Global Information Assurance Certification Paper

No Safe Harbor: Collecting and Storing European Personal Information in the U.S.

GIAC (GLEG) Gold Certification

Author: Alyssa Robinson, lyssanr@yahoo.com
Advisor: Benjamin Wright
Accepted: April 24, 2017

Abstract

When the European Court of Justice nullified the Safe Harbor Framework in October of 2015, it left more than 4,000 companies in legal limbo regarding their transfer of personal data for millions of European customers (Nakashima, 2015). The acceptance of the Privacy Shield Framework in July of 2016 expands the options for U.S. companies that need to transfer EU personal data to the US but does little to ameliorate the upheaval caused by the Safe Harbor annulment. This paper covers the history of data privacy negotiations between the Europe and the United States, providing an understanding of how the current compromises were reached and what threats they may face. It outlines the available mechanisms for data transfer, including Binding Corporate Rules, Standard Contractual Clauses, and the Privacy Shield Framework and compares their requirements, advantages, and risks. With this information, US organizations considering storing or processing European personal data can choose the transfer mechanism best suited to their situation.

1. Introduction

Under the 1995 Data Privacy Directive enacted in the European Union, transfer of personal data regarding EU residents is only allowed to a designated set of countries that provide an "adequate" level of personal data protection. These countries include Canada, Switzerland, New Zealand, and Israel, but not the United States (Association of Corporate Council, 2016). Standard Contractual Clauses and Binding Corporate Rules are established mechanisms for legal personal data transfer between EU companies and businesses in countries without adequate protection of personal data that sign onto these provisions (Association of Corporate Council, 2016). The Safe Harbor Framework provided an additional legal path for personal data transfer to the US from 2000 through 2015, when it was struck down by the European Court of Justice. In 2016, the Privacy Shield program filled the hole left by Safe Harbor, providing US companies with the ability to once again self-certify that they provide adequate privacy protections (Chung, 2016).

Currently Privacy Shield, direct Data Protection Authority contract approval, Standard Contractual Clauses, and Binding Corporate Rules are all possible legal mechanisms for European companies looking to transfer personal data to the US. Multiple legal challenges to the current data transfer mechanisms in Europe and changing political priorities in the United States have further muddied the waters. The challenges facing each mechanism add complications for organizations attempting to choose the right path for doing business with European consumers and has led some companies to pursue options for keeping European personal data in Europe (Scott, 2016). Without a mechanism for legal transfer of personal data to the US, US companies providing software and services would be unable process the financial and contract data of customers or business partners (ITIC, 2016) or provide many consumer services. Each available mechanism has its own set of benefits, drawbacks, and legal risks and should be considered in the full context of the business and its privacy program, as well as the current political climate.

Alyssa Robinson, lyssanr@yahoo.com

2. History of Safe Harbor

2.1. Privacy in the EU

A fundamental difference exists between the way privacy is viewed in the United States and in Europe. In the European Union, privacy is considered an intrinsic human right (Schriver, 2002), while the US still lacks a comprehensive approach to privacy, relying instead on a mishmash of state laws and regulations governing specific industries (Martin, 2016). Growing concerns over collection and use of personal data drove the creation of the European Data Protection Directive in 1995 (Schriver, 2002). At that time, differing privacy protections across the states of the European Union caused issues with cross-border transfers of data within the Union (Yuwono, 2016). The Data Protection Directive allows for free flow of data among member states, which are required to maintain laws consistent with the Directive's principles while preventing transfer to countries without strong privacy protections in place (Schriver, 2002).

The EU Data Protection Directive defines personal data as any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Sensitive Data, according to Article 8 of the Directive, is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, offenses, or criminal convictions; this data is protected and cannot be collected without explicit consent (European Commission, 2016). Under the Directive, personal data collection must be limited to what is required for "specific, explicit, and legitimate" purposes, must be accurate and can be kept only as required for those specific limited purposes (Schriver, 2002).

Between 1995 and 2016, privacy laws across Europe became fragmented once again, as principles from the Data Protection Directive were incorporated into national legislation (Yuwono, 2016). In January of 2012, the European Commission proposed a

reform of the 1995 Privacy Directive. These changes were aimed at strengthening protections and once again aligning privacy laws across the European Union, reducing the administrative burden on companies doing business in the EU (European Commission, 2016). After four years of discussion, the General Data Protection Regulation (GDPR) took four years of discussion before it was adopted in 2016 (Allen Overy, 2016) and will replace the 1995 Data Protection Directive on May 25, 2018, (European Commission, 2016). The General Data Protection Regulation is directly applicable in all member states, which are not required to pass their own national laws as was the case under the Data Protection Directive (Allen Overy, 2016).

2.2. Creation of Safe Harbor Framework

The Safe Harbor agreement was negotiated by the Clinton administration (which feared the loss of trade between Europe and the United States) following the passage of the Data Privacy Directive in Europe (Schriver, 2002). While the slow creation of national privacy regulations within Europe reduced pressure on the US to reach a deal, a unique agreement was eventually reached. The Safe Harbor framework enforced privacy principles similar to those required by EU law for US companies that self-certified compliance, deeming them adequate for personal data transfer (Coudert, 2015).

The Data Protection Directive gained particular relevance with the rise of the Internet, leading to increased data collection and transfer to third parties, sometimes without any notice to the subject (Schriver, 2002). Despite concerns from the European Parliament and privacy advocates that Safe Harbor "lacked teeth", EU member states deemed Safe Harbor adequate for personal data transfer in July 2000 (Wilhelm, 2016). In its negotiations, the Clinton Administration tried to balance EU privacy requirements and American business concerns about increased bureaucracy, allowing American businesses to avoid negotiating with Data Protection Authorities in each member state by means of signing on to the Safe Harbor framework. Despite this, Safe Harbor was slow to pick up momentum in the US. Many companies were watching and waiting to see what would happen, and only 168 firms had registered by 2002 (Schriver, 2002). US companies complained early on about Safe Harbor compliance being "costly, unworkable, and unfair" (Future of Privacy Foundation, 2013).

In 2001, the European Commission began to take action against Ireland, France, Germany, Luxembourg, and Netherlands in the European Court of Justice for failure to implement the Data Protection Directive (European Commission, 2003). These actions demonstrated that the EU was getting serious about enforcing the new regulations. Safe Harbor came to be used by companies employing Europeans as well as those doing business with European customers (ITIC, 2016) and eventually became the most common legally-approved method for personal data transfer from the EU to the US (Association of Corporate Council, 2016).

2.3. Safe Harbor Requirements

The US Department of Commerce's International Trade Administration, working in conjunction with the European Commission, developed Safe Harbor as a compromise solution with the goal of allowing the flow of data between the US and the EU while still protecting personal data (Future of Privacy Foundation, 2013). The Consulting firm Galexia described Safe Harbor in a 2008 report as an "uneasy compromise between the legislative approach adopted by European nations and the self-regulatory approach preferred by the US" (Connolly, 2008). Safe Harbor outlines seven principles which align closely with those of the Data Protection Directive:

- **Notice** about the personal data being collected and the purposes for which it will be used.
- **Choice** regarding whether the data can be used for other purposes or disclosed to additional third parties. Opt-in is required for sensitive data.
- **Onward Transfer** of data to third parties must abide by the notice and choice principles.
- **Access** to the personal data held about a particular EU citizen must be provided if requested.
- **Security** of the personal data must be ensured with "reasonable precautions."
- **Data Integrity** requires personal data held must be accurate, complete, current, and relevant to the purposes for which it will be used.
- **Enforcement** procedures for dispute resolution via an independent third party must be available to consumers (International Trade Association, 2013).

Entering into Safe Harbor was a voluntary decision on the part of US companies, which needed to be under the jurisdiction of either the Federal Trade Commission or the

Department of Transportation to enroll (Department of Commerce, 2009). By self-certifying yearly that they complied with Safe Harbor requirements, they provided assurance to EU organizations and consumers that there would be adequate protection of personal data (Department of Commerce, 2009). Self-certifying organizations needed to state in their privacy policy that they adhered to the Safe Harbor Framework, must have a point of contact designated for handling questions and complaints, and must have procedures in place for verifying compliance with the Framework (Department of Commerce, 2009). Safe Harbor enforcement was mainly accomplished by required private sector dispute resolution mechanisms, backed up by FTC fines and enforcement measures. Self-certifying organizations could name an independent third party such as TRUSTe or the Better Business Bureau for dispute resolution or rely on Data Protection Authorities in the EU (JAMS, 2017). The reputational risk for member companies that failed to comply also helped to ensure compliance (Future of Privacy Foundation, 2013).

The Department of Commerce's International Trade Association reviewed every application and re-application for Safe Harbor to confirm that the guidelines were met: in 2013, 56% of first-time certifiers required changes or further clarification (Future of Privacy Foundation, 2013). While complaints from EU member state Data Protection Authorities were imagined be a primary enforcement mechanism at Safe Harbor inception, only a handful of complaints were ever filed this way. The FTC brought its first enforcement action under Safe Harbor in 2009, against a retailer that made false claims about Safe Harbor membership. This first FTC complaint was settled with a $500,000 fine (Future of Privacy Foundation, 2013). Six additional companies faced enforcement action for similar deception, while Google, Facebook, and MySpace, among others, faced FTC suits for violations of the Safe Harbor principles (Future of Privacy Foundation, 2013). In all, the FTC brought charges against 40 companies for Safe Harbor violations during the time it was in effect (Weiss & Archick, 2016).

2.4. Nullification of Safe Harbor

Leaks from former National Security Agency contractor Edward Snowden in 2013 revealed Agency access to the private data of Europeans via cooperation from Google,

Facebook, Apple and other US companies (Future of Privacy Foundation, 2013). Following Snowden's disclosure of widespread US government surveillance, European Union Commission Vice President Viviane Reding stated that repairs would be needed to the Safe Harbor program or it would be suspended (Wilhelm, 2016). The European Commission released a report in November of 2013 critical of Safe Harbor, citing shortcomings in the form of deficient enforcement, lack of transparency in privacy policies, and ineffective application of privacy principles (Future of Privacy Foundation, 2013). Reding called for the review of Safe Harbor and improvements were suggested by the European Commission, however talks with the US stalled due to disagreements about data sharing with US law enforcement (Coudert, 2015).

That same year, Austrian privacy advocate Max Schrems filed a complaint with the Irish Data Protection Authority challenging Facebook's transfer of his personal data from Ireland to the US. His complaint alleged that the United States offered no protection against government surveillance for data transferred there (EPIC, 2017). The Irish Data Protection Commissioner originally rejected Schrems's claims, as the EU Commission had already ruled that protections under Safe Harbor were adequate, but the case was later reviewed and referred to the European Court of Justice (Nakashima, 2015).

The CJEU declared the Safe Harbor agreement of 2000 invalid, stating that it placed "National security, public interest, or law enforcement requirements" over privacy rights (Nakeshima, 2015). Additionally, the Court of Justice ruled that Data Protection Authorities have full investigative rights when claims are made about the adequacy of protections (Coudert, 2016) and can suspend data transfer to non-EU countries that violate protections, even if those protections were previously ruled adequate (Meyer, 2016-1). In its decision, the court cited specific protections that would be needed to guarantee "adequate" data protections, taking aim at Section 702 of the Foreign Intelligence Surveillance Act (St. Vincent, 2015). FISA Section 702 allows intelligence services to target communications of non-US persons and was used to authorize warrantless surveillance of individuals outside of US borders for intelligence purposes and formed the basis of the PRISM and Upstream collection programs at the NSA

(Rotenberg & Fitzgerald, 2017). By March of 2014, Safe Harbor privacy principles had been deemed inadequate by the EU Parliament, which called for its suspension (Wilhelm, 2016).

Four thousand US businesses used the Safe Harbor framework to legally transfer European personal data to the US before it was invalidated (Chung, 2016). When Safe Harbor was struck down, data transfer did not grind to a halt, but thousands of companies were in danger of facing sanctions for being out of compliance with Europeans laws regarding personal data (Nakashima, 2015). Following the Schrems case, a conference of German Data Protection Authorities issued a position paper stating that transfers based solely on Safe Harbor were prohibited. The DPAs also called a moratorium on rulings for new Binding Corporate Rules and export agreements (Ritzer, 2015). A statement from the Article 29 Working Party confirmed that Binding Corporate Rules and Standard Contractual Clauses could still be used for data transfer. The Article 29 Working Party's statement also called on EU member states to open discussions with the US regarding solutions enabling data transfers that "respect fundamental rights." (Article 29 Working Party, 2016).

EU Data Protection Authorities delayed enforcement of continued transfers of data to the US until January 2016, with the first crackdown on continued data transfer under Safe Harbor coming from the Hamburg DPAs (Meyer, 2016) Three companies were questioned and found not to have updated their data transfer practices after the Safe Harbor invalidation. Adobe, Punica, and Unilever were fined thousands of euro based on their continued reliance on the invalidated Safe Harbor framework; larger fines were possible but reduced when the businesses began using legal methods of data transfer (Segalis, 2016).

The Article 29 Working party made the following statement regarding Schrems Case decision:

> "Transfers to third countries where the powers of state authorities to access information go beyond what is necessary in a democratic society will not be considered as safe destinations for transfers" (Article 29 Working Party, 2016)

The Safe Harbor program contained exceptions for national security that had no limitations imposed (Coudert, 2016), and the major concern in overturning Safe Harbor was mass surveillance by US intelligence agencies (Mullock, 2016). Many of the companies involved in the US government's PRISM surveillance program were themselves Safe Harbor certified (Coudert, 2015). The Court of Justice of the EU, in its examination of the validity of Safe Harbor, did not assess the legitimacy of the United States' PRISM surveillance program. Instead, it decided that Safe Harbor was an invalid mechanism because it bound only the self-certifying company, not the US government itself (Coudert, 2016). Unfortunately for US companies, the same could be said of most other data transfer mechanisms without lasting reforms to US policy.

3. Contractual Protections

3.1. Data Protection Authority Approval

The Data Protection Directive established Data Protection Authorities in each member state which monitor and enforce the data protection laws; these authorities are independent of the government and advise national institutions on data protection matters. Some variation exists in the powers afforded to DPAs across the EU member states based on national law, but all have enforcement power and the ability to bring sanctions and legal action within their own member state (Gabel & Hickman, 2016-2). A business may transfer data to a third country if the Data Protection Authority from its member state has deemed protection of the receiving company adequate (European Commission, 2016). This option offers higher flexibility than the Standard Contractual Clauses but can have high overhead, as each Data Protection Authority has its own rules and processes and would need to be consulted for any contract amendments (Taylor Wessing, 2013).

Alyssa Robinson, lyssanr@yahoo.com

Data Protection Authorities for the data controller's country can authorize transfer to a third country if contractual provisions fulfill requirements laid out in the Data Protection Directive (European Commission, 2016). The General Data Protection Regulation also allows transfer pursuant, to self-regulating adherence, to approved "codes of conduct". Similarly, certification of processors and controllers outside of the EU will permit data transfer (Myers, 2016). Given the findings of the CJEU in the Schrems case, these same Data Protection Authorities have the right to review and remove their approval if circumstances change.

3.2. Standard Contractual Clauses

Standard Contractual Clauses, also known as "Model Clauses," are contractual provisions drafted by the European Commission or individual member-state Data Protection Authorities which can be used to authorize cross-border data transfer (Gabel & Hickman, 2016) between a Data Controller and a Data Processor. The Data Controller is the legal entity that determines the "Purposes and means of the processing of personal data," while the Data Processor is the legal entity that collects, stores, alters or uses that data (European Commission, 2016). Standard Contractual Clauses must be inserted into contracts verbatim and be incorporated into all sub-processor contracts for onward transfer to be valid (Association of Corporate Council, 2016).

The European Commission has created two sets of Standard Contractual Clauses for transfer of data to data controllers outside of the EU, as well as one set for data processors. The two sets of Standard Contractual Clauses provide similar levels of data protection, but the second set – laid out by the Commission in 2004 – has clauses related to litigation, audit, and responsibility that are more business-friendly (European Commission, 2016). These clauses give greater power to Data Protection Authorities to intervene when needed; data transfer can be blocked if the clauses are not being complied with, or if the laws of the third country will not allow the importer to adequately respect the clauses (European Commission, 2016). The Standard Contractual Clauses are enforceable only by the Data Protection Authorities and the data subjects themselves (Association of Corporate Council, 2016), though the Model Clauses do provide a right of audit for the data exporters (Neiditze, 2016). Standard Contractual Clauses do not

currently address government surveillance activities, which has left them vulnerable to legal challenges (Association of Corporate Council, 2016).

4. Binding Corporate Rules

Binding Corporate Rules govern data personal data transfer within a multi-national corporation and must be approved by the relevant Data Protection Authorities (Gabel & Hickman, 2016). They are designed for strictly hierarchical multinational companies, not loose conglomerates; when used as safeguards, they must be both binding and legally enforceable, with disciplinary sanctions for breach (EC, 2009). It is recommended that multinational corporate groups have a single set of rules for all personal data being processed, with enforcement of those rules directed by the member company based in the EU (EC, 2016).

The exact content of the Binding Corporate Rules is left to the corporations bound by them, though the Article 29 Working Party has created a sample framework to help organizations develop these rules (European Commission, 2009). Similar to the rights outlined in the standard contractual clauses, the principles which a data subject should be entitled to enforce as third party beneficiary rights are as follows:

- Purpose limitation
- Data quality and proportionality
- Criteria for making the processing legitimate
- Transparency and easy access to Binding Corporate Rules
- Rights of access, rectification, erasure, blocking of data and objection to the processing
- Rights in case automated individual decisions are taken
- Security and confidentiality
- Restrictions on onward transfers outside of the group of companies
- National legislation preventing respect of BCR
- Right to complain through the internal complaint mechanism of the companies

- Cooperation duties with Data Protection Authority
- Liability and jurisdiction (European Commission, 2009)

Binding Corporate Rules must guarantee training that focuses on awareness and implementation of the rules, audit of compliance – either internally or by external independent auditors – in addition to a system for handling complaints (European Commission, 2009). The General Data Protection Regulation provides additional guidance on what must be included in the Binding Corporate Rules, as well as giving them full legal recognition and expanding their use beyond multi-national corporations to groups of business partners (Paternaki, 2016).

5. Privacy Shield

5.1. Program Creation

The Court of Justice of the European Union invalidated Safe Harbor in October of 2015 and companies were required to immediately seek other legal mechanisms for personal data transfer, with the Article 29 Working Party calling for enforcement actions after January 2016 for those that did not comply (Weiss & Archick, 2016). On February 2, 2016, the Privacy Shield agreement was announced, with the full text released on February 29. This original draft was rejected due to, among other issues, a lack of protection against the mass surveillance of EU citizens (Chung, 2016). The Article 29 Working Party was concerned that the initial Privacy Shield proposal did not include an obligation to delete data that was no longer relevant and did not fully exclude continued mass surveillance.

The final Privacy Shield agreement was approved in July of 2016 by representatives from EU member states and endorsed by the European Commission four days later (Chung, 2016). It included clarifications regarding data retention rules, onward transfer rules, bulk data collection and "mass surveillance" as well as the role of the Privacy Shield Ombudsman (Mullock, 2016).

Alyssa Robinson, lyssanr@yahoo.com

When the Article 29 Working Party published its opinion on Privacy Shield, it was neither strongly for nor against the solution. It acknowledged the improvements made from Safe Harbor, specifically calling out its applicability to government data access (Jeppesen, 2016) but notes that bulk data collection is still authorized under FISA Section 702 and raises questions about whether the Privacy Shield Ombudsman is sufficiently independent (Jeppesen, 2016). Its adequacy decision cites privacy improvements made by President Obama in Presidential Policy Directive 28 and the USA Freedom Act. PPD-28, which so far remains in force with the change of administration, states that signals intelligence activities in the US must have appropriate safeguards for individuals regardless of nationality (European Commission, 2016-2). Under PPD-28, targets should be specific and focused, and mass collection can only be used for specific national security threats, following the principles of necessity and proportionality (European Commission, 2016-2). The USA Freedom Act prohibits bulk records collection based on pen register or trap and trace, requiring the use of specific "selection terms" (European Commission, 2016).

5.2. Differences from Safe Harbor

As with Safe Harbor, companies self-certify that they meet the Privacy Shield requirements by signing up on the Privacy Shield website. A corporate officer completing the Privacy Shield self-certification must provide data about the organization, its use of personal data and privacy policies, as well as an independent recourse mechanism for unresolved complaints (IT, 2016). Once signed up, the commitment to comply with the Privacy Shield framework is enforceable under US law (ITA, 2016). Overall, the principles of the Privacy Shield program are largely the same as those of the Safe Harbor framework (Paul Hastings, 2016), including seven principles that must be followed.

Privacy Shield was designed to provide stronger protections for EU personal data than the Safe Harbor program (Neiditz, 2016). While Safe Harbor was never intended to restrict collection of data for national security purposes (Future of Privacy Foundation, 2013) Privacy Shield provides limitations and oversight for law enforcement and intelligence access to private data (Paul Hastings, 2016). With Privacy Shield, companies also move from a self-regulated Safe Harbor system to active monitoring by the

Department of Commerce (Paul Hastings, 2016). While these key differences enabled the EU approval of Privacy Shield, it is the surrounding regulations and policies of the US government that will decide whether it stands.

6. Questions About the Future

6.1. Schrems II

Following the CJEU ruling in the Schrems case that struck down the Safe Harbor framework, Facebook switched to using Standard Contractual Clauses as a legal mechanism for transferring personal data to the US (Edwards, 2017). Max Schrems, now a lawyer, has updated his original complaint against Facebook, alleging that the Standard Contractual Clauses now in use also fail to provide adequate legal protection (EPIC, 2017). The Irish Data Protection Authority issued a draft decision on Schrems II in May of 2016, stating that without any legal remedy for EU citizens under US law, the Contractual Clauses were invalid (Edwards, 2016). The Irish DPA did not determine that it had the authority to declare the European Commission's Standard Contractual Clauses inadequate, so it referred the cases to the Irish High Court, which referred the Schrems case to the EU Court of Justice for a ruling (Epic, 2017). Once decided, this case could invalidate the use of Standard Contractual Clauses for US transfer entirely or require updates to huge numbers of contracts already in use.

As of 2016, 80% of the companies transferring personal data from the EU to the US were using Standard Contractual Clauses (Edwards, 2016). Collectively, the European Union is the US's largest trading partner, with $260 million in digital services exchanged annually (Kerry & Raul, 2017). Invalidating the Model Clauses as a transfer mechanism could leave many businesses unable to carry out business activities (Edwards, 2017). The Schrems case was heard before the Irish High Court beginning in February 2017, but no judgment has yet been made. Significant changes have been made to US law regarding surveillance data on US Citizens since the first Schrems case, but issues such as FISA Section 702 remain. Data protection authorities are already given the power to block data transfer if the third country's laws do now allow Standard Contractual Clauses to be adequately followed (European Commission, 2016), providing a path that blocks transfer

via Model Clauses to the US without disrupting trade to other countries. Given the populist policies of the Trump Administration, such a move could be seen as an attack on American businesses, resulting in increased protectionism and trade barriers with Europe.

6.2. Challenges to Privacy Shield

By early 2017, more than 1700 companies had enrolled in the Privacy Shield program, and the program was already being challenged by both the Irish privacy group Digital Rights Ireland (Edwards, 2017) and a collection of French groups led by privacy advocate La Quadrature (Reuters, 2016). Max Schrems, whose case challenging Standard Contractual Clauses is still pending, has also vowed to fight Privacy Shield (Chung, 2016).

Digital Rights Ireland has made several claims regarding the inadequacy of Privacy Shield, including the allegation that the "privacy principles" outlined are not an international commitment within the framework of the EU Data Protection Directive (Edwards, 2016). The Digital Rights Ireland case asserts that laws regarding surveillance must still limit storage of personal data, access to that data, and restrictions on further use. Individual must also have the right to legal remedy regarding those matters (Coudert, 2016). The claim, filed with the General Court of the European Union, seeks to annul the "finding of adequacy" decision for Privacy Shield (Edwards, 2016). While this case has not been settled, it contributes to the general climate of uncertainty around Privacy Shield and personal data transfer (Usturan, Cohen & Gasztonyi, 2016).

The challenge from La Quadrature also centers on inadequate protections around mass surveillance (Reuters, 2016), including limitations on collection and flaws in the redress and oversight mechanisms (La Quadrature, 2017). La Quadrature believes that reform of the US FISA Amendments Act, which authorized the PRISM and Upstream surveillance programs, is necessary to meet the standard of data protection required for EU citizens. With multiple legal challenges focusing on Section 702 of FISA, EPIC and other groups are recommending enhanced public reporting and strengthening of the FISA court authority to better balance national security and privacy rights in the US (Rotenberg & Fitzgerald, 2017). The FISA Amendments Act will expire at the end of 2017 unless extended by Congress. So far, proposed reforms do provide further protection for US

citizens, but not those of the EU (La Quadrature, 2017). Both the Digital Rights Ireland and the La Quadrature cases are still pending but may be struck down because suits can only be brought to the EU court by a challenger directly affected by the law (Reuters, 2016). Should these cases be dismissed, it is hard to imagine that another challenger would not take up the fight with a stronger case. Challenges to both Privacy Shield and the use of Standard Contractual Clauses could be used to pressure the United States into reforms for FISA Section 702, providing more meaningful limits and reporting on mass surveillance of EU citizens.

6.3. Trump Executive Orders

Both the Privacy Shield and the EU-US Umbrella Agreement, which goes into effect February 1, 2017, were enacted under the Obama Administration to enhance privacy protections for EU citizens (Burgess, 2017). The EU-US Data Protection Umbrella Agreement provides protection for data transferred as a part of law enforcement cooperation, ensuring limitations on use, onward transfer, retention and right of access (European Commission, 2016). As part of this agreement, the lawfulness of data transfers is guaranteed, and EU citizens are granted the same rights of redress in privacy breaches as US citizens under the Judicial Redress Act (EPIC, 2017).

In January of 2017, US President Trump issued the "Enhancing Public Safety in the Interior of the United States" Executive Order. While primarily concerned with enforcement of immigration laws, this order excludes non-US citizens from the privacy policies of US Government agencies such as the Federal Bureau of Investigation and the National Security Agency (Burgess, 2017). The order also requires federal agencies to clarify that the Privacy Act extends only to citizens and lawful permanent residents of the US (Hunton Williams, 2017). Following the order, the Department of Homeland Security's website now states that it will "no longer afford Privacy Act rights and protections to persons" who aren't citizens or lawful permanent residents. This act further threatened the viability of Privacy Shield; with no clear statements from the Trump Administration the EU must watch to see how future cases are handled.

The 1974 Privacy Act prohibited the sharing of personal data about a particular subject between federal agencies without consent unless the sharing fell under one of twelve exceptions (Training, 2017). One of these exceptions was for "Law Enforcement Requests", with no requirement that the request be backed by necessity (Training, 2017). The Judicial Redress Act, signed by Obama, had extended these rights to citizens of covered countries (Hunton Williams, 2017). This action formed part of the basis for Privacy Shield's adequacy decision; this Executive Order will focus scrutiny on the Privacy Act, which the US Justice Department itself has called outdated and difficult to apply (Training, 2017). The Executive Order does refer to federal agencies acting in a manner "compliant with applicable law" – in this case, the Judicial Redress Act -- which could preserve the rights of Europeans (Hunton Williams, 2017). Even if those rights are preserved, the tenor of Trump's actions in this regard could have a negative effect on the Privacy Shield review coming in 2017 (Hunton Williams, 2017), with EU Justice Commissioner Vera Jourova stating in January of 2017 "I need to be assured that Privacy Shield can remain." Other European leaders have engaged in similarly strong rhetoric with regard to Trump policies, potentially causing more friction and uncertainty.

7. Practical Comparison of Options for Legal Data Transfer

When determining which data transfer mechanism works best for a particular organization, there are many factors to consider, including the types of data being transferred and their sensitivity, as well as any transfer mechanisms that might currently be in place (Paul Hastings, 2016). Also important to consider are the legal challenges and political threats that could require changes or even nullify the ability to transfer data legally over the coming months or years.

For organizations looking to transfer human resource or customer data internally, Binding Corporate Rules are an obvious option. Binding Corporate Rules are often viewed as providing greater privacy protections than the EU Standard Contractual Clauses (Ritzer, 2015). Their flexibility and low administrative burden also make them a favored data transfer mechanism (Myers, 2016). Binding Corporate Rules are, however,

full privacy programs. They can work well for large global corporations, where putting Standard Contractual Clauses in place between affiliates may be cumbersome or even impossible, if all are operating as one legal entity. They may, however, fail to scale down for smaller companies – as of 2016, only 80 organizations had Binding Corporate Rules in force (Future of Privacy Foundation, 2013). Initial setup can require years to get approval from multiple DPAs, and the ongoing program requires accountability in the form of training, audit, and Data Protection Officers (Allen Overy, 2013). These internal rules, of course, do not cover transfers outside of a corporation, so some other mechanism may also need to be put in place. With the expansion of Binding Corporate Rules under the General Data Protection Regulation to cover partner relationships and the lack of legal challenges facing Binding Corporate Rules, it is likely they will become increasingly popular over the coming years (Pateraki, 2016).

For transfers of data outside of the organization, businesses can consider using the EU Model Clauses or signing up for the Privacy Shield program. Companies that have been successful with Standard Contractual Clauses may not wish to take on the additional requirements for certification and enforcement required by the Privacy Shield program (Neiditz, 2016). Privacy Shield compliance requires annual re-certification, with review and oversight from the Department of Commerce. While the Standard Contractual Clauses do not require the involvement of the US government, they may require EU Data Protection Authorities to verify the clauses in some countries (Association of Corporate Council, 2016) until the GDPR goes into effect in 2018. Privacy Shield enforcement falls under multiple bodies, including the Federal Trade Commission, the Department of Commerce, the Privacy Shield Panel, required independent dispute resolution bodies and in some cases the EU member state Data Protection Authorities as well (Association of Corporate Council, 2016). Requirements for enforcement, review, and complaints are more rigorous than those laid out in the Standard Contractual Clauses, and the FTC is likely to enforce Privacy Shield more actively, given the history of Safe Harbor (Neiditz, 2016). Given the extremely low overhead involved in signing up for the Privacy Shield program, there is danger organizations may self-certify without fully committing to the program and find themselves in trouble if they do not follow through on their promises.

Alyssa Robinson, lyssanr@yahoo.com

Up until now, the Standard Contractual Clauses have not required any updates following adoption (Association of Corporate Council, 2016). Should there be future revisions to the Standard Contractual Clauses, however, contract reviews would be required for all customers and sub-processors with whom the Model Clauses had been leveraged (Association of Corporate Council, 2016) and changes could be likely following the current legal challenge in the Schrems case. Those not yet leveraging Standard Contractual Clauses extensively may find the Privacy Shield mechanism more streamlined than negotiating with business partners and potentially updating terms into multiple contracts (Neiditz, 2016).

Overall, Privacy Shield is the most flexible of the possible mechanisms for data transfer, since it covers most transfers of personal data from the EU to the US without proscribed contractual provisions (Paul Hastings, 2016). Privacy Shield may also offer a competitive advantage to certifying companies based on their perceived commitment to security and privacy rights (Neiditz, 2016). The EU Model Clauses may be inflexible for certain business situations, and can also deprive consumers of transparency about data transfers since they are contained within private contracts (Future of Privacy Foundation, 2013). On the other side, none of the Standard Contractual Clauses include any explicit sanctions for violations, whereas Privacy Shield may require compensation for individual losses, as well as requiring data deletion in cases of non-compliance (Neiditz, 2016). If an organization has a small number of business partners with whom they transfer data and have business needs that can be met by the Model Clauses, they can avoid involving multiple US government agencies in their European business.

With legal and political threats facing both Standard Contractual Clauses and Privacy Shield, neither holds a clear advantage in stability. There is a strong possibility that the current Privacy Shield challenges will be unsuccessful, given that the plaintiffs have not been directly harmed by the program (Reuters, 2016). Even without another challenger, however, the European Commission will re-visit Privacy Shield in 2017, this time in the political climate of a Trump Administration that campaigned on a position of protecting

America at the expense of other nations. With the Irish DPA already finding cause to question the adequacy of protection provided by Standard Contractual Clauses, it may be difficult for the CJEU to let the Clauses stand as-is (Gardner, 2016). Given the high stakes involved in US-EU trade, both sides will be anxious to patch the holes needed to restore legal cross-border data transfer.

7.1. Keeping Data Within Europe

Given the challenges of finding a data transfer mechanism that fits all of an organization's needs and the costs associated with a mechanism being invalidated or substantially changed, more companies are finding ways to keep European personal data inside of Europe (Scott, 2016). While some business data regarding customers may need to reside within headquarters or be distributed throughout an organization's operating locations, personal data on European consumers can be stored within European datacenters, keeping the data subject to EU privacy laws. The General Data Protection Regulation, when it goes into effect in 2018, will make it explicitly illegal to transfer any personal data out of the EU in response to a third country's law enforcement request (Myers, 2016).

Keeping customer data within Europe may require changes to overall systems architecture, for example using a federated architecture to allow customers to pull reporting data from multiple geographically-distinct sources. Merely storing the personal data within Europe, however, is not enough to relieve the burden of legal data transfer mechanisms for multi-national corporations, since personal data could be accessed, rendered or downloaded by a US employee. New policies or authorization requirements may need to be enforced around data access or administration to ensure processing activities happen entirely within the EU (Rossi, 2016), or compromises may be made to functionality to limit mixing of US and EU data.

With huge growth continuing in public cloud service adoption (IDC, 2016), Infrastructure as a Service provide an easy way for companies to store data in Europe without an investment in hardware and real estate. IaaS providers such as Amazon, Google, and Microsoft provide hosting in multiple European locations and guarantee that

data will not be transferred out of a customer's desired region (Amazon, 2016). In 2014, Microsoft received approval from the Article 29 Working Party for its cloud service offering's data processing agreement (Smith, 2014), with Google and Amazon Web Services following suit in 2015 (Vogels, 2015). All three also participate in the Privacy Shield program, providing flexibility for their customers and hedging their bets on the future of these mechanisms for personal data transfer. Many service providers also provide benefits in the form of security features which can be used to ensure data protection and regulatory compliance.

Table 1 Transfer Mechanism Reference Table

TRANSFER MECHANISM	APPLICABILITY	ADVANTAGES	DISADVANTAGES	THREATS & ISSUES
Data Protection Authority Approval	An "ad hoc" contract can be approved for transfer of personal data outside of the EU by Data Protection Authority in the member state of the data controller if it is deemed to provide an "essentially equivalent" level of protection.	Flexible: does not require set contractual clauses, can be leveraged within a corporation or between unrelated organizations.	May require approval from multiple Data Protection Authorities, applying different rules. Subject to periodic review and challenge.	Approval decisions are subject to periodic review and changing political climate could lead to challenges for contracts previously found to provide an adequate level of protection.
Binding	Applies to transfer	Low overhead,	Don't cover data	No current

Corporate Rules	of personal data between parts of a multi-national corporation.	flexible, demonstrates a commitment to development and enforcement of multi-national privacy program.	transfer outside of a corporation. Require infrastructure to maintain and enforce full privacy program, so may not scale down to smaller organizations. Require DPA review and approval.	challenges, but invalidation of SCCs could have implications for BCRs as well.
Standard Contractual Clauses	Applicable to contracts for data transfer that can use the model clauses verbatim.	Do not require further approval or periodic review. Have not yet required modification.	Inflexible, as must be used without modification. Must be negotiated into each contract and may require update across multiple contracts if changes are introduced.	Currently facing challenge in Schrems v. Facebook. Initial finding of inadequacy, referral to CJEU for decision in 2017.
Privacy Shield	Transfer of personal data from EU to US for all self-certifying organizations.	Flexible, covers all possible transfers of personal data to US. Demonstrates commitment to	Requires annual re-certification. Explicit sanction provisions for violation. Multiple authorities have stake in	Currently facing challenge from Digital Rights Ireland, La

		privacy program.	enforcement, including FTC, DPAs, US Dept. of Commerce, Privacy Shield Panel	Quadrature. Several others, including Schrems committed to challenge.

8. Conclusion

Organizations have multiple options for legal transfer of personal data to the United States, including approval by Data Protection Authorities, Binding Corporate Rules, Standard Contractual Clauses, and the Privacy Shield Program. When examining the methods for legal transfer of personal data from the EU to the US, companies have to consider the types of data they will handle, along with their industry and associated regulations. They need to understand their global market, their footprint, their exposure to EU citizens, as well as their internal vendor management programs, and human resources and contracts management capabilities (Paul Hastings, 2016). They must also carefully consider the political actions and legal threats that may negate current options in the future. As shown by the recent challenges, all of these options are likely to evolve quickly in the coming years, forcing corporations to adapt following new legislation, shifting consumer awareness, judicial rulings and political climates. Businesses with a large proportion of European customers may be wise to consider keeping personal data within Europe or investing in privacy programs that align with General Data Protection Regulations, regardless of the legal mechanism chosen for data transfer.

Alyssa Robinson, lyssanr@yahoo.com

References

Allen & Overy. (2016). The EU General Data Protection Regulation. Retrieved February 15, 2017, from http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

Amazon Web Services. "Whitepaper on EU Data Protection." N.p., Dec. 2016. Web. 6 Mar. 2017.

Article 29 Working Party. "Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision." April 13, 2016. Accessed January 29, 2017. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

Association of Corporate Council. (2016, May 24). Legal Resources. Retrieved January 17, 2017, from http://www.acc.com/legalresources/publications/topten/transferring-personal-data.cfm

Bamberger, K., & Mulligan, D. (2016, June 06). Opinion: Is your data really safer in Europe? Retrieved January 29, 2017, from http://m.csmonitor.com/World/Passcode/Passcode-Voices/2016/0606/Opinion-Is-your-data-really-safer-in-Europe

Burgess, M. (2017, January 27). New presidential order could wreck US-EU Privacy Shield. Retrieved February 02, 2017, from http://www.wired.co.uk/article/trump-privacy-shield-data

Kelly, C., and A. Raul. "The Economic Case for Preserving PPD-28 and Privacy Shield." *Lawfare*. N.p., 17 Jan. 2017. Web. 12 Mar. 2017.

Chung, M., Howell, C., Kalyvas, J., Millendorf, S., & Tantleff, A. (2016, January 12). Safe Harbor Replacement EU-US Privacy Shield Approved. Retrieved January 09, 2017, from http://www.natlawreview.com/article/safe-harbor-replacement-eu-us-privacy-shield-approved

Connolly, C. (2008, December 2). Galexia Internet. Retrieved February 26, 2017, from http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/

Coudert, F. (2015, October 14). Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities. Retrieved February 04, 2017, from http://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/

Determann, L., Hengesbaugh, B., & Weigl, M. (2016, September 12). The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options. Retrieved January 11, 2017, from https://www.bna.com/euus-privacy-shield-n57982076824/

Edwards, E. (2016, November 09). Formal challenge to Privacy Shield pact published. Retrieved February 11, 2017, from http://www.irishtimes.com/business/technology/formal-challenge-to-privacy-shield-pact-published-1.2861688

Edwards, E. (2017, February 06). All you need to know in the Max Schrems-Facebook case. Retrieved February 11, 2017, from http://www.irishtimes.com/business/technology/all-you-need-to-know-in-the-max-schrems-facebook-case-1.2965482

European Commission. (2003). Analysis and impact study on the implementation of Directive EC 95/46 in Member States. Retrieved March 5, 2017, from http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf

European Commission. (2009). "FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES." Retrieved January 26, 2017, from European Commission, 2009. Http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf. Web. 26 Jan. 2017.

European Commission. "Model Contracts for the transfer of personal data to third countries." *Model Contracts for the transfer of personal data to third countries - European Commission*. N.p., 24 Nov. 2016. Web. 23 Jan. 2017.

European Commission. (2016, December 1). Questions and Answers on the EU-U.S. Data Protection "Umbrella Agreement". Retrieved February 02, 2017, from http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm

European Commission. (2016, July 12). COMMISSION IMPLEMENTING DECISION of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Retrieved March 14, 2017, from http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

Evans, M., and S. Daddar. "Irish Data Protection Commissioner to Request Court Declaration as to Validity of Personal Data Transfers to the US Under EU Model Clauses." Data Protection Report. May 26, 2016. Accessed January 29, 2017. http://www.dataprotectionreport.com/2016/05/irish-data-protection-commissioner-to-request-court-declaration-as-to-validity-of-personal-data-transfers-to-the-us-under-eu-model-clauses/.

Future of Privacy Forum. (2013, December). The US-EU Safe Harbor; An Analysis of the Framework's Effectiveness in Protecting Personal Privacy. Retrieved February 21, 2017, from https://fpf.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf

Gabel, D., & Hickman, T. (2016, July 22). Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation. Retrieved January 10, 2017, from http://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection

Gabel, D., & Hickman, T. (2016, July 22). Chapter 14: Data Protection Authorities – Unlocking the EU General Data Protection Regulation. Retrieved February 04, 2017, from http://www.whitecase.com/publications/article/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection

Hunton & Williams. (2017, January 31). Privacy Shield: Impact of Trump's Executive Order:. Retrieved March 08, 2017, from https://www.huntonprivacyblog.com/2017/01/28/privacy-shield-impact-of-trumps-executive-order/

International Trade Association. (2013). U.S.-EU Safe Harbor Overview. Retrieved January 14, 2017, from: http://2016.export.gov/safeharbor/eu/eg_main_018476.asp

International Trade Association. (2016). Welcome to the EU-U.S. Privacy Shield. Retrieved January 10, 2017, from https://www.privacyshield.gov/welcome

ITIC. (2016, February 16). The EU-U.S. Privacy Shield: What's at Stake. Retrieved January 9, 2017, from http://www.itic.org/dotAsset/9/b/9b4cb3ad-6d8b-469d-bd03-b2e52d7a0ecd.pdf

JAMS. (2017). EU-US Privacy Shield and Safe Harbor Programs | JAMS Mediation, Arbitration, ADR Services. Retrieved February 21, 2017, from https://www.jamsadr.com/eu-us-privacy-shield

Jeppesen, J. (2016, April 15). Center for Democracy & Technology | Keeping the Internet Open, Innovative and Free. Retrieved March 14, 2017, from https://cdt.org/blog/european-data-protection-authorities-chime-in-on-privacy-shield/

Martin, A. (2016, May 31). Top EU data cop slams Safe Harbor replacement as inadequate. Retrieved January 09, 2017, from http://www.theregister.co.uk/2016/05/31/eu_data_boss_says_safe_harbor_replacement_is_inadequate/

Meyer, David. "Here's a Big Reason Not To Breathe Easy About EU-U.S. Data Transfers Just Yet." Here's a Big Reason Not to Breathe Easy About EU-U.S. Data Transfers |

Fortune.com. February 03, 2016. Accessed January 29, 2017. http://fortune.com/2016/02/03/regulators-uneasy-privacy-shield/.

Meyer, David. "Here Comes the Post-Safe Harbor EU Privacy Crackdown." Post-Safe Harbor Privacy Crackdown Begins (Exactly Where You'd Expect) | Fortune.com. February 26, 2016. Accessed January 29, 2017. http://fortune.com/2016/02/25/safe-harbor-crackdown/.

Mullock, J., & Fenelon, J. (2016, January 18). Safe Harbor Replacement Approved By European Commission. Retrieved January 09, 2017, from https://www.twobirds.com/en/news/articles/2016/global/safe-harbor-replacement-approved-by-european-commission

Myers, A. (2016, January 19). Top 10 operational impacts of the GDPR: Part 4 - Cross-border data transfers. Retrieved February 02, 2017, from https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

Nakashima, E. (2015, October 6). Top E.U. court strikes down major data-sharing pact between U.S. and Europe. Retrieved January 10, 2017, from https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html?utm_term=.d2b15493e9d2

Neiditz, J. (2016, February 29). Privacy Shield or Model Clauses: Which is Better for You? Retrieved January 19, 2017, from http://datalaw.net/privacy-shield-model-clauses-better-you/

Pateraki, A. "EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?" *World Data Protection Report*. Bloomberg, Mar. 2016. Web. 16 Mar. 2017. Reuters. "French Privacy Groups Challenge the EU's Personal Data Pact with U.S." *Privacy Shield: French Groups Challenge EU-U.S. Pact | Fortune.com*. Fortune, 02 Nov. 2016. Web. 13 Mar. 2017.

Ritzer, C., Zieger, C., Ashkar, D., & Evans, M. (2015, October 30). German Data Protection Authorities Suspend BCR approvals, question Model Clause transfers. Retrieved January 29, 2017, from http://www.dataprotectionreport.com/2015/10/german-data-protection-authorities-suspend-bcr-approvals-question-model-clause-transfers/

Rossi, B. "How the EU's unified data law will transform storage systems." *Information Age*. N.p., 19 Oct. 2015. Web. 16 Mar. 2017.

Rotenberg, M., & Fitzgerald, C. (2017, March 01). RE: Hearing on Section 702 of the Foreign Intelligence Surveillance Act [Letter to House Committee on the Judiciary]. Electronic Privacy Information Center, Washington, DC. https://epic.org/testimony/congress/EPIC-HJC-Section702-Mar2017.pdf

Schriver, R. (2002), *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777. Available at: http://ir.lawnet.fordham.edu/flr/vol70/iss6/29

Scott, Mark. "U.S. Tech Giants Are Investing Billions to Keep Data in Europe." *The New York Times*. The New York Times, 03 Oct. 2016. Web. 5 Mar. 2017.

Segalis, B., Ritzer, C., & Hoffman, A. (2016, June 08). Hamburg DPA's Safe Harbor Fines Spell Further Uncertainty and Risk for Global Companies. Retrieved January 29, 2017, from http://www.dataprotectionreport.com/2016/06/hamburg-dpa-fines-three-companies-for-continued-reliance-on-safe-harbor/

Smith, B. (2015, October 05). Privacy authorities across Europe approve Microsoft's cloud commitments. Retrieved February 28, 2017, from https://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/#sm.0001wk328zkpkfi4zyq1dxi6zmld5

St. Vincent, S. "Center for Democracy & Technology | Keeping the Internet Open, Innovative and Free." *Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance Reform | Center for Democracy & Technology*. N.p., 26 Oct. 2015. Web. 15 Mar. 2017.

Taylor Wessing. (2013, January). Using Model transfer terms and private contracts. Retrieved March 06, 2017, from https://www.taylorwessing.com/globaldatahub/article_model_transfer_terms.html

Training, A. (2017, January 30). Has President Trump's executive order on 'Public Safety' killed off Privacy Shield? Retrieved March 08, 2017, from https://www.theregister.co.uk/2017/01/30/trump_executive_order_public_safety_privacy_shield/

Trump, D. (2017, January 25). Executive Order: Enhancing Public Safety in the Interior of the United States. Retrieved March 08, 2017, from https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united

U.S. Department of Commerce. (2009, March). Guide to Self-Certification U.S.-EU Safe Harbor Framework. Retrieved February 21, 2017, from http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf

Usturan, E., Cohen, B., & GASZTONYI, K. (2016, November 13). Details of Legal Challenge to Privacy Shield Revealed. Retrieved March 05, 2017, from http://www.hldataprotection.com/2016/11/articles/consumer-privacy/details-of-legal-challenge-to-privacy-shield-revealed/

Vogels, W. (2015, March 31). European Union Data Protection Authorities Approve Amazon Web Services' Data Processing Agreement. Retrieved February 28, 2017, from http://www.allthingsdistributed.com/2015/03/aws-and-eu-data-protection.html

Wilhelm, E. (2016). A Brief History of Safe Harbor. Retrieved January 18, 2017, from https://iapp.org/resources/article/a-brief-history-of-safe-harbor/

Weiss, M., & Archick, K. (2016, March 19). U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Retrieved February 28, 2017, from https://fas.org/sgp/crs/misc/R44257.pdf