31-50 (EC).
[64] *See Id.*

in order to keep exploiting individuals is still more profitable than not committing the offenses in the first place.[65]

To add more gray area, Safe Harbor policies have increased the middle ground for US businesses.[66]

> The US response to the 1995 Directive was embodied in the International Safe Harbor Privacy Principles, a move to resolve the major trade conflict that the new rules sparked by allowing US companies to self-certify that they met an 'adequacy' requirement for E.U. privacy protection.[67]

In effect, those businesses that qualify under Safe Harbor can operate within the EU while maintaining their data centers and places of operation in the United States. Safe Harbor has been a point of contention for EU member states that wish to sequester their data within the EU and would prefer for none of that data to ever be stored within the United States for fear of seizure and/or exploitation.[68]

The Safe Harbor provisions are as follows:

> (i) notice of the purpose for collection of the information and how individuals can contact the organization and to whom it will be shared;
> (ii) a choice to opt out;
> (iii) the obligation to follow EU contracting standards in onward transfers to third parties;
> (iv) access rights so individuals may correct data;
> (v) security precautions must be adequate;
> (vi) data integrity steps should ensure that data is "reliable for its intended use [and] is accurate, complete and current"; and
> (vii) enforcement provisions that empower the organization to enforce complaints and verify compliance with other principles.[69]

---

[65] Alo, *supra* note 8, at 1132–37.
[66] Wolf, *supra* note 15, at 250–52.
[67] Suuberg, *supra* note 4, at 279.
[68] *See id.*
[69] Meyer, *supra* note 32, at 111–12.

Those arguing that big businesses have free-reign in the current system have decried the current Safe Harbor structure as an inadequate protection; they view the current system as not stringent enough.[70] These provisions are much closer to the EU standard since notice, access rights, and the option to opt out are mainstays of the EU regime. However, the Safe Harbor principles rely on the Federal Trade Commission (FTC) for enforcement, and detractors say that the incentive for the FTC to enforce them is minimal because they do not necessarily increase compliance with US law.[71] In effect, companies would be able to self-certify without the veracity of their certification being challenged.

Ultimately, many feel that the current system allows large American companies an unfair advantage. The data they carry is necessary, but they do not have to follow the same rules as most EU companies. This gives them a competitive advantage overseas, especially when their data does not have to be stored within the EU. US Companies are allowed to access the data under the more lenient US privacy regime while the data is stored in US data centers.

2. Challenges Under New Legislation

US-based business will have to adapt if the proposed legislation is enacted as is. Not only will the penalty structure be more prohibitive, but also many of the exemptions will be lost.[72] Specifically, Safe Harbor might no longer be recognized as a legitimate protection within the EU, which would force data collectors to change their data transfer and storage policies a great deal.[73] Safe Harbor was intended to bridge the gap between the two regimes to allow US companies to reach some level of EU acceptable protection, but if the situation continues as is, those companies will have to

[70] BENDER, *supra* note 6.
[71] Wolf, *supra* note 15, at 250–55.
[72] *See generally id.*
[73] *Id.*

maintain compliance with two separate protocols.[74] The exemption structure has proven lucrative for these US businesses and for the countries they operate in, and the new penalty structure may be too harsh. "John Higgins, director general of DigitalEurope, which represents companies including Apple, Microsoft, and IBM, urged member states to look critically at it. 'Rushing through a half-baked law risks throwing away a vital and much needed opportunity to stimulate economic growth.'"[75]

In 2014, the Transatlantic Trade and Investment Partnership indicated that meeting the demands of two separate regulatory structures is needlessly difficult.[76] The European Commission echoed this sentiment by saying, "Regulatory barriers have long been recognized as the most significant impediment to trade and investment between the EU and the USA."[77] Furthermore, it is not always clear which regulatory scheme to follow when they conflict.[78] Companies are going to have to figure out the most cost effective methods through trial and error.

US companies also face a dilemma with regard to the right to be forgotten, and it has been hotly debated whether that provision is even possible given freedom of speech concerns in the United States.[79] If they are ordered to comply with a petition to be forgotten, will they then have to delete the same data on their US databases? The question has been asked but not answered, and the EU has not yet finalized a concrete set of rules for this provision.[80]

---

[74] *See* Alo, *supra* note 8, at 1139.
[75] Rampe, *supra* note 47.
[76] KOMMERSKOLLEGIUM NATIONAL BOARD OF TRADE, REGULATORY CO-OPERATION AND TECHNICAL BARRIERS TO TRADE WITHIN TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP (TTIP) 2, 24–25 (2014).
[77] *EU – USA – Regulatory Cooperation*. EUROPEAN COMM'N (Jan. 3, 2013), http://ec.europa.eu/enterprise/policies/international/cooperating-governments/usa/regulatory-cooperation/index_en.htm.
[78] Alo, *supra* note 8, at 1138–39.
[79] Timberg & Halzach, *supra* note 11.
[80] *See* Paulina Whitaker & Clare Lynch, King & Spalding LLP, *The General Data Protection Regulation: Update on the Latest Developments*, LEXOLOGY (Oct. 22, 2014),

III. US PRIVACY LAW

As discussed previously, the United States differs greatly from the EU with regard to personal data protection. Part of this gap (which has widened since 9/11) exists because of the prioritization of security over personal privacy in the United States, but there are also inherent differences in the basic structure of the US regime. The sectoral structure creates both advantages and disadvantages for those seeking to protect personal privacy.

A. Sectoral System

The idea behind the sectoral system is that regulations for data protection are determined sector by sector, as opposed to relying on a uniform set of regulations across all areas, like the EU omnibus structure does.[81] This system allows for flexibility because different sectors have different privacy concerns. Similarly, the personal data concerns of some sectors are much more sensitive than those of others.[82]

Consider the medical industry, for example. In this manner, the sectoral system is able to focus protections. It "concentrates on situations where abuse will likely cause injury."[83] The Health Insurance Portability and Accountability Act (HIPAA) is a perfect example of this structure. It is a compliance scheme for personal medical data and it does not apply to other types of data.[84] Remember that under the EU scheme, the regulations are pervasive across all forms of data. The practical effect of HIPAA is that people's sensitive personal medical data is protected and can only be shared under specific and limited instances. Outside or unauthorized access to this

---

http://www.lexology.com/library/detail.aspx?g=49dc9633-e8d6-4cf9-abeb-348a6b59a464.

[81] BENDER, *supra* note 6.

[82] *Id.*

[83] *Id.*

[84] HHS.GOV, *supra* note 17.

sensitive information is only possible by following the guidelines set out by HIPAA.[85]

In the same manner that HIPAA increased the protections of certain types of data, the US system has reduced protections for other types. Among these reductions in protection are the Foreign Intelligence Surveillance Act (FISA) and National Security Letters (NSL).[86]

FISA opens the door for the United States to access the data of foreign persons and organizations, despite other protections limiting that access.[87] FISA includes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers."[88] Because of this focus on non-US information, it is often pointed to as one of the main contentions that EU member states have with the US data privacy regime.[89]

NSL works as a sort of exception to US data protection and, like FISA, allows broader access to otherwise protected information.[90] NSLs are administrative subpoenas issued by the Federal Bureau of Investigation (FBI) in authorized national security investigations "to protect against international terrorism or clandestine intelligence activities."[91] In effect, US agents are allowed to seize and access data that would be protected if it is part of an ongoing national security investigation. Detractors have argued that the FBI issues these NSLs arbitrarily without much of a showing of cause or necessity.[92]

---

[85] *Id.*
[86] Lakatos, *Part 2*, *supra* note 30.
[87] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq. (2015).
[88] *Id.*
[89] *See, e.g.*, Lakatos, *Part 2*, *supra* note 30.
[90] *National Security Letters*, ELEC. PRIVACY INFO. CTR,, https://epic.org/privacy/nsl/ (last visited Dec. 6, 2014).
[91] *Id.*
[92] Alex Lakatos, *The Patriot Act and the Cloud: Part 1*, LAW 360 (Jan. 23, 2012), http://www.law360.com/articles/301718/the-patriot-act-and-the-cloud-part-1[hereinafter Lakatos, *Part 1*].

Personal privacy advocates point to the sectoral structure as an indication that outside data, or data including non-US private information, is not prioritized as needing stringent protections.[93] Certainly, this argument is backed by the fact that the US regime protects its own citizens' private data in areas that it deems sensitive, such as healthcare, but opens the door in multiple ways for the collection and access of foreign data through mechanisms such as FISA and NSL. In practice, foreign data is actually easier to seize because it often falls within the realm of national security concerns, and the United States has explicitly noted that national security will be prioritized over personal privacy, especially when it involves foreign information.[94] This type of prioritization has only increased in the last 15 years as terrorist acts and increased national security concerns have ushered in even more lax protections of personal information.[95]

B. Post-9/11

The most common method for the US government to skirt data protection regulation is through the use of search warrants and grand jury subpoenas.[96] The Fourth Amendment of the US Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probably cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[97]

This Amendment applies to data protection as well. If the language of the Fourth Amendment is followed, data may be seized and searched. However, the government is not limited to just these mechanisms when it tries to

---

[93] *See* BENDER, *supra* note 6.
[94] *See, e.g.*, Lakatos, *Part 1, supra* note 92.
[95] *Id.*
[96] Lakatos, *Part 2, supra* note 30.
[97] U.S. CONST. amend. IV.

confiscate data, and in the wake of 9/11, their powers of search and seizure expanded greatly.[98]

The PATRIOT Act expanded the powers of both NSL and FISA. After the PATRIOT Act, foreign data was easier to legally obtain, and what was considered within the realm of a national security investigation was more broadly interpreted.[99] Surveillance, collection, and access of data were allowed under more tenuous and subjective grounds. FBI subpoenas are more easily obtained and sometimes are not even considered necessary for the access of data. Furthermore, both of these mechanisms were extended into previously unaffected areas.[100] For instance, what was considered "foreign" or having an effect on "national security" was much more loosely construed.[101] In effect, though personal data of non-US citizens was the focus before 9/11, domestic data was brought within the net afterwards.

The result of the loosening of the restrictions on data seizure is called the NSA Data Vacuum. The NSA Data Vacuum involves indiscriminate collection of data without first establishing cause or necessity.[102] In theory, the vacuum is supposed to collect vast amounts of internet and cell phone data that will remain stored but not accessed. Access to the data should only be made with good cause or a showing of necessity.[103] In practice, however, there have been wide-ranging abuses. Edward Snowden, a whistleblower, brought many of these abuses into the public limelight.[104]

Although the collection of data does not necessarily mean that the data is being accessed or abused, the reaction of those in both the United States and abroad has been resoundingly negative. This is because abuses are not only

---

[98] Lakatos, *Part 1*, *supra* note 92.
[99] *Id.*
[100] *Id.*
[101] *See, e.g.*, Lakatos, *Part 2*, *supra* note 30.
[102] *Id.*
[103] *See* U.S. CONST. amend. IV.
[104] Gellman, *supra* note 3.

possible but are also presently occurring.[105] This type of data collection also directly conflicts with the EU's prioritization of personal privacy as an inherent right not to be superseded by other interests without good cause.

The reality of the data seizure situation is that, despite the PATRIOT Act's extension of FISA and NSL powers, and despite the presence of the NSA Data Vacuum, it is still vastly more common for the US government to seize data through traditionally legitimate means, such as a warrant or subpoena.[106] This fact not only means that access without cause is rare but also that the United States could possibly abandon arbitrary access methods with limited detrimental impact. Warrant and subpoena are the same means that are largely accepted throughout the EU regime as well. Furthermore, many of the EU member states have provisions in place to provide for the seizure of data in cases involving national security, though their methods may be less arbitrary.[107]

To address many of the perceived gaps in US data protection, US-based businesses and government agencies have increasingly relied more on privatized personal privacy protection.[108] Data privacy professionals have been used to consult and protect the personal data of US citizens in new and innovative ways. These professionals are able to tailor the protections to specific industries, and this move toward privatized data protection has arguably resulted in more actual personal privacy protection in the US than in the EU, where the EU member states are almost completely reliant on a slow-changing bureaucratic approach.[109] While these professionals have largely been engaged in the business sector, their expertise could also translate into increased personal protections as new innovations become more widely available.

---

[105] *Id.*
[106] Lakatos, *Part 2*, *supra* note 30.
[107] *Id.*
[108] *See generally* Meyer, *supra* note 32.
[109] BENDER, *supra* note 6.

C. EU Skepticism

Critics of the US privacy protection regime have consistently pointed to US protections of personal data as being "inadequate" because of the perception that data may be arbitrarily seized and accessed and that certain types of data do not receive the same protections as data that the US government has deemed "sensitive."[110] To some degree, these detractors have a strong foundation for their skepticism. It is true that foreign data, specifically, has received less protection, has been collected, and has been accessed in the past.

The strongest proponents of stringent data regulation in the EU have pushed to sequester all EU business and personal data onto EU servers.[111] They would like to effectively block data sharing with the US government and US-based corporations. This, they believe, would limit the exposure of their data to abuses by both government and corporate bodies that face less stringent regulations within the United States.[112] Doing so would require putting an end to the Safe Harbor provisions and other exceptions.

Data privacy professionals have argued, however, that it is virtually impossible to maintain complete separation.[113] Considering the realities of the internet and the information age, sequestering all of the data may not be feasible, and even if it could be done, there could be a huge detrimental impact on those under the protection of both regimes.[114]

As discussed above, the EU has many of the same cause and necessity-based mechanisms for skirting Directive provisions as the United States to facilitate personal data seizure. What EU members are mostly worried about, however, is that data seizures will occur arbitrarily or that their data will be abused in the name of profit.

---

[110] *Id.*
[111] *See generally* Meyer, *supra* note 32.
[112] *Id.*
[113] *See, e.g.*, Alo, *supra* note 8.
[114] *See, e.g.*, Meyer, *supra* note 32.

IV. RECENT DEVELOPMENTS

Despite the rift between the two regimes, recent developments in both the United States and EU have signaled the possibility of compromise. Practical security concerns among EU member states, an increased focus on privacy concerns in US policy, and the relative ease with which the United States has developed a mutually beneficial data-sharing agreement with Canada are among the promising signs.

A. Increased Security Concerns Among EU Members

Although the Directive leaves EU member states to fend for themselves when it comes to national security concerns, those states still must maintain overall compliance with the Directive. The result has been that data is less easy to access, regardless of its importance to maintaining security. Recent attacks have necessitated a reliance on outside sources of data collection, namely, those employed by US intelligence agencies.

1. Terrorism and National Security

Bombings and terrorist attacks in EU member states have led to an increased emphasis on security.[115] Recent attacks, such as those in Madrid,[116] have forced a change in policy among the affected nations. "The March 2004 terrorist bombings in Madrid injected a greater sense of urgency into EU counterterrorism efforts, and gave added impetus to EU initiatives aimed at improving travel document security and impeding terrorist travel . . . [e]nhancing intelligence-sharing."[117] Other incidents solidified this stance, and there has been a strong push toward allowing for access and seizure of data in the interest of security. For instance, the 2005

[115] ARCHICK, *supra* note 21, at 2.
[116] *Madrid Train Attacks*, BBC NEWS, http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/ (last visited June 30, 2015).
[117] ARCHICK, *supra* note 21, at 2.

subway bombings in London "prompted additional efforts to improve police, judicial, and intelligence cooperation."[118]

The EU regime currently allows for data access but requires a showing of cause. Because of this, valid access is determined on a case-by-case basis, as opposed to allowing for blanket data collection by certain agencies.[119] In effect, the US system allows for a "collect first, ask permission later" mentality, and while personal privacy is diminished, security is enhanced. The EU's model tends to take longer, and often the process is too slow to allow for an adequate reaction to security concerns. It is "a traditionally slow-moving body because of its intergovernmental nature and largely consensus-based decision-making processes."[120]

2. Reliance on US Intelligence Services

EU member states have actually benefited greatly from "catches" provided by the US Data Collection Vacuum. This is despite the fact that the Data Collection Vacuum, and especially the methods employed by the NSA, has been used as an indicator that the US security regime cannot exist in conjunction with the Directive or future EU legislation.[121] These "catches" are potential threats flagged within the US data collection net, and the United States has been fairly open about sharing information on serious threats with its allies within the EU.[122]

When one of these catches is made, the EU state can work to counter the threat without having to sacrifice its own integrity on personal privacy grounds. Prominent members of the global community have noted this hypocrisy.[123] In his article on the actual levels of privacy provided by the two regimes, David Bender writes:

---

[118] *Id.*
[119] Council Directive 95/46, 1995 O.J. (L 281) 23 (EC).
[120] ARCHICK, *supra* note 21, at 2.
[121] Alo, *supra* note 8, at 1103.
[122] BENDER, *supra* note 6.
[123] *Id.*

> One can almost see the intelligence chief in each of those nations respectfully tapping the head of state on the shoulder and whispering: 'Um, you know, we've gotten some helpful information from that US surveillance. Oh, and by the way, we do some of that stuff, too.'[124]

Some European countries, such as France and England, have even increased their reliance on the US security network, and it is not unheard of for this heavy reliance to result in countries waiting for US agencies to flag potential threats as part of an early warning system.[125] In "Missed Opportunity or Eternal Fantasy?: The Idea of a European Security and Defence Policy," Helen Sjursen notes the importance of "European dependence on US intelligence."[126] She also points out that European nations are often reliant on US intelligence to take military and defensive action.[127]

Furthermore, European nations have eagerly invited law enforcement and intelligence cooperation agreements. Bilateral Mutual Legal Assistance Treaties (MLAT) are common between US and European governments and are not superseded by the Directive or other EU privacy legislation.[128] As discussed previously, the Directive leaves security matters to the individual states to handle, so their agreements with the United States are used to improve their own security.

On top of the MLATs between the United States and specific countries, the EU itself has an MLAT with the United States that says "[g]eneric restrictions . . . for processing personal data may not be imposed . . . as a condition . . . to providing evidence or information."[129] These types of agreements indicate that perhaps the EU is not that far removed from the

---

[124] *Id.*
[125] *See generally* SJURSEN, *supra* note 42.
[126] *Id.* at 103.
[127] *Id.* at 103.
[128] *See* Lakatos, *Part 2*, *supra* note 30.
[129] *Id.*

US's protection-over-privacy methodology. However, personal privacy can still be adequately protected if the two regimes can work together on developing a comprehensive framework.

B. Emphasis on Privacy Concerns in the US

In addition to the increased focus on security among EU member states, the United States has shown a marked uptick in weight given to privacy concerns. Some of this shift is the result of policies driven by business and consumer concerns, but others have arisen through the judiciary.

1. Business and Consumer Policy

The White House recently issued a report on "Big Data" that addressed many of the issues at hand with regard to the dichotomy between corporate concerns, innovation, and technology and personal privacy concerns.[130]

The report recognizes that big data can improve the economy and save lives; it also notes that big data practices present certain privacy-related challenges, increase the risk and scope of data security breaches, and weaken consumer protection.[131] The report concludes by recommending six safeguards that the administration believes are necessary for big data analytics to truly benefit society[132]

The six safeguards are as follows: (1) advance the Consumer Privacy Bill of Rights; (2) pass national data breach legislation; (3) extend privacy protections to non-US persons; (4) ensure data collected on students in school is used for educational purposes; (5) expand technical expertise to stop discrimination; and (6) amend the Electronic Communications Privacy Act.[133]

---

[130] Johnson, *supra* note 26.
[131] *Id.*
[132] *Id.*
[133] *Id.*

Although both the US and EU standards were derived from the same Fair Information Practice Principles developed in the 1970s, they have diverged greatly since then. This Big Data report acknowledges that some global criticism of the privacy policy in the United States is fair, and it expresses an intention for the United States to move closer to international norms in an effort to legitimize global data privacy interoperability.[134]

Aside from the report itself, there are other indications that US interests are gravitating toward the mean with the help of business-generated criteria. One such indicator is the Consumer Privacy Bill of Rights, which is a "framework for protecting privacy and promoting innovation in the global digital economy."[135] There has been recognition that global cooperation is necessary to preserve advancement of technology and to protect the rights of individuals.[136]

There has also been an expansion in recent years of protections for non-US citizens, notably, from those countries with which the United States has the strongest economic ties.[137] These increased protections came about in response to calls for more stringent regulation when US corporations transfer data.[138]

Ultimately, it seems that both regimes have indicated that they agree on at least one fundamental point—the need for a global system so that protections are maintained across borders.

2. Judicial Decisions

Freedom from illegal search and seizure is an important right for US citizens to protect themselves from government entities.[139] Unfortunately, there has been confusion as to how this right pertains to personal data.

---

[134] *Id.*
[135] THE WHITE HOUSE, *supra* note 22.
[136] *See generally id.*
[137] *See* Meyer, *supra* note 32.
[138] *See id*.
[139] U.S. CONST. amend. IV.

Some clarity on the issue was recently provided in an opinion delivered by Justice Roberts. *Riley v. California* had to do with seizure of cell phones, and the data contained therein, during an arrest.[140] While it may seem like this issue is dissimilar from the seizure of data through the internet because of the involvement of arrests and the non-involvement of national security interests, the language pertaining to data in particular is useful. Additionally, data on cell phones is often not stored on the devices themselves. Increasingly, the data is stored by the cell company through cloud computing, so seizure of this kind of information is more complex than it would seem and more similar to mass data seizure as well.[141]

In the decision, Chief Justice Roberts says that the issue to consider with seizures is "balancing the degree to which it intrudes upon an individual's privacy against the degree to which it is needed to promote legitimate government interests."[142] He goes on to say that cell phones place vast quantities of personal information in the hands of individuals.[143] The confiscation of the data stored in a cell phone could result in a massive intrusion on an individual's privacy. Furthermore, the decision recognizes that certain types of data are qualitatively different. Internet browsing history, photos, emails, and the like could represent a significant and sensitive part of peoples' lives.[144]

Roberts points out that for a seizure of this type of sensitive information, authorities should have "clear" and "workable" limitations when accessing data.[145] Requiring a warrant, or at least exigent circumstances, would satisfy the court that there was cause and a legitimate government interest in the invasion of personal privacy.[146] The decision reflects an increasing trend (as

---

[140] Bender, *supra* note 23.
[141] *Id.*
[142] *See Riley*, 134 U.S. at 2484.
[143] *Id.* at 2485.
[144] *See id.* at 2489.
[145] *Id.* at 2491.
[146] *See id.*

seen in both this case and in the White House data report) toward the protection of personal privacy and weighing that privacy more than the principles of efficiency or security.

If this were to be the case for all seizures of data, the treatment would be similar to that in the EU privacy regime. In the EU, personal privacy is considered inviolable unless there is good cause, and the need for proof of cause or exigent circumstance to seize or access data in the United States has been called for by the international community.

C. Canadian Cooperation

The ability of the US and Canadian governments to come to a workable compromise with regard to data privacy is proof that compromise is possible between the United States and EU as well. Canada employs a data privacy structure much more similar to that in the EU than to that in the United States.[147]

One of the pillars of Canadian privacy law is the Personal Information Protection and Electronic Documents Act (PIPEDA).[148] PIPEDA is similar in many ways to the Safe Harbor principles, but with some notable additions.[149] They are as follows:

> 1) consent to collect and use the information must be express or implied;
> 2) all organizations subject to PIPEDA must designate a privacy officer;
> 3) written policies must be available for review;
> 4) written data retention guidelines must be implemented on the preservation and destruction of data; and

[147] *See* Meyer, *supra* note 32.
[148] *Id.* at 112.
[149] *See generally id.*

> 5) cross-border transfers are not prohibited or restricted; however, the organization remains responsible for data wherever it is located.[150]

In effect, these regulations are functionally similar to those used for Safe Harbor, but they also provide increased protections more similar to those called for by the EU privacy community.[151] Ultimately, the Canadian system is much more closely related to the EU regime than to that in the United States.

However, Canada and the United States have found common ground. Both have started to accept and promote the existence of security professionals and security officers as the normal operating procedure.[152] Confidentiality obligations in common commercial practice are enforceable in both countries because of legal cooperation between them.[153] Both also have strict limitations on the use of certain types of data (like health information).[154] Although much has been made, even in Canada, of the US data vacuum, PIPEDA Section 7 allows the Canadian government to collect data about Canadian citizens with a subpoena.[155] Canada often supplies that data to US intelligence agencies for national security and legal purposes. In effect, much of the information that would be subjected to the data vacuum is supplied to the United States by the Canadian government anyway.[156]

Despite being more similar to the EU privacy regime and, more importantly, despite a preference for the EU policies and regulations, Canada has been able to work amicably with the United States to develop strong data storage and sharing interactions.[157] Much of this cooperation happened because of practicality. It would be virtually impossible for

---

[150] *Id. at 113.*
[151] *See generally id*.
[152] *See id.*
[153] *Id.* at 114.
[154] *See generally id.*
[155] *Id.* at 118.
[156] *Id.* at 108.
[157] *See id.*

Canadian government agencies and corporations to completely sequester their data outside the United States.[158] Canadians do, however, sometimes experience problems when dealing with privacy restrictions that differ from sector to sector and from state to state. However, these issues have been largely addressed through the use of third-party data privacy professionals, whose job is to keep the differing regulations straight for their clients.[159]

There are numerous detractors among Canadian privacy professionals who harbor fears of "inadequacy" in the US privacy protection system. Others, however, argue that these fears of abuse of non-US citizen data are largely overstated.[160] They point to the realities of the successful interactions between the two countries thus far as proof that the differences in policy and legislation are not as profound as many believe.[161]

V. PROPOSALS FOR COMPROMISE NEEDED FOR GLOBAL INTEROPERABILITY

Global interoperability is the ultimate goal for those interested in providing the best protections possible of both the right to privacy and the need for security. According to the European Council, there are multiple organizations working toward this goal, but no concrete resolution has been reached.[162] If the rift between the regimes were to increase, there would be an untenable situation in which efficiency would dwindle and actual protections would decrease.

A. Abandonment of Unworkable Provisions

In the interest of furthering global cooperation and increased privacy security around the world, the EU should abandon the most controversial and least workable provisions of their proposed legislation. Not only have

---

158 *See generally id.*
159 *See id.*
160 *See id.*
161 *See id.*
162 EUROPEAN COMM'N, *supra* note 77.

these provisions held up the legislation, which many deem as necessary to the protection of individual freedoms, but even EU member states cannot agree on their validity. They will only serve to widen the rift between the EU regime and the US system.

Although the United States has objections to many of the provisions of the proposed legislation, and those objections have sometimes fallen on deaf ears, EU member states have largely found those same provisions to be the least palatable.[163] The proposed legislation became necessary because the EU wanted more deterrent legislation, and unenforceable provisions of the Directive impeded that goal.[164] If the legislation passed as is, there would be multiple provisions that would be unworkable globally, which would again leave the protection regime with a reputation for being ineffective.

Some believe the limits on US exemptions to be knee-jerk reactions to recent revelations about NSA data collection and possible abuses by the US government, while others express a feeling that large US-based corporations have taken advantage of Directive loopholes.[165] Either way, instituting policies designed just to get back at the US entities will not further the goal of global interoperability, and it will ultimately only limit the protections of citizens both within and outside of the EU.[166]

The right to be forgotten is an especially dubious proposition. It would be nearly impossible to force companies across the globe to erase specific data across all platforms and from all databases. The United States faces a particularly difficult problem regarding this provision. It is fundamentally opposed to one of the foundational tenets of the United States to force censorship of speech because an individual did not want that speech to be

---

[163] BENDER, *supra* note 29.
[164] BENDER, *supra* note 6.
[165] Lakatos, *Part 2*, *supra* note 30.
[166] *Id.*

heard. To mandate the removal of information from the web could catalyze serious controversy in the United States.

The right to be forgotten could also involve a dangerous hindrance to the right to information. Craig Newman, in his article "'A Right to be Forgotten' Will Cost Europe," asks, "Should links to a doctor's negative reviews be removed? The past behavior of a politician making a comeback bid? The conviction of a man who possessed images of child abuse?"[167]

Newman goes on to explain that the financial burden imposed on US businesses under the proposed legislation would cause them to avoid establishing operational bases in Europe.[168] If this provision were to be passed, no US company with an operational base in Europe would be completely free from the possibility of EU penalties.[169] If this were to happen, these European states would also lose out on any financial benefit that the companies bring to the table.[170] Abandoning the provision would not only result in quicker passage of the new legislation and greater global acceptance, but it would also prove mutually beneficial to both businesses and governments in the EU.

Best of all, this compromise is feasible and would still enable proponents of the right to be forgotten to enact it within their own states.[171] For any of those member states that feel that this provision is integral to furthering personal privacy protections, the EU's structure allows them to implement said provision locally. Instead of imposing an overarching rule that could dampen both the foreign and domestic economic climates of European countries, each state should be able to weigh the advantages and

---

[167] Newman, *supra* note 56.
[168] *Id.*
[169] *Id.*
[170] Craig Timberg, *In Google Case, E.U. Court Says People are Entitled to Control Their Own Online Histories,* WASH. POST (May 13, 2014), http://www.washingtonpost.com/business/technology/eu-court-people-entitled-to-control-own-online-histories/2014/05/13/8e4495d6-dabf-11e3-8009-71de85b9c527_story.html.
[171] Ustaran, *supra* note 27.

disadvantages on their own to decide whether to implement. In a situation like Spain's, where the country believes the right to be forgotten is beneficial, they would still be free enact that legislation on their own (as evidenced by the Google Spain case).[172]

B. Using Cell Phone Decisions as a Framework

While search and seizure of personal property during an arrest differs from personal privacy concerns during data collection and storage, both situations involve the collection of private information and, in some ways, electronic property is even more personal. The language of the recent warrantless cell phone decision reflects a marked increase in concern for privacy over security in the United States. The decision comments on both the qualitative and quantitative differences between data and other forms of property, and the qualitative portions especially should be considered in reforming national privacy policy.[173]

If it is illegal for police to access data stored on a cell phone during the course of an arrest, how then can it be legal to access and seize huge amounts of personal data indiscriminately? The main qualm the EU has with US data collection is that it can be accessed and used without a show of cause or exigent circumstance.[174] The cell phone case, coupled with the White House's "Big Data Report," indicates a growing trend toward these types of invasions of personal information as highly objectionable activities. These trends should be expanded upon to help assuage some of the fears of non-US entities.

Cell phones can be seized at the time of arrest, but the data cannot be accessed without a show of cause or that the safety of officers or others is at risk.[175] This could be extrapolated to governmental data collection to give

---

[172] *Id.*
[173] *See generally Riley*, 134 U.S. at 2473.
[174] *See* Suuberg, *supra* note 4
[175] *See Riley*, 134 U.S. at 2473.

individual privacy adequate weight. By using this reasoning, the government could still collect data using their broad nets, but they would not be able to access or use the data unless they have a valid reason for doing so. Security should not supersede a right to privacy unless there is legitimate danger. The presence of these more stringent controls on data access would cause the US regime to conform more closely to international norms and would go a long way in shortening the rift with the EU.

It could be argued that it is not the role of the judiciary to set policy, and that the language used in the cell phone decisions is not relevant to interaction with foreign nations. This is true in terms of the president being responsible for foreign policy concerns under the political question doctrine.[176] However, the judiciary does have the power to weigh in on the constitutionality of domestic concerns, of which the current US privacy regime is one. Furthermore, judicial language is often used in informing the legislature when promulgating laws designed to protect the rights of its constituents. When this decision is paired with the Executive Branch's willingness to find a workable solution, it is clear that US legislation must begin to revert to the international mean.

C. Modeling US/EU Discourse After US/Canada Data Sharing

Much like the judicial decisions can be used as a more pervasive framework for data privacy concerns, the interplay between the United States and Canada with regard to data security should be looked to as an example for the relationship between the United States and the EU. Although Canada more closely follows the EU model of data protection than the US model, it has managed to find common ground with its southerly neighbor; finding common ground should be possible between the larger US and EU regimes.

[176] United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936).

A huge catalyst for this success has been the reliance on data privacy professionals. These unbiased third parties have laid the groundwork for successful data interaction by both businesses and governments.[177] Third-party consultants have proven more apt at discovering the middle ground and providing stronger protections. This largely has to do with their flexibility in not being bound by bureaucracy, and they have the freedom to explore new technology and innovation.[178] It is also in their best interest to do so as they stand to gain monetarily by providing cutting-edge protection. Leaks in data hurt their bottom line, and corporations already rely on these professionals to keep information safe. Allowing the standard practices of the private data security industry to guide the policies of the data protection regimes would fulfill the goals of both the United States and EU. The United States would be able to continue to maintain its sectoral system flexibility by allowing the sectors themselves to determine the best practices, and the EU would be able to point to increased protections as furthering their privacy interests.

Another large realization helped the United States and Canada come to a reasonable resolution. It would have been economically impractical to try to sequester all sensitive data within one country or organization. Using this realization as a starting point made cooperation a necessity. The Canadian and US governments officially recognized the importance of the free flow of information between the two countries in their Statement of the Free Flow of Information and Trade in North America.[179] "The governments jointly noted that 'Cross-border data flows are an important underpinning of

---

[177] *See* Meyer, *supra* note 32.
[178] *See id.*
[179] KRIS KLINE, APPLYING CANADIAN PRIVACY LAW TO TRANSBORDER FLOWS OF PERSONAL INFORMATION FROM CANADA TO THE UNITED STATES: A CLARIFICATION (2008), *available at* https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf/$file/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf.

all international trade transactions. . . .'"[180] The same should apply to the ongoing debate between the United States and EU. It is unfeasible to say that US-based business and government entities will have no access to personal European data. Furthermore, it is unenforceable.[181] Global transfer and storage of data is more the norm than an outlier, and the only way to provide comprehensive protection is through global interoperability.[182]

Such arguments have facilitated cooperation between the United States and EU in the past. The 2014 report from the Transatlantic Trade and Investment Partnership commented on the state of cross-border regulatory harmonization in investment legislation.[183] They noted that because of the joint recognition of economic priorities,

> what was initially presented as impossible, such as the compatibility of regulatory agencies and structures for standardization in the EU and the U.S., does not appear quite so difficult; that is, if the EU and the U.S. can agree on joint processes when developing more compatible and coherent regulations in various areas.[184]

This sort of joint recognition of priorities prompted the dialogue and cooperation between the United States and Canada. The United States and EU should feel comfortable collaborating in the same way on data privacy issues.

Much like the fears of arbitrary data seizure by the United States have proved to be overstated in Canada because of similar Canadian legislation, and the cooperative data sharing that already takes place, the EU should find that their concerns are overstated as well. Anti-terrorism and law enforcement data sharing already takes place between the United States and the EU and between the United States and individual member states of the

---

[180] *Id.* at 12.
[181] *Id.*
[182] *See generally* THE WHITE HOUSE, *supra* note 22.
[183] KOMMERSKOLLEGIUM NATIONAL BOARD OF TRADE, *supra* note 76, at 6.
[184] *Id.*

EU. These agreements should be highlighted to limit the negative perception of PATRIOT Act data collection and should be built upon to strengthen the connections. The Canadian government published a clarification on the actual state of data-sharing cooperation between the countries in which it debunks some of the misconceptions, and the EU could do the same.[185]

EU member states and the United States should build upon their MLATs and come to data-sharing agreements similar to the one between Canada and the United States. Doing so would provide those member states better protection from arbitrary data seizure by the United States, but would also allow the United States access to that data that most closely involves national security.

The social concerns are numerous in deciding how to proceed, but as with Canada, the EU should allow their business and economic concerns to foster opportunity, innovation, and contractual safeguards. In turn, the reliance on the use of better technology by third-party professionals should lead to increased personal information protection while not limiting citizen safety. In this manner, a viable solution is possible.

VI. CONCLUSION

The point of the data privacy reform taking place in the EU is to take the Directive a step further and to provide the best possible protection of personal privacy to EU citizens. This can be accomplished without widening the gap between the EU's regime and that of the United States. Much has been made about the differences between the two regimes, but there are clear-cut indicators that the two can workably interact.

Global interoperability and a more uniform system of protection across nations is the only way to ensure that protections are maintained, and those protections do not have to fundamentally hinder national security,

[185] *See generally* KLINE, *supra* note 179.

innovation, or business interests. Both the EU and US authorities have expressed the desire to strive for this sort of interoperability, but they have yet to take steps toward implementing it. Compromise would be mutually beneficial, and it could be achieved by following recent trends. The EU needs to acknowledge its security concerns, and needs to abandon provisions of its legislation that inhibit passage and cooperation. Similarly, the United States needs to acknowledge the weight and sensitivity of personal privacy concerns, as noted by the Supreme Court, and must extrapolate that weight into increased protections. Finally, both regimes should look toward the cooperative nature of the Canadian regime as a roadmap for further discussion.

This article is by no means meant to cover a complete list of data privacy concerns across the two relevant regimes, nor is it meant to imply that the three compromises proposed are the only avenue for interoperability. However, for citizens of both the United States and the EU to be actually and justly protected by these protection regulations, and for individual rights to be honored in the face of growing security concerns, there must be at least a modicum of cooperation and uniformity. Otherwise, personal privacy will continue to slip through the gaps between the two systems.