CENTER FOR EUROPEAN STUDIES
A JEAN MONNET CENTER OF EXCELLENCE

BRIEF: TRANSATLANTIC DATA PRIVACY

This document has been produced with the assistance of the European Union and the U.S. Department of Education. The contents of this publication are the sole responsibility of the UNC Center for European Studies and in no way can be taken to reflect the views of the European Union or the U.S. Department of Education.

INTRODUCTION:

Many Europeans use the internet and data services of US owned multinational corporations. Facebook and Google have assumed ubiquitous status across Europe, and have hundreds of millions of daily users across the continent. Other software as a service style companies, like Dropbox, Apple (who are better known as an integrated hardware and software provider) and Amazon (on its non-retail side) have smaller user communities, but their services are still widely used in Europe. These large internet-based companies have traditionally maintained their largest data-centers in the US. Consequently, the emails, photographs, videos and instant messages of European citizens have been stored in US data-centers. In transmitting this data across the Atlantic to be stored in the US, these companies committed themselves to upholding EU privacy standards. The voluntary regime that covered that commitment was known as Safe Harbor, and 4000 American companies had signed up to its principles.

The Safe Harbor principles involved businesses issuing an annual statement self-certifying that they were in compliance with the principles. The US Department of Commerce validated the vast majority of self-certifications and similarly managed a list of those companies with a valid certificate. Any monitoring of compliance with the principles was done by the Federal Trade Commission, who could deal with any breach of the code as an unfair or deceptive practice under the Free Trade Commission Act. Any of the signatory companies could disregard the principles or the promises made under Safe Harbor for certain defined law enforcement or national security purposes. In reality the penalties for breaching Safe Harbor or any of the existing European regulations were not substantial – indeed it was more expensive to comply than it was to pay the fines for breaching codes, but the reputational risk for businesses ignoring the provisions were stark.

The Safe Harbor system was effectively ended by a legal case in the European Court of Justice (ECJ) that was brought by the Austrian law student, Max Shrems.[1] In his case against Facebook, Shrems was able to successfully argue that Facebook had breached EU privacy laws and this in turn caused the ECJ to declare on 6th October 2015 that Safe Harbor did not provide 'adequate protection of Europeans personal data'. The ECJ cited the revelations - and accusations - of Edward Snowden about the US intelligence community's mass interception, storage and analysis of European communications data as weighing heavily on their concerns about the use of data in the United States. Given that Safe Harbor had covered the transfer of EU citizens' data, it was equally clear that the ECJ's annulment needed to be addressed quickly, in order that both European citizens and companies wishing to operate in the EU know what rules they are operating under. The European Commission and US authorities finalized their negotiations on data and privacy between October 2015 and January 2016 to provide an agreement that would comply with the ECJ's concerns. They announced this negotiated compromise as 'The Privacy Shield' on 29 February

2016, but it has still to work its way through the European Parliament and the various legal compliance committees required for it to become operative in the EU. To partly address the concerns regarding US intelligence activity in this space and as part of the new Privacy Shield, Robert Litt – from the US Office of the Director of National Intelligence - sent a letter to Brussels vowing not to violate the rights of EU citizens. Privacy campaigners have not been convinced by this letter, or the legal weight it might hold, given that any intrusion by US intelligence has to be reported to a named US diplomat for investigation and thus – they argue- is unlikely to see rulings against the US intelligence machinery.

The Privacy Shield mechanism agreement was struck with the aim of providing the balance between data flows for commercial purposes and to adequately protect EU personally identifiable information (PII). The Privacy Shield locates PII as being personally held rather than as the abstract concept as implied by Safe Harbor. The Shield also gives European citizens the right to seek redress against US companies in US courts, a measure that improves the protection of EU citizens. Both the EU and US stated that they see the Shield as being a complementary agreement with those measures agreed on Passenger Name Records (PNR) and banking transactions (SWIFT/TFTP). Although the Shield is yet to be fully enacted (as it is still needs to be approved by EU member states, and is likely to be challenged in the ECJ as Safe Harbor was) we are likely to be able to observe a bifurcation of redress, from relatively strong protections against US companies (albeit without the prospect of financial redress), to relatively weak protections against a US intelligence community that has enjoyed great success and analytical traction from mass surveillance. The US intelligence community has been often subject to regulation by revelation, rather than by official oversight processes, in the last decade and has come to be seen as a sector that can do as it pleases: something which is a touch unfair.

Like Safe Harbor, the Privacy Shield enables companies to self-certify that they are in compliance, and once they have announced that they are in compliance breaches are initially addressed to the data-controller and can later be redressed through the US courts system if necessary. The costs of bringing a case under the Privacy Shield falls to the company, rather than on the individual bringing the case, which opens up access to justice for EU citizens. The measures also allow for greater cooperation between US and EU authorities, and similarly place at the center of the plans greater access to information so that European citizens have a greater opportunity to understand how their data is used and protected, and what rights they have in relation to data protection. It strengthens the requirements placed by Safe Harbor in terms of the requirements in place for using third party companies (like data warehouses) and also sets in train an annual updating process at the EU-US level to allow both sides to respond quickly to changes in technology (something that regulators have proved to be bad at), and to respond to valid criticisms before they get to the ECJ, thus avoiding the potential for a re-run of the Safe Harbor judgment.

In wider terms, finding alignment between the US and EU on data privacy legally and culturally has been a recurring problem of the past decade. The debates and negotiations across the Atlantic have been organized around three key issues: 1) Passenger Name Records, 2) Financial records (SWIFT), and 3) the Safe Harbor rules, which - as has been mentioned above - the European Court of Justice struck down in October 2015. These agreements have covered both the commercial and security dimensions of data privacy. Whilst Passenger Name Records and financial data (SWIFT) have been primarily focused on security, Safe Harbor and its replacement the Privacy Shield have been most focused on the commercial dimension, which currently accounts for an estimated $260bn per annum. It is the overlap between the commercial and security applications which concerns European privacy campaigners the most, particularly in the context of the received European view of US intelligence machinery engaging in dragnet surveillance of European citizens.

The misalignment of political cultures and traditions concerning data privacy is the root cause of the disagreements between the EU and US concerning data privacy. Excluding the undoubted nuance that exists on both sides of the Atlantic, the broad positions are:

Europeans are more comfortable with bigger government, with state provided services, and the state regulating a large amount of everyday life.

They are not - though - willing to tolerate a large security state or states having strong surveillance capabilities. Indeed, for European citizens – and this position is beginning to change in patches – they are more willing to tolerate terrorist atrocities as a consequence of constraining the ability of states to carry out intrusive surveillance.

In comparison, American citizens prefer ever smaller government and to remove the state and federal government from regulating ordinary life. But American citizens have shown themselves to be more tolerant of the state having well developed intelligence capabilities in order to protect national security and core US interests.

There have been many attempts to explain why there is such a difference in approach across the Atlantic, but the historic experience and legacy in Europe of the misuse of government power during the twentieth century seems to provide the most persuasive explanation of the enduring concern felt about losing control of personal data.

Gartner, a research company, has underscored the importance of data privacy - in terms of its scale - assessing that over half of the *Global 1000* businesses will have personal and customer sensitive data stored in data clouds by the end of 2016. This kind of dispersal has ramifications for those whose data is being held, and also data controllers: data may well be being stored across multiple jurisdictions. For businesses based in the US and EU, and operating in this new data environment, they need to know how to treat this personally identifiable information and how to protect it - as data controllers - in compliance with various legal codes, when data centers are spread across multiple jurisdictions.

As a response to the fall in data storage costs, the amount of data being stored, and the complexity of multiple jurisdiction storage, governments across Europe and the developed world are in the process of creating and amending regulations to cover personally identifiable information (PII), along with regimes to control and punish those who breach these rules. Knowing what is counted as PII, and what these regulatory regimes are have direct impacts upon controlling business is an increasingly important part of the compliance picture for businesses, both in terms of formal legal and regulatory compliance and the softer sort of compliance that can cause customer dissatisfaction and business losses. There are some obvious examples of personally identifiable information, such as names and addresses, dates of birth and zip code. But equally it might be possible to identify someone from social media photographs and video content, certain sorts of views that they express, career details, details about their schooling, and so on. In the case of social media, the file does not necessarily need to be tagged to become PII. So, the definition of PII is wide, precisely because the classes of information that can be used to identify someone are also wide.

EU DATA RULES

The rules governing EU data are currently controlled by the 1995 EU Data Directive.[2] The Directive sets down that information which originates or is generated within the EU area cannot travel outside of the wider European Economic Area (EEA) (EU plus three additional states) without being subject to adequate controls. The 1995 Directive sets out where data may travel without additional controls and equally where additional controls must apply. The European Parliament is currently (April 2016) debating amendments to a new data privacy directive that would place control of the use of personal data in the hands of individuals, whilst specifying how judicial and policing authorities can access it. All the states within the EEA are free to receive data without additional controls, and those nations outside of the EEA that meet the requirements of broad equivalence with EU protections are certified by the EU.[3] There are three basic criteria assessed by the Directive: 1) the robustness of the political and judicial system in the receiving nation, 2) the contractual controls in place and whether these deliver adequate protections, 3) the extent to which the contractual controls can be monitored and enforced. The United States is absent from the EU's list of approved nations. Both the EU and the US have insisted in the pre-eminence of their own respective rules and standards for data-privacy, which has resulted in an incompatibility. The absence of the US from the approved list is particularly unfortunate as the EU is keen for data to be capable of being transferred to the EU for the purposes of carrying on trade and other

commercial exploitation. Safe Harbor and now the Privacy Shield have been created to generate a bespoke solution to the absence of the US from the list of approved nations.

Outside of Safe Harbor and the impending Privacy Shield, there are four mechanisms recognized by the EU that allow businesses to sit in compliance with European data privacy rules. The four mechanisms are: 1) Binding corporate rules (BCRs), 2) binding corporate rules for processors (BCRP), 3) EU model contract clauses, and 4) customized contract clauses. The first two are rules that govern the global behavior of a firm towards data privacy, not just towards the EU rules. The BCR covers the usage of data by companies, whilst the BCPR covers companies offering cloud computing services. The EU believes that such a system would make data processing and storage firms attractive business partners as there would be no further compliance work to be done to do business with them. The EU's model contract clauses have been created so that they can be dropped into contracts - unamended - to bring any contractual arrangements around data into compliance, and to reduce the costs to business of creating their own customized contract clauses (the fourth route to compliance) which might be open to regulatory or legal challenge.

As the cost of cloud computing and cloud data storage continues to drop there will be an increased pressure for businesses to place PII in cloud servers. The risks to this data of being in the cloud have been brought into sharp relief by the alleged systematic intrusion by the intelligence agencies of Australia, Canada, New Zealand, the United Kingdom and the United States who collectively sit within an umbrella group known as the *Five-Eyes group* of strong intelligence nations. In reality though theoretical risks are created by movement of data across multiple jurisdictions by cloud service providers seeking to reduce their costs by contracting services across the world. Risks to the data and to compliance might therefore occur outside of the control of the business who is responsible for the data. This will place additional burdens on business procurement processes, who will have to account for the relative complexity of data privacy regulations and cloud servers based across the globe.

SAFE HARBOR AND THE PRIVACY SHIELD

Many Europeans use the internet and data services of US owned multinational corporations. Facebook and Google have assumed a ubiquitous status across Europe, and have hundreds of millions of daily users across the continent. Other software as a service style companies, like Dropbox, Apple (who are better known as an integrated hardware and software provider) and Amazon (on its non-retail side) have smaller user communities, but their services are still widely used in Europe. These large internet-based companies have traditionally maintained their largest data-centers in the US. Consequently, the emails, photographs, videos and instant messages of European citizens have been stored in US data-centers. In transmitting this data across the Atlantic to be stored in the US, these companies committed themselves to upholding EU privacy standards. As mentioned earlier in this brief, the voluntary regime that covered that commitment was known as Safe Harbor, and 4000 companies had signed up to its principles. These principles involved businesses issuing an annual statement self-certifying that they complied with the principles. The US Department of Commerce validated the vast majority of self-certifications and similarly managed a list of those companies with a valid certificate. Any monitoring of compliance with the principles was done by the Federal Trade Commission, who could deal with any breach of the code as an unfair or deceptive practice under the Free Trade Commission Act. Any of the signatory companies could disregard the principles or the promises made under Safe Harbor for certain defined law enforcement or national security purposes. In reality the penalties for breaching Safe Harbor or any of the existing European regulations were not substantial – indeed it was more expensive to comply than it was to pay the fines for breaching

codes, but the reputational risk for businesses ignoring the provisions were stark.

The Safe Harbor system was effectively ended by a legal case in the European Court of Justice (ECJ) that was brought by the Austrian law student, Max Shrems.[4] In his case against Facebook, Shrems was able to successfully argue that Facebook had breached EU privacy laws and this in turn caused the ECJ to declare on 6th October 2015 that Safe Harbor did not provide 'adequate protection of Europeans personal data'. The ECJ cited the revelations - and accusations - of Edward Snowden about the US intelligence community's mass interception, storage and analysis of European communications data as weighing heavily on their concerns about the use of data in the United States. Given that Safe Harbor had covered the transfer of EU citizens' data, it was equally clear that the ECJ's annulment needed to be addressed quickly, in order that both European citizens and companies wishing to operate in the EU know what rules they are operating under. The European Commission and US authorities finalized their negotiations on data and privacy between October 2015 and January 2016 to provide an agreement that would comply with the ECJ's concerns. They announced this negotiated compromise as 'The Privacy Shield' on 29 February 2016, but it has still to work its way through the European Parliament and the various legal compliance committees required for it to become operative in the EU. To partly address the concerns regarding US intelligence activity in this space and as part of the new Privacy Shield, which replaces Safe Harbor, Robert Litt – from the US Office of the Director of National Intelligence sent a letter to Brussels vowing not to violate the rights of EU citizens. Privacy campaigners have not been convinced by this letter, or the legal weight it might hold, given that any intrusion by US intelligence has to be reported to a named US diplomat for investigation and thus – they argue- is unlikely to see rulings against the US intelligence machinery.

The Privacy Shield mechanism agreement was struck with the aim of providing the balance between data flows for commercial purposes and to adequately protect EU personally identifiable information (PII). The Privacy Shield locates PII as being personally held rather than as the abstract concept as implied by Safe Harbor. The Shield also gives European citizens the right to seek redress against US companies in US courts, a measure that improves the protection of EU citizens. Both the EU and US stated that they see the Shield as being a complementary agreement with those measures agreed on Passenger Name Records (PNR) and banking transactions (SWIFT/TFTP). Although the Shield is yet to be fully enacted (as it is still needs to be approved by EU member states, and is likely to be challenged in the ECJ as Safe Harbor was) we are likely to be able to observe a bifurcation of redress, from relatively strong protections against US companies (albeit without the prospect of financial redress), to relatively weak protections against a US intelligence community that has enjoyed great success and analytical traction from mass surveillance. The US intelligence community has been often subject to regulation by revelation, rather than by official oversight processes, in the last decade and has come to be seen as a sector that can do as it pleases: something which is a touch unfair.

Like Safe Harbor, the Privacy Shield enables companies to self-certify that they are in compliance, and once they have announced that they are in compliance breaches are initially addressed to the data-controller and can later be redressed through the US courts system if necessary. The costs of bringing a case under the Privacy Shield falls to the company, rather than on the individual bringing the case, which opens up access to justice for EU citizens. The measures also allow for greater cooperation between US and EU authorities, and similarly place at the center of the plans greater access to information so that European citizens have a greater opportunity to understand how their data is used and protected, and what rights they have in relation to data protection. It strengthens the requirements placed by Safe Harbor in terms of the requirements in place for using third party companies (like data warehouses) and also sets in train an annual updating process at the EU-US level to allow both sides to

respond quickly to changes in technology (something that regulators have proved to be bad at), and to respond to valid criticisms before they get to the ECJ, thus avoiding the potential for a re-run of the Safe Harbor judgment.

INTELLIGENCE AND COMPATIBILITY WITH PRIVACY RIGHTS

The attacks in Paris and in Brussels have brought into sharp relief the imperative on western intelligence agencies to be sharing a wide range of intelligence data in order to effectively combat the insidious threats presented by Islamic State and its affiliates (see accompanying brief). Attempts at countering the radicalization of a section of young Muslims is likely to take too long in the context of preventing further attacks on US and European soil. The earlier measures concerning Passenger Name Records (agreed in 2011), and SWIFT (agreed in 2010) were both explicitly designed to improve the ability of US and European intelligence and security agencies to track the movement of people of concern and the financial logistics line of those people in response to the growing threat from transnational terrorism. In both cases there was concerted opposition from a significant cleavage of European policy makers, albeit on different grounds in each case.

With regards to PNR data, the complaints from European policy makers centered on the types of data being collected, and the end use of the data. For many European Parliamentarians the collection of data of travel being made exclusively within the European Union area seemed intrusive, similarly they complained about the collection of information they deemed to be irrelevant: such as data on relationship statuses and so on. In terms of the end-use, and this debate occurred prior to the Snowden debacle, there was considerable concern that there was no European control, nor adequate protections for the end use of the data, nor controls over where the data might be passed to. Some of these concerns were eased by a Parliamentary trip to the Department for Homeland Security in the Fall of 2010 to be briefed on how the data would typically be used. The PNR agreement has to be renewed in 2018. It is relatively easy to speculate that following the Snowden revelations European policy-makers will once again seek to enhance the protections covering data transferred to the US against the perceived excesses of the US intelligence machinery. However, this will be strongly counterbalanced by the need for enhanced cooperation between European and US intelligence to help counter the threats presented by Jihadist terrorists on mainland Europe. The near-collapse of Schengen and the realization that the free movement of people - whilst ideal for the running of a single market economy - presents a serious set of security vulnerabilities will likely see the use of PNR enhanced, rather than diminished and so there will be no need for the US Administration to use coercive diplomacy again around visa travel to secure a renewal of this agreement.

In the case of the 2010 SWIFT agreement, this allowed for American access to EU financial transaction data, for the purposes of tracking terrorist financing, as part of the 9/11 response from the Treasury Department which was encapsulated by the Terrorist Financing Tracking Program (TFTP). When the Belgian finance firm, SWIFT, which oversaw much of the international monetary exchange based its European and EEA records wholly in Europe this effectively barred the US from gaining US warrants to examine the data, as it had been able to before. The opposition from European policy-makers was again, as they saw it, the weak protections offered for bulk data transfers. Agreement was struck with Europol (the EU's policing and intelligence arm) being given oversight of whether such data requests were necessary for national security purposes. With the passing of time, we now know that financial tracking has been helpful in identifying security threats, and in forcing terrorist networks to explore analogue methods of transferring funds (known as *hawala*, which sees money physically moved through independent brokers which are immune to electronic surveillance) but which increase the risk to the money and those forced to use this method over and above contemporary banking tools.

SUMMARY

There are cultural and regulatory differences on data privacy between the US and EU. These differences have, since 2001, often been stark, with European legislators being less willing to use all means available in the fight against global terrorism than their American counterparts. This has meant that European legislators have constantly frustrated US legislators with their unwillingness to agree to measures that would improve collective counterterrorism efforts. With an increasing number of attacks on European soil, and a more complicated threat matrix that would be partly mitigated by an improved analysis of private data, there is a slow realization in Europe that it needs to align more closely with the US' view of data privacy for security purposes. This transformation will not be fully realized, and nor will it necessarily occur in the short-term, but the direction of travel seems set in those European states with capable intelligence agencies.

We can observe a similar picture with regards to the commercial use of personally identifiable information data, but in this instance the EU has been more assertive about the primacy of its rules and regulations concerning the use and protection of this data and consequently the EU has had to negotiate separate regimes with the US. This first regime, known as Safe Harbor, was struck down by the European Court of Justice in October 2015. Its negotiated replacement, the Privacy Shield - announced at the end of February 2016, is still to be ratified but improves protections for European citizens, whilst putting in place sensible review periods to allow both the US and EU to keep up with developing technologies. The soon-to-be ubiquity of cloud-based computing does place some tensions on the security of personal data (both in terms of variable practices, and also because of its vulnerability to cyber-attacks). Data that is tradable for commercial and security reasons has an intrinsic (and often monetary) value. Such a trade will form a significant backdrop to EU-US economic relations in the mid to long term, and as such the Privacy Shield, and other forms of reassurance and common understanding, will place this relationship on a firm footing.

WRITTEN: 8 APRIL 2016

ANNEX A
EU-US PRIVACY SHIELD: 29TH FEBRUARY 2016[5]

EU-U.S. PRIVACY SHIELD FRAMEWORK

1. EU individuals' rights and legal remedies:
    a. Individuals may bring a complaint directly to a Privacy Shield participant and the participant must respond to the individual within 45 days.
    b. Privacy Shield participants must provide, at no cost to the individual, an independent recourse mechanism by which each individual's complaints and disputes can be investigated and expeditiously resolved.
    c. If an individual submits a complaint to a data protection authority (DPA) in the EU, the Department of Commerce has committed to receive, review and undertake best efforts to facilitate resolution of the complaint and to respond to the DPA within 90 days.
    d. The U.S. Federal Trade Commission (FTC) has committed to work closely with the DPA to provide enforcement assistance, which, in appropriate cases, could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB ACT.
    e. The FTC has committed to vigorous enforcement of the Privacy Shield Framework. This includes prioritizing referrals from EU Member State DPAs, the Department of Commerce, privacy self-regulatory bodies, and independent recourse mechanisms. To better enable handling of EU DPA referrals, the FTC has committed to create a standardized referral process, designate a point of contact at the agency for EU DPA referrals, and exchange information on referrals with referring enforcement authorities, subject to confidentiality laws and restrictions.
    f. EU individuals are able to pursue legal remedies through private causes of action in U.S. state courts, including private causes of action for misrepresentation and similar types of claims.
    g. Privacy Shield participants must also commit to binding arbitration at the request of the individual to address any complaint that has not been resolved by other recourse and enforcement mechanisms.
    h. Program oversight and cooperation with EU DPAs:
        i. The Department of Commerce has committed to robust administration and supervision of the Privacy Shield Framework, including to:
            1. Verify prior to finalizing a company's self-certification that the company has provided all required information and registered with the identified independent recourse mechanism, in instances where the provider requires registration;
            2. Follow up with organizations whose self-certifications lapse or who have voluntarily withdrawn from the Privacy Shield Framework to verify whether the organization will return, delete or continue to apply the Principles to the

personal information that they received while they participated in the Privacy Shield Framework;

3. Search for and address false claims of participation and where appropriate refer matters to the FTC, Department of Transportation or other appropriate enforcement agency; and
4. Conduct periodic ex officio compliance reviews and assessments of the program.

i. The Department of Commerce has committed to increase cooperation with EU DPAs, including to:
    i. Establish a dedicated point of contact at the Department to act as a liaison with DPAs and receive and undertake best efforts to facilitate resolution of complaints referred;
    ii. Assist DPAs seeking information related to specific organization's participation in the program or implementation of specific Privacy Shield requirements; and
    iii. Provide DPAs with material regarding the Privacy Shield Framework for inclusion on their own websites to increase transparency for EU citizens and EU businesses.
j. The FTC has committed to increase cooperation with EU DPAs, including to:
    i. Establish a dedicated point of contact at the FTC and standardized process through which EU DPAs can refer complaints;
    ii. Exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions; and
    iii. Work closely with EU DPAs to provide enforcement assistance.
k. The Department of Commerce, the FTC and other agencies as appropriate will hold annual meetings with the Commission, interested DPAs and appropriate representatives from the Article 29 Working Party, where the Department will discuss current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield Framework.

2. Key new requirements for participating companies:
    a. Informing individuals about data processing
        i. Privacy Shield participant must include in its privacy policy a declaration of the organization's commitment to comply with the Privacy Shield Principles, so that the commitment becomes enforceable under U.S. law.
        ii. When a participant's privacy policy is available online, it must include a link to the Department of Commerce's Privacy Shield website and a link to the website or complaint submission form of the independent recourse mechanisms that is available to investigate individual complaints.
        iii. A participant must inform individuals of their rights to access their personal data, the requirement to disclose personal information in response to lawful request by public authorities, which enforcement authority has jurisdiction over the organization's compliance with the Framework, and the organization's liability in cases of onward transfer of data to third parties.
    b. Maintaining data integrity and purpose limitation
        i. Privacy Shield participants must limit personal information to the information relevant for the purposes of processing.
    c. Ensuring accountability for data transferred to third parties
        i. To transfer personal information to a third party acting as a controller, a Privacy Shield participant must:

1. Comply with the Notice and Choice Principles
2. Enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles.

ii. To transfer personal data to a third party acting as an agent, a Privacy Shield participant must:

1. Transfer such data only for limited and specified purposes;
2. Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles;
3. Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles;
4. Upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and
5. Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

3. Cooperating with the Department of Commerce
   a. Privacy Shield participants must respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield Framework.
   b. Transparency related to enforcement actions
   c. Privacy Shield participants must make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC if the organization becomes subject to an FTC or court order based on non-compliance.
4. Ensuring commitments are kept as long as data is held
   a. If an organization leaves the Privacy Shield Framework, it must annually certify its commitment to apply the Principles to information received under the Privacy Shield Framework if it chooses to keep such data or provide "adequate" protection for the information by another authorized means.
   b. Demonstration of limitations and safeguards on national security and law enforcement access to data:
      i. In connection with finalization of the new Privacy Shield Framework, the U.S. Intelligence Community has laid out in writing to the European Commission the multiple layers of constitutional, statutory, and policy safeguards that apply to its operations, with active oversight provided by all three branches of the U.S. Government.
      ii. The Department of Justice has provided an overview regarding limits on U.S. Government access to commercial data and other record information held by corporations in the United States for law enforcement and public interest purposes.
      iii. The Privacy Shield Framework provides, for the first time, a specific channel for EU individuals to raise questions regarding signals intelligence activities. The Department of State has committed to establish a new Ombudsperson through whom European Union individuals will be able to submit inquiries regarding the United States' signals intelligence practices. As a part of this process, the United States is making the

commitment to respond to appropriate requests regarding these matters, consistent with our national security obligations.

---

[1] For details of the case, please see: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf accessed 23 March 2016.

[2] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046

[3] These currently include Argentina, Canada, Israel, New Zealand and Uruguay.

[4] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf accessed 23 March 2016.

[5] https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework