EUROPEAN
COMMISSION

Brussels, 29.2.2016
COM(2016) 117 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Transatlantic Data Flows: Restoring Trust through Strong Safeguards

1. INTRODUCTION: THE ROLE OF PERSONAL DATA EXCHANGES IN THE EU-U.S. RELATIONSHIP

A solid transatlantic partnership between the European Union and the United States is as vital today as it has ever been. We share common values, pursue shared political and economic objectives, and cooperate closely in the fight against common threats to our security. The enduring strength of our relationship is evidenced by the extent of our commercial exchanges and our close cooperation in global affairs.

The transfer and exchange of personal data is an essential component underpinning the close links between the European Union (EU) and the United States (U.S.) in the commercial area as well as in the law enforcement sector. These data exchanges require a high level of data protection and corresponding safeguards.

In June 2013, reports concerning large-scale intelligence collection programmes in the U.S. raised serious concerns at both EU and Member State level about the impact on the fundamental rights of Europeans of large-scale processing of personal data by both public authorities and private companies in the United States.

In response, on 27 November 2013 the Commission issued a Communication on Rebuilding Trust in EU-U.S. Data Flows[1] setting out an action plan to restore trust in data transfers for the benefit of the digital economy, the protection of European individuals' rights, and the broader transatlantic relationship. The Communication set out the following key actions to achieve this objective:

(i) adopting the data protection reform package proposed by the Commission in 2012[2];

(ii) making the Safe Harbour safer on the basis of the 13 recommendations laid out in the Communication on the Safe Harbour[3]; and

(iii) strengthening data protection safeguards for law enforcement cooperation, notably by concluding negotiations on the EU-U.S. Data Protection Umbrella Agreement. The latter also included the objective of obtaining commitments from the U.S. on enforceable

---

1 Communication from the Commission to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final, 27.11.2013 (hereafter "the 2013 Communication" or "the Communication"), available at: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

2 Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012, and Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2012, available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

3 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27.11.2013, pp. 18-19 (hereafter "the Safe Harbour Communication"), available at: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

individual rights, including avenues for obtaining judicial redress, in particular through the enactment of a Judicial Redress Act extending certain rights enshrined in the 1974 U.S. Privacy Act to EU citizens that at the time were only available to U.S. citizens and permanent residents.

These objectives were reaffirmed in the political guidelines[4] of the Juncker Commission: "*Data protection is a fundamental right of particular importance in the digital age. In addition to swiftly finalising the legislative work on common data protection rules within the European Union, we also need to uphold this right in our external relations. In view of recent mass surveillance revelations, close partners such as the United States must convince us that the current safe harbour arrangements really are safe if they want them to continue. The U.S. must also guarantee that all EU citizens have the right to enforce data protection rights in U.S. courts, whether or not they reside on U.S. soil. This will be essential for restoring trust in transatlantic relations.*"

Since then, the Commission has worked to achieve these objectives. The Commission stepped up negotiations on the Umbrella Agreement which was initialled by the parties on 8 September 2015. The inter-institutional discussions on the data protection reform package were intensified, resulting in a political agreement between the Council and the European Parliament on 15 December 2015. As for transatlantic data transfers in the commercial sphere, the Commission began discussions with the U.S. to strengthen the Safe Harbour in January 2014. The invalidation of the Safe Harbour Decision by the Court of Justice in the *Schrems* ruling on 6 October 2015[5] confirmed the need for a renewed framework and provided further guidance on the conditions that the framework should fulfil. Following the ruling, on 6 November 2015 the Commission issued guidance for companies setting out the alternative tools that allow the continued transfer of personal data to the United States[6]. On 2 February 2016, a political agreement was reached on a new framework for transatlantic data flows, the EU-U.S. Privacy Shield[7], to replace the previous arrangement.

These achievements will benefit the transatlantic relationship and should restore Europeans' trust in the digital economy while strengthening their fundamental rights. They will also equip the EU and its Member States with a stronger data protection legal framework that will lead to closer integration of the internal market, in particular the Digital Single Market, as well as enable the EU to step up its efforts to promote and develop international privacy and personal data protection standards.

---

[4] A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change Political Guidelines for the next European Commission.

[5] Judgment of 6 October 2015 in Case C-362/14 Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:650.

[6] See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (*Schrems*), COM(2015) 566 final, 6.11.2015. See also the Statement of the Article 29 Working Party on the Consequences of the *Schrems* Judgment of 3 February 2016, available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[7] See http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en

In parallel, important initiatives were launched that led to significant changes in the U.S. legal order. On 17 January 2014, President Obama announced[8] reforms of U.S. signals intelligence activities which were subsequently laid down in Presidential Policy Directive 28 (PPD-28)[9]. Importantly, these reforms provided for the extension of certain privacy protections to non-Americans as well as a refocussing of data collection away from bulk collection towards an approach that prioritises targeted collection and access. The Commission welcomed those new orientations as an important step in the right direction[10]. This reform process was also instrumental in informing the discussions with the U.S. on the EU-U.S. Privacy Shield. Further changes have been introduced since then. For instance, in June 2015 the U.S. passed the USA Freedom Act[11] which modified certain U.S. surveillance programmes, strengthened judicial oversight and increased public transparency about their use. Finally, on 10 February 2016, the U.S. Congress passed the Judicial Redress Act which was signed into law by President Obama on 24 February 2016.[12]

It is against this background that the present Communication takes stock of how far we have come in realising the objectives formulated in the 2013 Communication. It will also highlight areas where more work is still required to cement and fully restore trust in transatlantic data flows.

2. THE EU DATA PROTECTION REFORM

2.1 The context

In order to seize the opportunities and address the challenges of an increasingly digital inter-connected world, the European Commission put forward its Data Protection Reform package ("the reform") in January 2012. By strengthening EU-internal rules and by providing individuals with more control over their personal data, the reform aims at fostering trust in the digital economy whether personal data is processed within one Member State, in the EU or in third countries, such as United States.

The reform package comprises two legal instruments, a General Data Protection Regulation[13] ("the Regulation") setting out a common EU framework for data protection, and a Data Protection Directive in the area of police and judicial cooperation ("the Police Directive")[14]. By proposing a regulation that will be directly applicable in the Member States, the Commission's aim was to establish one common data protection standard for all, thereby eliminating differences in the level of protection amongst Member States. Likewise, the Police Directive will for the first time lay down a common set of rules at EU level, while

[8] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
[9] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
[10] http://europa.eu/rapid/press-release_MEMO-14-30_en.htm
[11] USA FREEDOM Act of 2015, Pub. L., No. 114-23, § 401, 129 Stat. 268.
[12] H.R.1428 - Judicial Redress Act of 2015. It will enter into force 90 days after enactment.
[13] COM(2012) 11 final, 25.1.2012: see footnote 2.
[14] COM(2012) 10 final, 25.1.2012: see footnote 2.

taking account of the specificities of the judicial and law enforcement traditions in the Member States.

On 15 December 2015 the European Parliament and the Council reached a political agreement on the reform package, thereby fulfilling one of the key actions set out in the 2013 Communication.

2.2 What has changed?

The Regulation updates, modernises and in some cases strengthens the data protection principles enshrined in the 1995 Data Protection Directive[15] to guarantee privacy rights. It focuses on reinforcing individuals' rights, deepening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards. The rules are designed to make sure that EU individuals' personal data are protected – no matter where they are sent, processed or stored – even outside the EU, as may often be the case in the digital world. A number of features in the reform are particularly relevant to highlight.

First, **territorial scope:** the Regulation makes clear that it also applies to companies established in a third country if they are offering goods and services, or monitoring the behaviour of individuals, in the EU. Companies based outside of the EU will have to apply the same rules as companies based in the EU. This ensures the comprehensive protection of EU individuals' rights. It also creates a level-playing field between EU and foreign companies, thereby avoiding competitive imbalances between EU and foreign companies when operating in the EU or targeting consumers in the EU.

Second, **stronger enforcement** of data protection rules: the Regulation provides for an effective sanctions regime by harmonising the powers of national data protection supervisory authorities (DPAs). They will be empowered to impose fines reaching up to EUR 20 million or up to 4% of the total worldwide annual turnover of a company. This power to impose dissuasive sanctions for non-compliance with the data protection rules in conjunction with the territorial scope mentioned above will ensure that companies doing business in the EU will have every incentive to comply with EU law. The new rules also introduce a clearer and stricter liability regime for controllers and processors.

Third, **harmonised rules for law enforcement cooperation:** the Police Directive will apply general data protection principles and rules to the processing of personal data by police and judicial authorities in the Member States for criminal law enforcement matters. This includes harmonised rules for international transfers of personal data in the context of criminal law enforcement cooperation[16]. The new Directive will raise the level of protection for individuals

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.95, p. 31 ("the Data Protection Directive").

[16] Unlike under the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which only covers cross-border exchanges of data between Member States' competent authorities, the application of such rules under the Police Directive will no longer depend on whether those data have previously been exchanged between the criminal law enforcement authorities of the Member States.

while ensuring that the data of victims, witnesses, and suspects of crimes are duly protected in the context of a criminal investigation or a law enforcement action. Supervision is ensured by independent national data protection authorities and individuals must be afforded effective judicial remedies. At the same time, more harmonised laws will enable the police and judicial authorities to cooperate more effectively, amongst Member States as well as between Member States and their international partners, to combat crime and terrorism more effectively. This is a crucial part of the European Agenda on Security.[17]

Fourth, **strong rules for safer international transfers**: both the Regulation and the Police Directive provide transparent, detailed and comprehensive rules for personal data transfers to third countries. They cover all forms of international transfers, be they for commercial or law enforcement purposes, between private parties or public authorities, or between private entities and public authorities. While the architecture of the rules on international transfers remains essentially the same as under the current Data Protection Directive (i.e., adequacy decisions, standard contractual clauses and binding corporate rules, as well as certain derogations from the general prohibition to transfer personal data outside the EU), the reform clarifies and simplifies those rules in a number of ways while reducing red tape. It also introduces some new tools for international transfers.

The Regulation furthermore strengthens the **powers of EU data protection authorities**, including with respect to international transfers. Compared to the current Data Protection Directive, the provisions on the independence, functions and powers of EU DPAs are spelled out in more detail and substantially enhanced. This expressly includes the power to suspend data flows to a recipient in a third country or to an international organisation. The Police Directive contains similar provisions with regard to international transfers and the powers of DPAs over the law enforcement sector.

More specifically, as regards the rules on Commission **adequacy decisions**, the Regulation provides for a precise and detailed catalogue of elements that the Commission must take into account when assessing the level of data protection provided in the legal order of a third country. This process consists of a comprehensive assessment that the Commission must undertake and which should cover – an element that is also in line with the *Schrems* ruling – rules governing the access by the public authorities of a third country to personal data. Another crucial feature of this assessment is that individuals are provided with effective and enforceable data protection rights and may obtain effective administrative and judicial redress.

Furthermore, the Regulation expressly requires the Commission to **periodically review**, at least every four years, all of its adequacy decisions in order to keep abreast of all relevant developments in a third country that may have a direct, or indeed adverse, impact on the level of protection in its legal order. This continuous monitoring of adequacy will be a more

[17] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM(2015) 185 final, 28.4.2015.

dynamic process as it will also entail a dialogue with the authorities of the third country in question.

As regards transfers to third countries for which there is no adequacy decision, the Regulation provides the conditions governing the use of **alternative transfer tools** such as standard contractual clauses and binding corporate rules. It also adds other instruments for transfers, such as approved codes of conduct and approved certification mechanisms. Finally, it clarifies the situation when **derogations** can be used.

2.3 The way forward

The data protection reform is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. Consumer trust in EU and third country operators will fuel and thus benefit the European and global digital economy. It will impact positively on our commercial relations with the U.S., our biggest trading partner. It will bring clarity and a stable environment for EU and foreign businesses to operate in. For their part, U.S. businesses will benefit from the legal certainty that comes from doing business with an integrated economic area that applies a uniform set of data protection rules.

Common rules in the law enforcement sector will ensure that individuals' data are better protected and that they are entitled to effective judicial remedies. Facilitating cross-border cooperation amongst police and judicial authorities in the Member States will increase the efficiency of criminal law enforcement and thus create conditions for more effective crime prevention in the EU. At the same time this will enable smoother cooperation with their counterparts in third countries.

The formal adoption of the reform package by the European Parliament and Council is expected to take place during the first semester of 2016. The Regulation will apply two years after adoption while the Police Directive provides for a two-year implementation period. The two-year transition period should be used by all concerned stakeholders both inside and outside the EU to prepare for the new rules. The Commission will play its part. During this transition period, the Commission will work closely with Member States, DPAs and other interested parties to ensure a uniform application of the rules and promote a compliance-ready environment.

3. THE EU-U.S. PRIVACY SHIELD: A NEW TRANSATLANTIC FRAMEWORK FOR PERSONAL DATA FLOWS

3.1 The context

In order to facilitate personal data flows between the EU and the U.S. for commercial exchanges while ensuring the protection of those data, the Commission had, back in 2000, recognised the Safe Harbour framework as providing an adequate level of protection[18]. As a

[18] Commission Decision 2000/520/EC of 20 July 2000. In this decision, based on Article 25(6) of the Data Protection Directive, the Commission had recognised the Safe Harbour Privacy Principles and accompanying

result, despite the absence of a general data protection law in the U.S., personal data could be freely transferred from EU Member States to companies in the U.S. that had signed up to the privacy principles underpinning the framework.

In the 2013 Safe Harbour Communication[19], the Commission pointed to a number of weaknesses in the functioning of the arrangement over time, notably a lack of transparency by companies concerning their adherence to the scheme and a lack of effective enforcement by U.S. authorities of those companies' compliance with the scheme's privacy principles. Moreover, the surveillance revelations earlier that year raised concerns as regards the scale and scope of certain U.S. intelligence programmes and the level of access by U.S. public authorities to Europeans' personal data transferred under the Safe Harbour. Taking these and other elements[20] into consideration, the Commission concluded that the Safe Harbour had to be reviewed. Against this background, the Commission formulated 13 recommendations[21] to strengthen and update the data protection guarantees built into the framework. These recommendations focused on: (i) strengthening the substantive privacy principles and increasing the transparency of U.S. self-certified companies' privacy policies incorporating these principles; (ii) better and effective supervision, monitoring and enforcement by the U.S. authorities of companies' compliance with the principles; (iii) the availability of affordable dispute resolution mechanisms for individual complaints; and (iv) the need to ensure that the use of the national security and law enforcement exception provided in the 2000 Safe Harbour Decision would be limited to what is strictly necessary and proportionate.

On the basis of these 13 recommendations, the Commission entered into discussions with the U.S. authorities in January 2014. The subsequent invalidation of the Safe Harbour Decision on 6 October 2015 by the Court of Justice confirmed the need for a stronger and new framework for transatlantic commercial data flows. While the Court's ruling draws on the Commission's 2013 recommendations, it further underscores the need to have limitations, safeguards and judicial control mechanisms in place in order to ensure the continued protection of the personal data of EU individuals, including when the data are accessed and used by public authorities for national security, public interest or law enforcement purposes.

On 2 February 2016, after two years of intensive discussions, the EU and the U.S. reached a political agreement on the new framework, the EU-U.S. Privacy Shield. This new arrangement comprises important new safeguards and will guarantee a high level of protection of the fundamental rights of EU individuals. It will provide the necessary legal certainty for companies on both sides of the Atlantic that want to do business together. And it will inject a new momentum into the transatlantic partnership.

Frequently Asked Questions issued by the U.S. Department of Commerce as providing adequate protection for the purposes of personal data transfers from the EU. The functioning of the Safe Harbour arrangement relied on commitments and self-certification of adhering companies. The rules were binding under U.S. law for those entities and enforceable by the U.S. Federal Trade Commission.

[19] See footnote 3.

[20] These elements included the exponential increase in data flows and their critical importance for the transatlantic economy as well as the rapid growth of the number of U.S. companies adhering to the Safe Harbour scheme. See the Safe Harbour Communication, p. 37.

[21] Safe Harbour Communication, pp. 18-19.

Following conclusion of the negotiations with the U.S., the Commission will submit the new arrangement to the "Article 29 Working Party" (comprising the EU DPAs) for an opinion on the level of protection provided. Furthermore, the adequacy decision will go through the comitology procedure before it can be adopted. The European Data Protection Supervisor will also be consulted.

3.2 What has changed?

The EU-U.S. Privacy Shield provides a robust and effective response to both the Commission's 13 recommendations and the *Schrems* ruling. It contains a number of important improvements, compared to the previous framework, with respect to the commitments that must be undertaken by U.S. companies. It also contains important new commitments and detailed explanations of relevant U.S. laws and practice by U.S. authorities. Unlike its predecessor, the Privacy Shield covers not only commitments in the commercial sector but also, significantly and for the first time in EU-U.S. relations, in the area of access to personal data by public authorities including for national security purposes. This is a crucial and necessary element in light of the Court jurisprudence to restore trust in transatlantic relations following the surveillance revelations.

The most important achievements of this new arrangement can be grouped into four main categories:

First, **strong obligations on companies and robust enforcement**: the new arrangement will be more transparent and contain effective supervision mechanisms to ensure that companies follow the rules they have legally committed to uphold. U.S. companies wishing to import personal data from Europe under the Privacy Shield will need to accept robust obligations on how personal data is processed and individual rights are guaranteed. This includes tightened conditions and stricter liability provisions for Privacy Shield companies that transfer EU data, for instance for sub-processing activities, to third parties outside the framework, whether in the U.S. or in other third countries ("onward transfers"). As for supervision, the U.S. Department of Commerce has committed to a regular and rigorous monitoring of how companies comply with their commitments and to weed out "free-riders", i.e. companies that falsely claim adherence to the scheme. Companies' commitments are legally binding and enforceable under U.S. law by the Federal Trade Commission and companies that do not comply will be faced with severe sanctions.

Second, **clear limits and safeguards with respect to U.S. government access**: for the first time, the U.S. government, through the Department of Justice and the Office of the Director of National Intelligence as the body overseeing the entire U.S. intelligence community, has provided the EU with written representations and assurances that access by public authorities for law enforcement, national security and other public interest purposes will be subject to clear limitations, safeguards and oversight mechanisms. The U.S. will also establish a new redress mechanism for EU data subjects in the area of national security through an Ombudsperson who will be independent from the national security authorities. The Ombudsperson will be tasked with following-up complaints and enquiries by EU individuals into national security access and will have to confirm to the individual that the relevant laws

have been complied with or that any non-compliance has been remedied. This is a significant development that will apply not only to Privacy Shield transfers but to *all* personal data transferred to the U.S. for commercial purposes, irrespective of the basis used to transfer those data.

Third, **effective protection of EU individuals' privacy rights with several redress possibilities**: anyone in Europe who considers that his or her data have been misused under the new arrangement will benefit from several accessible and affordable avenues to obtain individual redress, including cost-free alternative dispute resolution bodies. Companies commit to reply to complaints within a fixed deadline. In addition, any company handling human resources data from Europe has to commit to comply with the decisions of the competent EU DPA while other companies may voluntarily make such a commitment. Individuals can also take their complaint to their 'home' DPA that will be offered a formalized procedure to refer complaints to the Department of Commerce and the Federal Trade Commission to facilitate the investigation and resolution of the respective claim within a reasonable timeframe. If a case is nevertheless not resolved by any of these avenues, individuals will be able to have recourse, as a last resort, to the Privacy Shield Panel, a dispute resolution mechanism that can take binding and enforceable decisions against U.S. Privacy Shield companies. Additionally, EU DPAs will be able to provide assistance to individuals to prepare their case. As mentioned above, for complaints on possible access by national intelligence authorities a new Ombudsperson will be created, providing a further avenue for redress.

Fourth and finally, an **annual joint review mechanism:** this will allow the Commission to regularly monitor the functioning of all aspects of the Privacy Shield, including the limitations and safeguards relating to national security access. The Commission and the U.S. Department of Commerce will carry out the review and involve EU data protection authorities and U.S. national security authorities and the Ombudsperson. In this way, the U.S. will be held accountable to its commitments. But the Commission will not stop there: it will also draw on all other sources of information available, including voluntary transparency reports by companies on the degree of government access requests[22]. The annual review goes beyond the new Regulation, which requires such reviews only at least every four years, thus demonstrating the resolve of both the EU and the U.S. to rigorously ensure full compliance.

This review will not be a formalistic exercise without consequences. In cases where the U.S. companies or public authorities are not abiding by their commitments, the Commission will activate the process to suspend the Privacy Shield. As the Court of Justice has stressed in the *Schrems* ruling, an adequacy decision must not be a dead letter; rather, U.S. companies and authorities have to breathe life into the framework and continuously sustain it by living up to their commitments. Where they fail to do so, the particular benefit for data transfers deriving from an adequacy finding is no longer justified and will be withdrawn.

[22] Major U.S. internet companies already produce such reports in order to regain the trust of their customers. The 2015 USA FREEDOM Act allows the publication of voluntary reports on access requests, at least within certain bands to protect national security interests.

3.3 The way forward

The commitments agreed by the U.S. under the Privacy Shield will provide the basis for, and be reflected in, a new Commission adequacy decision. Companies are encouraged to already begin their preparations so as to be in a position to join the new framework as soon as possible after it is in place following the adoption of the Commission decision. For its part, the U.S. government will publish its representations in the U.S. Federal Register, thereby publicly attesting to uphold its commitments.

The EU-U.S. Privacy Shield requires action from many actors:

- the participating U.S. companies that must fulfil their obligations under the framework in the full knowledge that it will be strictly enforced and they will be sanctioned if they are non-compliant. To strengthen trust with their consumers, companies are also encouraged to opt for EU DPAs as their chosen avenue to resolve complaints under the Privacy Shield, as European individuals are most likely to turn to these authorities. Similarly, the extent to which companies are prepared to utilise the possibility provided under U.S. law to publish transparency reports on national security and law enforcement access requests concerning EU data they receive will contribute to maintaining confidence that such access is limited to what is necessary and proportionate[23];

- the various U.S. authorities entrusted with overseeing and enforcing the framework, respecting the limitations and safeguards as far as access to data for law enforcement and national security purposes is concerned, and those entrusted with responding in a timely and meaningful manner to complaints by EU individuals about the possible misuse of their personal data;

- the EU DPAs that have an important role to play in ensuring that individuals can effectively exercise their rights under the Privacy Shield, including by channelling their complaints to the appropriate U.S. authorities and cooperate with the latter, triggering the Ombudsperson mechanism, assisting complainants in bringing their case to the Privacy Shield Panel, as well as exercising oversight over human resources data transfers; and

- the Commission that is responsible for making a finding of adequacy and reviewing it on a regular basis: these regular reviews mark a significant departure from the previous static situation by transforming the Privacy Shield adequacy finding into a closely monitored, living framework.

The annual joint review and the ensuing Commission report – as well as the prospect of suspending the arrangement in case of non-compliance – will thus play a central role in ensuring that the Privacy Shield will endure the test of time. Our mutual transatlantic ambition

[23] Such reporting would be made in accordance with the provisions in the 2015 USA FREEDOM Act. See footnote 22.

should be to develop together a strong culture of privacy compliance and protection of individual rights that restores and maintains trust.

4. THE UMBRELLA AGREEMENT: STRENGTHENING DATA PROTECTION SAFEGUARDS FOR LAW ENFORCEMENT COOPERATION

4.1 The context

An important dimension of our transatlantic relationship is the capacity for the EU, the Member States and the U.S. to respond effectively to common security threats and challenges in a cooperative and coordinated way. This collective response significantly relies on our ability to exchange personal data in the framework of police and judicial cooperation in criminal matters. A number of bilateral agreements between the Member States and the U.S. as well as between the EU and the U.S.[24] were concluded over time in pursuit of this aim. At the same time, it is equally important for these law enforcement agreements to provide effective data protection safeguards. The two-fold objective of working successfully with our U.S. partners to combat serious crime and terrorism while advancing the level of protection of Europeans in line with their fundamental rights and the EU data protection rules when transfers are made for those purposes, triggered the negotiations, launched in March 2011, on an international data protection agreement in the area of law enforcement, the EU-U.S. Data Protection "Umbrella Agreement"[25].

The EU and the U.S. finalised their negotiations in the summer of 2015. The two parties initialled the Umbrella Agreement on 8 September 2015 in Luxembourg[26], and the agreement is now waiting for its ratification on both sides of the Atlantic. The signing of the Umbrella Agreement was, however, conditional on the passage of the Judicial Redress Act by the U.S. Congress to provide, for the first time, equal treatment of EU citizens with US citizens under the 1974 U.S. Privacy Act[27]. The bill was approved by Congress on 10 February 2016 and was signed into law on 24 February 2016.

4.2 What has changed?

The Umbrella Agreement will enshrine, for the very first time, a harmonised and comprehensive set of data protection safeguards that will apply to all transatlantic exchanges between the relevant authorities in the area of criminal law enforcement. It is in effect a

[24] Notably, the EU-US Passenger Name Record (PNR) Agreement and the EU-US Terrorist Financing and Tracking Programme (TFTP).

[25] An agreement between the EU and the U.S. on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters.

[26] http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

[27] The Judicial Redress Act grants rights to citizens of "covered countries"', designated by the U.S. Government. This is in turn conditional on the following criteria: (a) the country [or regional organisation] has an agreement with the United States on privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses: (b) the country or [regional organization] permits the transfer of personal data for commercial purposes between it and the United States; and (c) the policies regarding the transfer of personal data for commercial purposes and related actions of the country or regional organization, do not materially impede the national security interests of the United States.

fundamental rights agreement setting a high-level standard of protection against which all data exchanges in existing and future agreements must be measured.

First, **the protections and safeguards provided by the Umbrella Agreement will horizontally apply to all data exchanges taking place in the context of transatlantic law enforcement co-operation in criminal matters**. This includes transfers on the basis of domestic laws, EU-US agreements, Member States-U.S. agreements (e.g. Mutual Legal Assistance Treaties) as well as specific agreements providing for the transfer of personal data by private entities for law enforcement purposes. The agreed provisions will thus immediately increase the level of protection guaranteed to EU data subjects when data is transferred to the U.S. It will also increase legal certainty for transatlantic law enforcement cooperation by ensuring that exiting agreements contain all necessary protections and can thus withstand possible legal challenges.

Second, the provisions cover all the core EU data protection rules in terms of **processing standards** (e.g. data quality and integrity, data security, accountability and oversight), **safeguards and limitations** (e.g. purpose and use limitations, data retention, onward transfers, processing of sensitive data) as well as **individual rights** (access, rectification, administrative and judicial redress).

Third, the agreement will ensure the availability of **judicial redress rights for denial of access, denial of rectification and unlawful disclosure**. This constitutes a major improvement and will significantly contribute to restoring trust in transatlantic exchanges. This key and long-sought for EU demand, which had remained unanswered for many years, has already been reflected in the Judicial Redress Act introduced in the U.S. Congress in March 2015 and passed on 10 February 2016. This Act will extend to EU citizens[28] three core judicial redress avenues under the 1974 U.S. Privacy Act that are currently reserved only to U.S. citizens and permanent residents. Thus, for the first time, EU citizens will be able to avail themselves of rights of general application for any transatlantic transfer of data in the criminal law enforcement sector. This removes a critical difference in treatment between EU and U.S. citizens.

Fourth, the Umbrella Agreement generalises and expands to the whole law enforcement sector the principle of **independent oversight** as a core data protection requirement, one that is not present in many of the existing bilateral agreements. This includes effective powers to investigate and resolve individual complaints as regards compliance with the Agreement.

Fifth, the effective implementation of the Umbrella Agreement will be subject to **periodic joint reviews**. Particular attention will be given in these reviews to the provisions relating to individuals' rights (access, rectification, administrative and judicial redress).

The Umbrella Agreement does not in itself authorise data transfers, nor does it constitute an adequacy decision.

[28] According to the Judicial Redress Act, other non-EU countries or "regional economic integration organisations" may equally be designated as "covered countries" with the effect that judicial redress rights would benefit their citizens.

4.3 The way forward

The entry into force of the Judicial Redress Act[29] will pave the way to the signing of the Umbrella Agreement. The Commission will shortly submit to the Council a proposal for a decision authorising the signing of the Umbrella Agreement. After signature, the decision concluding the Agreement will have to be adopted by the Council after obtaining the consent of the European Parliament. The Umbrella Agreement will significantly improve the present day situation which is characterised by fragmented, non-harmonised and often weak data protection rules in a patchwork of multilateral, bilateral, national and sectorial instruments. The Umbrella Agreement has a retrospective function in that it will supplement the data protection guarantees in current agreements when and to the extent these lack the requisite level of safeguards. In this respect, it will bring significant added value by essentially "filling in the gaps" of existing agreements which contain lower data protection standards than those found in the Umbrella Agreement. This will enable continuity in law enforcement cooperation while ensuring greater legal certainty when transfers are made. As regards future agreements, the Umbrella Agreement will represent a safety net below which the level of protection cannot fall. This is a very important guarantee for the future and a major shift from the present situation where safeguards, protections and rights have to be negotiated afresh for each individual new agreement. The Umbrella Agreement is thus a template containing the standard safeguards which cannot be negotiated downwards. This is a very important precedent not only for EU-U.S. relations but, more generally, for any future data protection or data exchange arrangement at international level.

Negotiated in parallel with the reform, the Umbrella Agreement is aligned with the EU's data protection acquis. The interaction between the Umbrella Agreement and the Police Directive is particularly relevant given the importance of having a high and common level of data protection, regardless of whether the personal data is processed at national level or exchanged across borders within the EU or with third countries. In this respect, the Umbrella Agreement will help to substantiate the general requirements of the reform in the transatlantic context.

Concluding negotiations on the Umbrella Agreement which sets common standards in a complex area of law and policy is a significant achievement. The future Umbrella Agreement will restore and reinforce trust, provide guarantees of lawfulness for data transfers and facilitate EU-U.S. cooperation in this field.

Going forward, there is a need to jointly address common challenges in the area of police and judicial cooperation. One important open issue is the question of direct access by law enforcement authorities to personal data held by private companies abroad. Such access should, in principle, take place in the framework of formal channels of co-operation, such as Mutual Legal Assistance (MLA) agreements or other sectorial agreements. Private companies currently risk facing legal uncertainty which could impact on their capacity to operate across different jurisdictions when asked to provide access to electronic evidence under the laws of one country for personal data subject to the laws of another. In parallel to the upcoming

[29] The Judicial Redress Act enters into force 90 days after its enactment.

review of the EU-U.S. MLA Agreement[30], the EU would welcome further exchanges with the U.S. on this matter, including addressing the development of common and more effective rules to collect electronic evidence.

5. CONCLUSION

The successful conclusion of the key actions outlined in the 2013 Communication demonstrates the EU's capacity to solve problems in a pragmatic and focused manner without sacrificing its strong fundamental rights values and traditions. It also demonstrates that the EU and the U.S. are able to resolve their differences and take difficult decisions in order to preserve a strategic relationship that has withstood the test of time. At the same time, as we turn a new chapter in our bilateral relations, the time for vigilance is not over as we continue to face common threats and challenges in an uncertain world.

Once the Privacy Shield and the Umbrella Agreement are in place, it is incumbent on both parties to ensure that these two important data transfer frameworks work effectively and in an enduring manner. Their success depends in large part on effective enforcement and the respect of the rights accorded to individuals. It also depends on the continual assessment of their functioning; this requires a shift in mind-set from a static to a more dynamic process.

Against this background, an important element of this process relates to the ongoing reform of U.S. intelligence programmes. In this respect, the Commission will follow closely the upcoming reports prepared by the Privacy and Civil Liberties Oversight Board (PCLOB) and the review of the Section 702 FISA programme relating to foreign surveillance due in 2017. In particular further reforms relating to transparency, oversight, and the extension of safeguards to non-U.S. persons will be followed closely.

More generally, given the significance of cross border data flows for transatlantic trade, the EU will follow closely further legislative progress on the U.S. side in the area of privacy. Now that Europe has equipped itself with a single, coherent and robust set of rules, we hope that the U.S. will also continue to pursue efforts towards a comprehensive system of privacy and data protection. It is through such a comprehensive approach that convergence between the two systems could be achieved in the longer term. In this respect, the Commission will hold an annual privacy summit with interested NGOs and other concerned stakeholders on both sides of the Atlantic.

The EU-U.S. partnership can be a driving force to develop and promote international legal standards for the protection of privacy and personal data. Initiatives at UN level, including the work of the Special Rapporteur on the Right to Privacy, can also play an important role in this regard. In the coming years, given the increasing centrality of these issues on the global stage, the EU and the U.S. should seize this opportunity to advance their common values of individual freedoms and rights in the globalised digital world.

[30] Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11.2009, p. 40-41.

European Commission - Fact Sheet

EU-U.S. Privacy Shield: Frequently Asked Questions

Brussels, 29 February 2016

What is the EU-US Privacy Shield?

After two years of negotiations, the European Commission and the U.S. Department of Commerce reached on 2 February 2016 a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield (IP/16/216). This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses.

The EU-U.S. Privacy Shield reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.

The new arrangement will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities. The new arrangement includes written commitments and assurance by the U.S. that any access by public authorities to personal data transferred under the new arrangement on national security grounds will be subject to clear conditions, limitations and oversight, preventing generalised access. The newly created Ombudsperson mechanism will handle and solve complaints or enquiries raised by EU individuals in this context.

What is an adequacy decision?

An "adequacy decision" is a decision adopted by the European Commission, which establishes that a non-EU country ensures an adequate level of protection of personal data by reason of its domestic law and international commitments.

The effect of such a decision is that personal data can flow from the 28 EU Member States (and the three European Economic Area member countries: Norway, Liechtenstein and Iceland) to that third country, without any further restrictions.

The EU-U.S. Privacy Shield framework ensures an adequate level of protection for personal data transferred to the U.S. The EU-US Privacy Shield consists of Privacy Principles that companies must abide by and commitments on how the arrangement will be enforced (written commitments and assurance by the State Secretary John Kerry, Commerce Secretary Penny Pritzker, the Federal Trade Commission and the Office of the Director of National Intelligence, amongst others).

What are the main differences between the old "Safe Harbour" arrangement and the new EU-U.S. Privacy Shield?

The EU-U.S. Privacy Shield addresses both the recommendations made by the Commission in November 2013 and the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.

The new arrangement provides **stronger obligations on companies** in the U.S. to protect the personal data of Europeans. It requires stronger monitoring and enforcement by the U.S. Department of Commerce (DoC) and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities.

The new arrangement includes commitments and assurance by the US that the competencies under US law for public authorities to access personal data transferred under the new arrangement will be subject to **clear conditions, limitations and oversight**, preventing generalised access. The newly created Ombudsperson mechanism will handle and solve complaints or enquiries raised by EU individuals in relation to possible access by national intelligence services.

The new agreement will include:

- **Strong obligations on companies and robust enforcement:** the new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies respect their obligations, including sanctions or exclusion if they do not comply. The new rules also include tightened conditions for onward transfers to other partners by the companies participating in the

scheme.

- **Clear safeguards and transparency obligations on U.S. government access:** for the first time, the U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. US Secretary of State John Kerry committed to establishing a **redress possibility** in the area of national intelligence for Europeans through an **Ombudsman mechanism** within the Department of State, who will be **independent** from national security services. The Ombudsman will follow-up complaints and enquiries by individuals and inform them whether the relevant laws have been complied with. All the written commitments will be published in the U.S. federal register.

- **Effective protection of EU citizens' rights with several redress possibilities: Complaints have to be resolved by companies within 45 days. A free of charge Alternative Dispute Resolution solution will be available. EU citizens can also go to their national Data Protection Authorities, who will work with the U.S. Department of Commerce and Federal Trade Commission to ensure that unresolved complaints by EU citizens are investigated and resolved**. If a case is not resolved by any of the other means, as a last resort there will be an enforceable arbitration mechanism. Moreover, companies can commit to comply with advice from European DPAs. This is obligatory for companies handling human resource data.

- **Annual joint review mechanism:** that will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available, including transparency reports by companies on the extent of government access requests. The Commission will also hold an annual privacy summit with interested NGOs and stakeholders to discuss broader developments in the area of U.S. privacy law and their impact on Europeans. On the basis of the annual review, the Commission will issue a public report to the European Parliament and the Council.

How are the requirements of the ECJ ruling satisfied?

- **Regular review of adequacy decisions**

The new arrangement will be transparent and contain **effective supervision mechanisms** to ensure that companies follow the rules they submitted themselves to.

The EU and the US have now agreed to establish a new mechanism to monitor the functioning of the Safe Harbour through an **annual joint review**.

The Commission and the Department of Commerce will carry out **this review,** which will serve to **substantiate the commitments** made. The joint review would involve, as appropriate, representatives of the US intelligence community and will provide a dynamic and ongoing process to ensure that the Privacy Shield is functioning in accordance with the principles and commitments made.

The US has committed to **stronger oversight** by the Department of Commerce, **stronger cooperation** between European Data Protection Authorities and the Federal Trade Commission. This will transform the system from a self-regulating one to an oversight system that is more responsive as well as proactive.

The Department of Commerce will monitor the compliance of companies with the Privacy Shield principles on an ongoing basis of companies, including through detailed questionnaires. These reviews will take place when the Department of Commerce receives specific complaints, when a company does not provide satisfactory responses, or when there is credible evidence suggesting that a company may not be complying with the Privacy Shield Principles. If companies do not comply in practice they face sanctions and removal from the list.

- **Limitations for access to personal data for national security purposes**

The U.S. authorities set out the safeguards and limitation and oversight mechanism in place for any access to data by public authorities for national security purposes. The U.S. affirms that there is no indiscriminate or mass surveillance. For complaints on possible access by national intelligence authorities, a new Ombudsperson mechanism will be set up, independent from the intelligence services.

- **All individual complaints will be handled and resolved**

There will be a number of ways to address complaints, starting with dispute resolution by the company and free of charge alternative dispute resolution solutions. Citizens can also go to the Data protection authorities who will work together with the U.S. Department of Commerce and Federal Trade

Commission to ensure that complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Redress possibility in the area of national security for EU citizens' will be handled by an Ombudsman independent from the US intelligence services.

How will the Privacy Shield work concretely?

American companies will register to be on the Privacy Shield List and **self-certify** that they meet the requirements set out. This procedure has to be done each year.

The US Department of Commerce will have **to monitor and actively verify** that companies' privacy policies are presented in line with the relevant Privacy Shield principles and are readily available.

The US has committed to maintaining an **updated list of current Privacy Shield members** and removing those companies that have left the arrangement. The Department of Commerce will ensure that companies that are no longer members of Privacy Shield must still **continue to apply** its principles to personal data received when they were in the Privacy Shield, for as long as they continue to retain them.

How can Europeans obtain redress in the US if their data is misused by commercial companies?

Any citizen who considers that their data has been misused will have several redress possibilities, under the new arrangement:

- **Lodge a complaint with the company itself:**Companies commit to reply to complaints within 45 days. In addition, any company handling human resources data from Europeans has to commit to comply with advice by the competent EU Data Protection Authority (DPA), while other companies may voluntarily make such a commitment. The Commission encourages companies to do so.
- **Take their complaint to their 'home' DPA:** The DPA will refer the complaint to the Department of Commerce, who will respond within 90 days, or the Federal Trade Commission, if the Department of Commerce is unable to resolve the matter.
- **Use the Alternative Dispute Resolution,** a free of charge tool to which US companies must sign up if they want to be Privacy Shield-certified. The companies will be required to include information in their published privacy policies about the independent dispute resolution body where consumers can address their complaints. They must provide a link to the website of their chosen dispute resolution provider and the Department of Commerce will verify that companies have implemented this obligation.
- If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Individuals will be able to have recourse to the **Privacy Shield Panel**, a dispute resolution mechanism that can take binding decisions against U.S. self-certified companies. It ensures that every single complaint is being dealt with and that the individual obtains a remedy.

What changes have been made in the U.S. since the Snowden revelations?

The U.S. Government and Congress launched important surveillance reforms in response to the Snowden revelations.

In January 2014, President Obama issued Presidential Policy Directive 28 (PPD-28), which imposes important limitations for intelligence operations. It specifies that data collection by the intelligence services should be targeted. Additionally, the PPD-28 limits the use of bulk collection of data to six national security purposes (detect and counter threats from espionage, terrorism, weapons of mass destruction, threats to the Armed Forces,or transnational criminal threats) to better protect privacy of all persons, including non-U.S citizens.

Since 2015, the USA Freedom Act also limits bulk collection of data and allows companies to issue transparency reports on the approximate number of government access requests.

The Commission will follow with interest the upcoming reports of the Privacy and Civil Liberties Oversight Board assessing the implementation of the PPD-28, as well as the review of the Section 702 FISA Programme relating to foreign surveillance due in 2017.

What are the guarantees regarding the national security access to data transferred to the US?

For the first time, the US has given the EU written assurance, to be published in the federal register, that the access of public authorities for law enforcement and national security purposes will be subject to **clear limitations, safeguards and oversight mechanisms**. The US assures there is no **indiscriminate or mass surveillance** on the personal data transferred to the US under the new arrangement. To regularly monitor the functioning of the arrangement and the commitments made, there will be an **annual joint review**, which will also include the issue of national security access. The

European Commission and the US Department of Commerce will conduct the review and invite national intelligence experts from the US and European Data Protection Authorities to it.

What will be the role of the Ombudsperson mechanism?

The possibility for redress in the area of national security for EU citizens' will be handled by an **Ombudsperson,** independent from the US intelligence services. This is a new mechanism introduced by the Privacy Shield arrangement.

The Ombudsperson mechanism will deal with individual complaints from Europeans if they fear that their personal information has been used in an unlawful way by US authorities in the area of national security. This redress mechanism will inform the complainant whether the matter has been properly investigated and that either US law has been complied with or, in case of non-compliance, this has been remedied.

What is the role of Judicial Redress Act?

The **Judicial Redress Act** was signed by President Obama on 24 February. Once in force, it will give EU citizens access to U.S. courts to enforce privacy rights in relation to personal data transferred to the U.S. for law enforcement purposes. The Judicial Redress Act will extend the rights US citizens and residents enjoy under the 1974 Privacy Act also to EU citizens. This is a long-standing demand of the EU.

What is the EU-US data protection "Umbrella Agreement"?

The EU-US data protection "Umbrella Agreement" puts in place a comprehensive high-level data protection framework for EU-US law enforcement cooperation. The Agreement covers all personal data (for example names, addresses, criminal records) exchanged between the EU and the U.S. for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism.

The Umbrella Agreement is not in itself a legal basis for data transfer nor an adequacy decision. It will provide safeguards and guarantees of lawfulness for data transfers made under different agreements. This will ensure that fundamental rights are fully respected, while facilitating EU-U.S. law enforcement cooperation and restoring trust.

With the signature of the Judicial Redress Act by President Obama on 24 February, EU citizens will soon benefit from equal treatment: they will have the same judicial redress rights as US citizens in case of privacy breaches. This point was outlined by President Juncker in his political guidelines, when he stated: " *The United States must [...] guarantee that all EU citizens have the right to enforce data protection rights in U.S. courts, whether or not they reside on U.S. soil. Removing such discrimination will be essential for restoring trust in transatlantic relations*"

For more information

See IP/16/433

MEMO/16/434

Press contacts:

Melanie VOIN (+ 32 2 295 86 59)
Christian WIGAND (+32 2 296 22 53)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

European Commission

February 2016

EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield imposes **stronger obligations on U.S. companies** to protect Europeans' personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbour framework invalid. The Privacy Shield requires the U.S. to **monitor and enforce more robustly**, and cooperate more with European Data Protection Authorities.

It includes, for the first time, written commitments and assurance regarding **access to data by public authorities**.

The new arrangement will include the following elements:

Commercial sector

Strong obligations on companies and robust enforcement:

> Greater transparency.

> Oversight mechanisms to ensure companies abide by the rules.

> Sanctions or exclusion of companies if they do not comply.

> Tightened conditions for onward transfers.

Redress

Several redress possibilities:

> **Directly with the company:** Companies must reply to complaints from individuals within 45 days.

> **Alternative Dispute Resolution:** free of charge.

> **With the Data Protection Authority:** they will work with U.S. Department of Commerce and Federal Trade Commission to ensure unresolved complaints by EU citizens are investigated and swiftly resolved.

> **Privacy Shield Panel:** As a last resort, there will be an arbitration mechanism to ensure an enforceable decision.

U.S. Government access

Clear safeguards and transparency obligations:

> For the first time, written assurance from the U.S. that any access of public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms.

> U.S authorities affirm absence of indiscriminate or mass surveillance.

> Companies will be able to report approximate number of access requests.

> New redress possibility through EU-U.S. Privacy Shield Ombudsperson mechanism, independent from the intelligence community, handling and solving complaints from individuals.

Monitoring

Annual joint review mechanism:

> Monitoring the functioning of the Privacy Shield and U.S. commitments, including as regards access to data for law enforcement and national security purposes.

> Conducted by the European Commission and the U.S. Department of Commerce, associating national intelligence experts from the U.S. and European Data Protection Authorities.

> Annual privacy summit with NGOs and stakeholders on developments in the area of U.S. privacy law and its impact on Europeans.

> Public report by the European Commission to the European Parliament and the Council, based on the annual joint review and other relevant sources of information (e.g. transparency reports by companies).

What will it mean in practice?

For American companies

> Self-certify annually that they meet the requirements.

> Display privacy policy on their website.

> Reply promptly to any complaints.

> (If handling human resources data) Cooperate and comply with European Data Protection Authorities.

For European individuals

> More transparency about transfers of personal data to the U.S. and stronger protection of personal data.

> Easier and cheaper redress possibilities in case of complaints —directly or with the help of their local Data Protection Authority.

COMMISSION IMPLEMENTING DECISION

of XXX

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Article 25(6) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

1. Introduction

(1) Directive 95/46/EC sets the rules for transfers of personal data from Member States to third countries to the extent that such transfers fall within its scope.

(2) Article 1 of Directive 95/46/EC and recitals 2 and 10 in its preamble seek to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms.[2]

(3) The importance of both the fundamental right to respect for private life, guaranteed by Article 7, and the fundamental right to the protection of personal data, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, has been emphasised in the case-law of the Court of Justice.[3]

(4) Pursuant to Article 25(1) of Directive 95/46/EC Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and the Member State laws implementing other provisions of the Directive are respected prior to the transfer. The Commission may find that a third country ensures such an adequate level of protection

[1] OJ L 281, 23.11.1995, p. 31.

[2] Case C-362/13, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems*"), EU:C:2015:650, paragraph 39.

[3] Case C-553/07, *Rijkeboer*, EU:C:2009:293, paragraph 47; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, paragraph 53; Case C-131/12, *Google Spain and Google*, EU:C:2014:317, paragraphs 53, 66 and 74.

by reason of its domestic law or of the international commitments it has entered into in order to protect the rights of individuals. In that case, and without prejudice to compliance with the national provisions adopted pursuant to other provisions of the Directive, personal data may be transferred from the Member States without additional guarantees being necessary.

(5) Pursuant to Article 25(2) of Directive 95/46/EC, the level of data protection afforded by a third country should be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations, including the rules of law, both general and sectorial, in force in the third country in question.

(6) In Commission Decision 520/2000/EC[4], for the purposes of Article 25(2) of Directive 95/46/EC, the "Safe Harbour Privacy Principles", implemented in accordance with the guidance provided by the so-called "Frequently Asked Questions" issued by the U.S. Department of Commerce, were considered to ensure an adequate level of protection for personal data transferred from the Union to organisations established in the United States.

(7) In its Communications COM(2013) 846 final[5] and COM(2013) 847 final of 27 November 2013[6], the Commission considered that the fundamental basis of the Safe Harbour scheme had to be reviewed and strengthened in the context of a number of factors, including the exponential increase in data flows and their critical importance for the transatlantic economy, the rapid growth of the number of U.S. companies adhering to the Safe Harbour scheme and new information on the scale and scope of certain U.S. intelligence programs which raised questions as to the level of protection it could guarantee. In addition, the Commission identified a number of shortcomings and deficiencies in the Safe Harbour scheme.

(8) Based on evidence gathered by the Commission, including information stemming from the work of the EU-US Privacy Contact Group[7] and the information on US intelligence programs received in the ad hoc EU-US Working Group[8], the Commission formulated 13 recommendations for a review of the Safe Harbour scheme. These recommendations focused on strengthening the substantive privacy principles, increasing the transparency of U.S. self-certified companies' privacy policies, better supervision, monitoring and enforcement by the U.S. authorities of compliance with those principles, the availability of affordable dispute resolution mechanisms, and the need to ensure that use of the national security exception

---

4 Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (OJ L 215 of 28.8.2000, p. 7).

5 Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-U.S. Data Flows, COM(2013) 846 final of 27.11.2013.

6 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final of 27.11.2013.

7 See e.g. Council of the European Union, Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, Note 9831/08, 28 May 2008, available on the internet at: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

8 Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27.11.2013, available on the internet at: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

foreseen in Commission Decision 520/2000/EC is limited to an extent that is strictly necessary and proportionate.

(9) In its judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*[9], the Court of Justice of the European Union declared Commission Decision 520/2000/EC invalid. Without examining the content of the Safe Harbour Privacy Principles, the Court considered that the Commission had not stated in that decision that the United States in fact 'ensured' an adequate level of protection by reason of its domestic law or its international commitments.[10]

(10) In this regard, the Court of Justice explained that, while the term 'adequate level of protection' in Article 25(6) of Directive 95/46/EC does not mean a level of protection identical to that guaranteed in the EU legal order, it must be understood as requiring the third country to ensure a level of protection of fundamental rights and freedoms 'essentially equivalent' to that guaranteed within the Union by virtue of Directive 95/46/EC read in the light of the Charter of Fundamental Rights. Even though the means to which that third country has recourse, in this connection, may differ from the ones employed within the Union, those means must nevertheless prove, in practice, effective.[11]

(11) The Court of Justice criticised the lack of sufficient findings in Decision 2000/520/EC regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and the existence of effective legal protection against interference of that kind.[12]

(12) In 2014 the Commission had entered into talks with the U.S. authorities in order to discuss the strengthening of the Safe Harbour scheme in line with the 13 recommendations contained in Communication COM(2013) 847 final. After the judgment of the Court of Justice of the European Union in the *Schrems* case, these talks were intensified, in order to come to a new adequacy decision which would meet the requirements of Article 25 of Directive 95/46/EC as interpreted by the Court of Justice. The documents which are annexed to this decision and will also be published in the U.S. Federal Register are the result of these discussions. The Privacy Principles (Annex II), together with the official representations and commitments by various U.S. authorities contained in the documents in Annexes I, III to VII, constitute the "EU-U.S. Privacy Shield".

(13) The Commission has carefully analysed U.S. law and practice, including these official representations and commitments. Based on the findings developed in recitals (112)-(116), the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.

---

9 See footnote 2.
10 *Schrems*, paragraph 97.
11 *Schrems*, paragraphs 73-74.
12 *Schrems*, paragraph 88-89.

2. The "EU-U.S. Privacy Shield"

(14) The EU-U.S. Privacy Shield is based on a system of self-certification by which U.S. organisations commit to a set of privacy principles – the EU-U.S. Privacy Shield Framework Principles, including the Supplemental Principles (hereinafter together: "the Privacy Principles") – issued by the U.S. Department of Commerce and contained in Annex II to this decision.

(15) This system will be administered by the Department of Commerce based on its commitments set out in the representations from the U.S. Secretary of Commerce (Annex I to this decision). With regard to the enforcement of the Privacy Principles, the Federal Trade Commission (FTC) and the Department of Transportation have made representations that are contained in Annex IV and Annex V to this decision.

2.1. Privacy Principles

(16) As part of their self-certification under the EU-U.S. Privacy Shield, organisations have to commit to comply with the Privacy Principles.[13]

(17) Under the *Notice Principle*, organisations are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data (e.g. type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability). Further safeguards apply, in particular the requirement for organisations to make public their privacy policies (reflecting the Privacy Principles) and to provide links to the Department of Commerce's website (with further details on self-certification, the rights of data subjects and available recourse mechanisms), the Privacy Shield List referred to in recital (24) and the website of an appropriate alternative dispute settlement provider.

(18) Under the *Choice Principle*, data subjects may object (opt out) if their personal data shall be disclosed to a third party (other than an agent acting on behalf of the organisation) or used for a "materially different" purpose. In case of sensitive data, organisations must in principle obtain the data subject's affirmative express consent (opt in). Moreover, under the Choice Principle, special rules for direct marketing generally allowing for opting out "at any time" from the use of personal data apply.

(19) Under the *Security Principle*, organisations creating, maintaining, using or disseminating personal data must take "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the data. In the case of sub-processing, organisations must conclude a contract with the sub-processor guaranteeing the same level of protection as provided by the Privacy Principles and take steps to ensure its proper implementation.

(20) Under the *Data Integrity and Purpose Limitation Principle*, personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended

[13] Special rules providing additional safeguards apply for human resources data collected in the employment context as laid down in the supplemental principle on "Human Resources Data" of the Privacy Principles. For instance, employers should accommodate the privacy preferences of employees by restricting access to the personal data, anonymising certain data or assigning codes or pseudonyms. Most importantly, organisations are required to cooperate and comply with the advice of Union Data Protection Authorities when it comes to such data.

use, accurate, complete and current. An organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject.

(21) Under the *Access Principle*, data subjects have the right, without need for justification and only against a non-excessive fee, to obtain from an organisation confirmation of whether such organisation is processing personal data related to them and have the data communicated within reasonable time. This right may only be restricted in exceptional circumstances; any denial of, or limitation to the right of access has to be necessary and duly justified, with the organisation bearing the burden of demonstrating that these requirements are fulfilled. Data subjects must be able to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Privacy Principles.

(22) Under the *Accountability for Onward Transfer Principle*, any onward transfer of personal data from an organisation to controllers or processors can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group) and (iii) only if that contract provides the same level of protection as the one guaranteed by the Privacy Principles. This should be read in conjunction with the *Notice* and especially with the *Choice Principle*, according to which data subjects can object (opt out) or, in the case of sensitive data, have to give "affirmative express consent" (opt in) for onward transfers. Where compliance problems arise in the (sub-) processing chain, the organisation acting as the controller of the personal data will have to prove that it is not responsible for the event giving rise to the damage, or otherwise face liability.

(23) Finally, under the *Recourse, Enforcement and Liability Principle*, participating organisations must provide robust mechanisms to ensure compliance with the other Privacy Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies. Once an organisation has voluntarily decided to self-certify under the EU-U.S. Privacy Shield, its effective compliance with the Privacy Principles is compulsory. To be allowed to continue to rely on the Privacy Shield to receive personal data from the Union, such organisation must annually re-certify its participation in the framework. Also, organisations must take measures to verify that their published privacy policies conform to the Privacy Principles and are in fact complied with. This can be done either through a system of self-assessment, which must include internal procedures ensuring that employees receive training on the implementation of the organisation's privacy policies and that compliance is periodically reviewed in an objective manner, or outside compliance reviews, the methods of which may include auditing or random checks. In addition, the organisation must put in place an effective redress mechanism to deal with such complaints (see in this respect also recital (30).

2.2. Transparency and Administration of the EU-U.S. Privacy Shield

(24) To ensure the proper application of the EU-U.S. Privacy Shield, it is necessary that organisations adhering to the Privacy Principles can be identified as such by interested parties, such as data subjects, data exporters and the national Data Protection Authorities ("DPAs"). To this end, the Department of Commerce (or its designee) has undertaken to maintain and make available to the public a list of organisations that have self-certified their adherence to the Privacy Principles and fall within the

jurisdiction of at least one of the government bodies mentioned in Annexes I, II to this decision ("Privacy Shield List"). The Department of Commerce will update the list on the basis of annual re-certification submissions and whenever an organisation withdraws or is removed from the EU-U.S. Privacy Shield. It will also maintain and make available to the public an authoritative record of organisations that have been removed from the list, in each case identifying the reason for such removal. Finally, it will provide a link to the list of Privacy Shield-related FTC cases maintained on the FTC website.

(25) Both the Privacy Shield List and the re-certification submissions will be made publicly available through the Department of Commerce's dedicated website and self-certified organisations must provide the web address for the Privacy Shield List. In addition, if available online, an organisation's privacy policy must include a hyperlink to the Privacy Shield website as well as a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.

(26) Organisations that have persistently failed to comply with the Privacy Principles will be removed from the Privacy Shield List and must return or delete the personal data received under the EU-U.S. Privacy Shield. In other cases of removal, the organisation may retain such data if it affirms to the Department of Commerce on an annual basis its commitment to continue to apply the Principles or provides adequate protection for the personal data by another authorised means (e.g. by using a contract that fully reflects the requirements of the relevant standard contractual clauses approved by the Commission). In this case, an organisation has to identify a contact point within the organisation for all Privacy Shield-related questions.

(27) When an organisation leaves the EU-U.S. Privacy Shield for any reason, it must remove all public statements implying that it continues to participate in the EU-U.S. Privacy Shield or is entitled to its benefits, in particular any references to the EU-U.S. Privacy Shield in its published privacy policy. Any misrepresentation to the general public concerning an organisation's adherence to the Privacy Principles in the form of misleading statements or practices is enforceable by the FTC, Department of Transportation or other relevant U.S. enforcement authorities; misrepresentations to the Department of Commerce are enforceable under the False Statements Act (18 U.S.C. § 1001).

(28) The Department of Commerce will *ex officio* monitor any false claims of Privacy Shield participation or the improper use of the Privacy Shield certification mark, and DPAs can refer organisations for review to a dedicated contact point at the Department. When an organisation has withdrawn from the EU-U.S. Privacy Shield, fails to re-certify or is removed from the Privacy Shield List, the Department of Commerce will on an on-going basis verify that it has deleted from its published privacy policy any references to the Privacy Shield that imply its continued participation and, if it continues to make false claims, refer the matter to the FTC, Department of Transportation or other competent authority for possible enforcement action. It will also send questionnaires to organisations whose self-certifications lapse or that have voluntarily withdrawn from the EU-U.S. Privacy Shield to verify whether the organisation will return, delete or continue to apply the Privacy Principles to the personal data that they received while participating in the EU-U.S. Privacy Shield and, if personal data are to be retained, verify who within the organisation will serve as an ongoing contact point for Privacy Shield-related questions.

2.3. Compliance review and complaint handling

(29) The EU-U.S. Privacy Shield, through the *Recourse, Enforcement and Liability Principle* and the commitments undertaken by the Department of Commerce, the FTC and the Department of Transportation, provides a number of mechanisms to ensure compliance by U.S. self-certified companies with the Privacy Principles. These include the oversight and enforcement through the Department of Commerce and independent authorities (such as the FTC and, in certain cases, the DPAs) as well as the possibility for EU data subjects to lodge complaints regarding non-compliance by U.S. self-certified companies and to have these complaints resolved, if necessary by a decision providing an effective remedy.

(30) First, EU data subjects may vindicate their rights and pursue cases of non-compliance with the Privacy Principles through direct contacts with the *U.S. self-certified company*. To facilitate resolution, the organisation must put in place an effective redress mechanism to deal with such complaints. This includes that an organisation's privacy policy must clearly inform individuals about a contact point, either within or outside the organisation, that will handle complaints (including any relevant establishment in the Union that can respond to inquiries or complaints) and about the independent complaint handling mechanisms. Upon receipt of a complaint, including through the Department of Commerce following referral by a DPA, the organisation must, within a period of 45 days, provide a response to the EU data subject. This response must provide an assessment of the merits of the complaint and, if so, information as to how the organisation will rectify the problem. Likewise, organisations are required to respond promptly to inquiries and other requests for information from the Department of Commerce (or, where the organisation has committed to cooperate with the DPAs, the handling authority designated by the panel of DPAs provided for in the supplemental principle on "The Role of the Data Protection Authorities") relating to their adherence to the Privacy Principles. Finally, organisations must retain their records on the implementation of their privacy policies and make them available upon request in the context of an investigation or a complaint about non-compliance to an independent recourse mechanism or the FTC (or other U.S. authority with jurisdiction to investigate unfair and deceptive practices).

(31) Second, organisations must designate an *independent dispute resolution body* (either in the United States or in the Union) to investigate and resolve individual complaints (unless they are obviously unfounded or frivolous) and to provide appropriate recourse free of charge to the individual. Sanctions and remedies imposed by such a body must be sufficiently rigorous to ensure compliance by organisations with the Privacy Principles and should provide for a reversal or correction by the organisation of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for findings of non-compliance. Independent dispute resolution bodies designated by an organisation will be required to include on their public websites relevant information regarding the EU-U.S. Privacy Shield and the services they provide under it. Each year, they must publish an annual report providing aggregate statistics regarding these services.[14]

[14] The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the

(32) Alternatively, where organisations opt to subscribe to private-sector developed *privacy programs* that incorporate the Privacy Principles into their rules, these must include effective enforcement mechanisms.

(33) In case the organisation fails to comply with the ruling of a dispute resolution or self-regulatory body, the latter must notify such non-compliance to the Department of Commerce and the FTC (or other U.S. authority with jurisdiction to investigate unfair and deceptive practices), or a competent court.

(34) Third, the *Department of Commerce* will systematically verify, in the context of an organisation's certification and re-certification to the framework, that its privacy policies conform to the Principles. It will maintain an updated list of participating organisations.

(35) On an ongoing basis, the Department of Commerce will conduct *ex officio* compliance reviews of self-certified organisations, including through sending detailed questionnaires. It will also systematically carry out reviews whenever it has received a specific (non-frivolous) complaint, when an organisation does not provide satisfactory responses to its enquiries, or when there is credible evidence suggesting that an organisation may not be complying with the Privacy Principles.

(36) In addition, the Department of Commerce has committed to receive, review and undertake best efforts to resolve complaints about an organisation's non-compliance with the Privacy Principles. To this end, the Department of Commerce provides special procedures for DPAs to refer complaints to a dedicated contact point, track them and follow up with companies to facilitate resolution. In order to expedite the processing of individual complaints, the contact point will liaise directly with the respective DPA on compliance issues and in particular update it on the status of complaints within a period of not more than 90 days following referral. This allows data subjects to bring complaints of non-compliance by U.S. self-certified companies directly to their national DPA and have them channelled to the Department of Commerce as the U.S. authority administering the EU-U.S. Privacy Shield. The Department of Commerce has also committed to provide, in the annual review of the functioning of the EU-U.S. Privacy Shield, a report that analyses in aggregate form the complaints it receives each year.

(37) The Department of Commerce will also verify that self-certified U.S. companies have actually registered with the independent recourse mechanisms they claim they are registered with. Both the organisations and the responsible independent recourse mechanisms are required to respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield.

(38) Where, on the basis of its *ex officio* verifications, complaints or any other information, the Department of Commerce concludes that an organisation has persistently failed to comply with the Privacy Principles it will remove such an organisation from the Privacy Shield list. Refusal to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body, including a DPA, will be regarded as a persistent failure to comply.

(39) The Department of Commerce will maintain an updated list of organisations that are no longer part of the framework, setting out the reasons for their removal from the list. In addition, it will monitor organisations that are no longer members of the EU-U.S.

---

length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed**.**

Privacy Shield, either because they have voluntarily withdrawn or because their certification has lapsed, to verify whether they will return, delete or retain the personal data received previously under the framework. In the latter case, organisations are obliged to continue to apply the Privacy Principles to these personal data. In cases where the Department of Commerce has removed organisations from the framework due to a persistent failure to comply with the Privacy Principles, it will ensure that those organisations must return or delete the personal data they received under the framework. Moreover, the Department of Commerce will actively search for and address false claims of participation in the framework, including by former members. Such false claims may be actionable by the FTC or other enforcement agency.

(40) Fourth, the *Federal Trade Commission* will give priority consideration to referrals of non-compliance with the Privacy Principles received from independent dispute resolution or self-regulatory bodies, the Department of Commerce and DPAs (acting on their own initiative or upon complaints) to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive practices has been violated. The FTC has committed to create a standardised referral process, to designate a point of contact at the agency for DPA referrals, and to exchange information on referrals. In addition, it will accept complaints directly from individuals and will undertake Privacy Shield investigations on its own initiative, in particular as part of its wider investigations of privacy issues.

(41) The FTC can enforce compliance through administrative orders ("consent orders"), and it will systematically monitor compliance with such orders. Where organisations fail to comply, the FTC may refer the case to the competent court in order to seek civil penalties and other remedies, including for any injury caused by the unlawful conduct. Alternatively, the FTC may directly seek a preliminary or permanent injunction or other remedies from a federal court. Each consent order issued to a Privacy Shield organisation will have self-reporting provisions[15], and organisations will be required to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC. Finally, the FTC will maintain an online list of companies subject to FTC or court orders in Privacy Shield cases.

(42) Fifth, where a national *Data Protection Authority* investigates a complaint regarding non-compliance with the Privacy Principles, organisations are obliged to cooperate in the investigation and the resolution of this complaint if it concerns processing of human resources data collected in the context of an employment relationship or if they have voluntarily submitted to the oversight by DPAs. Notably, they have to respond to inquiries, comply with the advice given by the DPA, including for remedial or compensatory measures, and provide the DPA with written confirmation that such action has been taken. In order to facilitate cooperation, the Department of Commerce will establish a dedicated contact point to act as a liaison and to assist with DPA inquiries regarding an organisation's compliance with the Privacy Principles. Likewise, the FTC has committed to provide the DPAs with investigatory assistance pursuant to the U.S. SAFE WEB Act.[16]

(43) The advice of the DPAs will be delivered through an informal panel of DPAs established at Union level, which will also help to ensure a harmonised and coherent

[15] FTC or court orders may require companies to implement privacy programs and to regularly make compliance reports or independent third-party assessments of those programs available to the FTC.

[16] U.S. SAFE WEB Act of 2006, Pub. L. 109-455 of 22.12.2006.

approach.[17] Advice will be issued after both sides in the dispute have had a reasonable opportunity to comment to provide any evidence they wish. The respective DPA will deliver advice as quickly as the requirement for due process allows, and as a general rule within 60 days after receiving a complaint. If an organisation fails to comply within 25 days of delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the FTC (or other competent U.S. enforcement authority), or to conclude that the commitment to cooperate has been seriously breached. In the first alternative, this may lead to enforcement action based on Section 5 of the FTC Act (or similar statute). In the second alternative, the panel will inform the Department of Commerce which will consider the organisation's refusal as a persistent failure to comply that will lead to the organisation's removal from the Privacy Shield List.

(44) Where a DPA, upon receiving a claim by an EU data subject, considers that the individual's personal data transferred to an organisation in the United States are not afforded an adequate level of protection, it can also exercise its powers vis-à-vis the data exporter and, if necessary, suspend the data transfer.

(45) In all these cases, if the DPA to which the complaint has been addressed has taken no or insufficient action to address a complaint, the individual complainant has the possibility to challenge such (in-) action in the national courts of the respective Member State.

(46) Sixth, as a recourse mechanism of 'last resort' in case none of the other available redress avenues has satisfactorily resolved an individual's complaint, the EU data subject may invoke binding arbitration by the *"Privacy Shield Panel"*. This panel will consist of a pool of at least 20 arbitrators designated by the Department of Commerce and the Commission based on their independence, integrity, as well as experience in U.S. privacy and Union data protection law. For each individual dispute, the parties will select from this pool a panel of one or three[18] arbitrators. The proceedings will be governed by standard arbitration rules to be agreed between the Department of Commerce and the Commission. While the arbitration will take place in the United States, EU data subjects may choose to participate through video or telephone conference, to be provided at no cost to the individual. Also, unless otherwise agreed, the language used in the arbitration will be English; however, upon a reasoned request, interpretation at the arbitral hearing and translation will normally[19] be provided at no cost to the data subject, who moreover may be assisted by his or her national DPA in preparing his or her claim. While each party has to bear its own attorney's fees, if represented by an attorney before the panel, the Department of Commerce will establish a fund supplied with annual contributions by the Privacy Shield organisations, which shall cover the eligible costs of the arbitration procedure, up to maximum amounts, to be determined by the U.S. authorities in consultation with the Commission.

(47) The Privacy Shield Panel will have the authority to impose "individual-specific, non-monetary equitable relief"[20] necessary to remedy non-compliance with the Privacy

[17] See the Supplemental Principle on "The Role of the Data Protection Authorities" (Sec. III.5.c of the Privacy Principles set out in Annex II).

[18] The number of arbitrators on the panel will have to be agreed between the parties.

[19] However, the panel may find that, under the circumstances of the specific arbitration, coverage would lead to unjustified or disproportionate costs.

[20] Individuals may not claim damages in arbitration, but in turn invoking arbitration will not foreclose the option to seek damages in the ordinary U.S. courts.

Principles. While the panel will take into account other remedies already obtained by other Privacy Shield mechanisms when making its determination, individuals may still resort to arbitration if they consider these other remedies to be insufficient. This will allow EU data subjects to invoke arbitration in all cases where the action or inaction of the competent U.S. authorities (for instance the FTC) has not satisfactorily resolved their complaints. Arbitration may not be invoked if a DPA has the legal authority to resolve the claim at issue with respect to the U.S. self-certified company, namely in those cases where the organisation is either obliged to cooperate and comply with the advice of the DPAs as regards the processing of human resources data collected in the employment context, or has voluntarily committed to do so. Individuals can enforce the arbitration decision in the U.S. courts under the Federal Arbitration Act, thereby ensuring a legal remedy in case a company fails to comply.

(48) Where an organisation does not comply with its commitment to respect the Principles and published privacy policy, additional avenues for judicial redress may be available under the law of the U.S. States which provide for legal remedies under tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract.

(49) In the light of the information in this section, the Commission considers that the Privacy Principles issued by the U.S. Department of Commerce as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the substantive basic principles laid down in Directive 95/46/EC.

(50) In addition, the effective application of the Privacy Principles is guaranteed by the transparency obligations and the administration of the Privacy Shield by the Department of Commerce.

(51) Moreover, the Commission considers that, taken as a whole, the oversight and recourse mechanisms provided for by the Privacy Shield enable infringements of the Privacy Principles by Privacy Shield organisations to be identified and punished in practice and offer legal remedies to the data subject to gain access to personal data relating to him and, eventually, to obtain the rectification or erasure of such data.

3. Access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities

(52) As follows from Annex II, Sec. I.5, adherence to the Privacy Principles is limited to the extent necessary to meet national security, public interest or law enforcement requirements.

(53) The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence[21], has provided the Commission with detailed representations

[21] The Office of the Director of National Intelligence (ODNI) serves as the head of the Intelligence Community and acts as the principal advisor to the President and the National Security Council. See the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 of 17.12.2004. Among others, the ODNI shall determine requirements for, and manage and direct the tasking, collection, analysis, production and dissemination of national intelligence by the Intelligence Community, including by

and assurances that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community. Finally, a representation from the U.S. Department of Justice, contained in Annex VII to this decision, describes the limitations and safeguards applicable to access and use of data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.

(54) The findings of the Commission on the limitations on access and use of personal data transferred from the European Union to the United States by U.S. public authorities and the existence of effective legal protection are further elaborated below.

3.1. Access and use by U.S. public authorities for national security purposes

(55) The Commission's analysis shows that U.S. law contains clear limitations on the access and use of personal data transferred under the EU-U.S. Privacy Shield for national security purposes as well as oversight and redress mechanisms that provide sufficient safeguards for those data to be effectively protected against unlawful interference and the risk of abuse.[22] Since 2013, when the Commission issued its two Communications (see recital (7)), this legal framework has been significantly strengthened.

3.1.1. Limitations

(56) Under the U.S. Constitution, ensuring national security falls within the President's authority as Commander in Chief, as Chief Executive and, as regards foreign intelligence, to conduct U.S. foreign affairs.[23] While Congress has the power to impose limitations, and has done so in various respects, within these boundaries the President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives. This of course also applies in those areas where no Congressional guidance exists. At present, the two central legal instruments in this regard are Executive Order 12333 ("E.O. 12333")[24] and Presidential Policy Directive 28.

(57) Presidential Policy Directive 28 ("PPD-28"), issued on 17 January 2014, imposes a number of limitations for "signals intelligence" operations.[25] This presidential directive has binding force for U.S. intelligence authorities[26] and remains effective

developing guidelines for how information or intelligence is accessed, used and shared. See Sec. 1.3 (a), (b) of E.O. 12333.

22 See *Schrems*, paragraph 91.

23 U.S. Const., Article II. See also the introduction to PPD-28.

24 E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981). To the extent that the Executive Order is publicly accessible, it defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities (in particular the need to promulgate specific procedural rules). According to Sec. 3.2 of E.O. 12333, the President, supported by the National Security Council, and the DNI shall issue such appropriate directives, procedures and guidance as are necessary to implement the order.

25 According to E.O. 12333, the Director of the National Security Agency (NSA) is the Functional Manager for signals intelligence and shall operate a unified organization for signals intelligence activities.

26 For the definition of the term "Intelligence Community", see Sec. 3.5 (h) of E.O. 12333 with n. 1 of PPD-28.

upon change in the U.S. Administration[27]. PPD-28 is of particular importance for non-US persons, including EU data subjects. Among others, it stipulates that:

(a) the collection of signals intelligence must be based on statute or Presidential authorisation, and must be undertaken in accordance with the U.S. Constitution (in particular the Fourth Amendment) and U.S. law;

(b) all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside;

(c) all persons have legitimate privacy interests in the handling of their personal information;

(d) privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities;

(e) U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of their nationality or where they might reside.

(58) PPD-28 directs that signals intelligence may be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purpose (e.g. to afford a competitive advantage to U.S. companies). Furthermore, it directs that collection shall always[28] be "as tailored as feasible", and that the Intelligence Community shall prioritise the availability of other information and appropriate and feasible alternatives.[29]

(59) In this regard, the representations of the Office of the Director of National Intelligence (ODNI) provide further assurance that these requirements, including the definition of bulk collection in PPD-28 (n. 5), express a general rule of prioritisation of targeted over bulk collection. According to these representations, Intelligence Community elements "should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (*e.g.* specific facilities, selection terms and identifiers)."[30] While PPD-28 explains that Intelligence Community elements must sometimes collect bulk signals intelligence in certain circumstances, for instance in order to identify new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence.[31] Hence, bulk collection will only be allowed where targeted collection via the use of discriminants is not possible "due to technical or operational considerations".[32] This applies both to the manner in which signals

---

27 See Memorandum by the Office of Legal Counsel, Department of Justice, to President Clinton, 29.01.2000. According to this legal opinion, presidential directives have the "same substantive legal effect as an Executive Order".

28 See ODNI Representations (Annex VI), p. 3.

29 It should also be noted that, according to Sec. 2.4 of E.O. 12333, elements of the IC "shall use the least intrusive collection techniques feasible within the United States".

30 ODNI Representations (Annex VI), p. 3.

31 See also Sec. 5(d) of PPD-28 which directs the Director of National Intelligence, in coordination with the heads of relevant Intelligence Community elements and the Office of Science and Technology Policy, to provide the President with a "report assessing the feasibility of creating software that would allow the Intelligence Community more easily to conduct targeted information acquisition rather than bulk collection." According to public information, the result of this report was that "there is no software-based alternative which will provide a complete substitute for bulk collection in the detection of some national security threats." See Signals Intelligence Reform, 2015 Anniversary Report.

32 See ODNI Representations (Annex VI), p. 3.

intelligence is collected and to what is actually collected.[33] According to representations of the ODNI all this ensures that the exception does not swallow the rule.[34]

(60) Furthermore, the representations of the ODNI provide assurance that decisions about what is "feasible" are not left to the discretion of individual intelligence agents, but are subject to the policies and procedures that the various U.S. Intelligence Community elements (agencies) are required to put in place to implement PPD-28.[35] Also, the research and determination of appropriate selectors takes place within the overall "National Intelligence Priorities Framework" (NIPF) which ensures that intelligence priorities are set by high-level policymakers and regularly reviewed to remain responsive to actual national security threats and taking into account possible risks, including privacy risks.[36] On this basis, agency personnel researches and identifies specific selection terms expected to collect foreign intelligence responsive to the priorities.[37] Selectors must be regularly reviewed to see if they still provide valuable intelligence in line with the priorities.[38]

(61) Finally, even where the United States considers it necessary to collect signals intelligence in bulk, under the conditions set out in recitals (58)-(60), PPD-28 limits the use of such information to a specific list of six national security purposes with a view to protect the privacy and civil liberties of all persons, whatever their nationality and place of residence.[39] These permissible purposes comprise measures to detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, to the Armed Forces or military personnel, as well as transnational criminal threats related to the other five purposes, and will be reviewed at least on an annual basis. According to the representations by the U.S. government, Intelligence Community elements have reinforced their analytic practices and standards for querying unevaluated signals intelligence to conform with these requirements; the use of targeted queries "ensures that only those items believed to be of potential intelligence value are ever presented to analysts to examine."[40]

(62) These limitations are particularly relevant to personal data transferred under the EU-U.S. Privacy Shield, in particular in case access to personal data were to take place outside the United States, including during their transit on the transatlantic cables from the Union to the United States. As confirmed by the U.S. authorities in the representations of the ODNI, the limitations and safeguards set out therein – including those of PPD-28 – apply to such access.[41]

---

33 ODNI Representations (Annex VI), p. 3.

34 ODNI Representations (Annex VI), p. 4.

35 See Sec. 4(b),(c) of PPD-28. According to public information, the 2015 review confirmed the existing six purposes. See ODNI, Signals Intelligence Reform, 2016 Progress Report.

36 ODNI Representations (Annex VI), p. 6 (with reference to Intelligence Community Directive 204). See also Sec. 3 of PPD-28.

37 ODNI Representations (Annex VI), p. 6. See, for instance, NSA Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014. See also ODNI Status Report 2014. For access requests under Sec. 702 FISA, queries are governed by the FISC-approved minimization procedures. See NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014.

38 See Signal Intelligence Reform, 2015 Anniversary Report. See also ODNI Representations (Annex VI), pp. 6, 8-9, 11.

39 See Sec. 2 of PPD-28.

40 ODNI Representations (Annex VI), p. 4. See also Intelligence Community Directive 203.

41 ODNI Representations (Annex VI), p. 2. Likewise, the limitations stipulated in E.O. 12333 (e.g. the need for collected information to respond to intelligence priorities set by the President) apply.

(63) Although not phrased in those legal terms, these principles capture the essence of the principles of necessity and proportionality. Targeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical or operational reasons. Even where *bulk collection* cannot be avoided, further "use" of such data through access is *strictly limited* to specific, legitimate national security purposes.[42]

(64) As a directive issued by the President as the Chief Executive, these requirements bind the entire Intelligence Community and have been further implemented through agency rules and procedures that transpose the general principles into specific directions for day-to-day operations. Moreover, while Congress is itself not bound by PPD-28, it has also taken steps to ensure that collection and access of personal data in the United States are targeted rather than carried out "on a generalised basis".

(65) It follows from the available information, including the representations received from the U.S. government, that once the data has been transferred to organisations located in the United States and self-certified under the EU-U.S. Privacy Shield, U.S. intelligence agencies may only[43] seek personal data where their request complies with the Foreign Intelligence Surveillance Act (FISA) or is made by the Federal Bureau of Investigation based on a so-called National Security Letter (NSL)[44]. Several legal bases exist under FISA that may be used to collect (and subsequently process) the personal data of EU data subjects transferred under the EU-U.S. Privacy Shield. Aside from traditional individualised electronic surveillance under Section 104 FISA[45] and the installation of pen registers or trap and trace devices under Section 402 FISA[46], the two central instruments are Section 501 FISA (ex-Section 215 U.S. PATRIOT ACT) and Section 702 FISA.[47]

---

42 See *Schrems*, paragraph 93.

43 In addition, the collection of data by the FBI may also be based on law enforcement authorizations (see Section 3.2 of this decision).

44 For further explanations on the use of NSL see ODNI Representations (Annex VI), pp. 13-14 with n. 38. As indicated therein, the FBI may resort to NSLs only to request non-content information relevant to an authorized national security investigation to protect against international terrorism or clandestine intelligence activities. As regards data transfers under the EU-U.S. Privacy Shield, the most relevant legal authorization appears to be the Electronic Communications Privacy Act (18 U.S.C. § 2709), which requires that any request for subscriber information or transactional records uses a "term that specifically identifies a person, entity, telephone number, or account".

45 50 U.S.C. § 1804. While this legal authority requires a "statement of the facts and circumstances relied upon by the applicant to justify his belief that (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power", the latter may include non-U.S. persons that engage in international terrorism or the international proliferation of weapons of mass destruction (including preparatory acts) (50 U.S.C. § 1801 (b)(1)). Still, there is only a theoretical link to personal data transferred under the EU-U.S. Privacy Shield, given that the statement of facts also has to justify the belief that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power". In any event, the use of this authority requires application to the FISC which will assess, among others, whether on the basis of the submitted facts there is probable cause that this is indeed the case.

46 50 U.S.C. § 1842 with § 1841(2) and Sec. 3127 of Title 18. This authority does not concern the contents of communications, but rather aims at information about the customer or subscriber using a service (such as name, address, subscriber number, length/type of service received, source/mechanism of payment). It requires an application for an order by the FISC (or a U.S. Magistrate Judge) and the use of a specific selection term in the sense of § 1841(4), i.e. a term that specifically identifies a person, account, etc. and is used to limit, to the greatest extent reasonably possible, the scope of the information sought.

47 While Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT) authorizes the FBI to request a court order aiming at the production of "tangible things" (in particular telephone metadata, but also business records) for foreign intelligence purposes, Sec. 702 FISA allows US Intelligence Community elements to seek access to

(66) In this respect, the USA FREEDOM Act, which was adopted on 2 June 2015, prohibits the collection in bulk of records based on Section 402 FISA (pen register and trap and trace authority), Section 501 FISA (formerly: Section 215 of the U.S. PATRIOT ACT)[48] and through the use of NSL, and instead requires the use of specific "selection terms".[49]

(67) While the FISA contains further legal authorisations to carry out national intelligence activities, including signals intelligence, the Commission's assessment has shown that, insofar as personal data to be transferred under the EU-U.S. Privacy Shield are concerned, these authorities equally restrict public interference to targeted collection and access.

(68) This is clear for traditional individualised electronic surveillance under Section 104 FISA[50]. As for Section 702 FISA, which provides the basis for two important intelligence programs run by the U.S. intelligence agencies (PRISM, UPSTREAM), searches are carried out in a targeted manner through the use of individual selectors that identify specific communications facilities, like the target's email address or telephone number, but not key words or even the names of targeted individuals.[51] Therefore, as noted by the Privacy and Civil Liberties Oversight Board (PCLOB), Section 702 surveillance "consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made".[52] Due to a "sunset" clause, Section 702 FISA will have to be reviewed in 2017, at which time the Commission will have to reassess the safeguards available to EU data subjects.

(69) Moreover, in its representations the U.S. government has given the European Commission explicit assurance that the U.S. Intelligence Community "does not engage in indiscriminate surveillance of anyone, including ordinary European citizens"[53]. As regards personal data collected within the United States, this statement is supported by empirical evidence which shows that *access requests* through NSL and under FISA,

---

information, including the content of internet communications, from within the United States, but targeting certain non-U.S. persons outside the United States.

48 Based on this provision, the FBI may request "tangible things" (e.g. records, papers, documents) based on a showing to the Foreign Intelligence Surveillance Court (FISC) that there are reasonable grounds to believe that they are relevant to a specific FBI investigation. In carrying out its search, the FBI must use FISC-approved selection terms for which there is a "reasonable, articulable suspicion" that such term is associated with one or more foreign powers or their agents engaged in international terrorism or activities in preparation therefore. See PCLOB, Sec. 215 Report, p. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016, pp. 4-6.

49 ODNI Representations (Annex VI), p. 13 (n. 38).

50 See footnote 45.

51 PCLOB, Sec. 702 Report, pp. 32-33 with further references. According to its privacy office, the NSA must verify that there is a connection between the target and the selector, must document the foreign intelligence information expected to be acquired, this information must be reviewed and approved by two senior NSA analysts, and the overall process will be tracked for subsequent compliance reviews by the ODNI and Department of Justice. See NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.04.2014.

52 PLCOB, Sec. 702 Report, p. 111. See also ODNI Representations (Annex VI), p. 9 ("Collection under Section 702 of the [FISA] is not 'mass and indiscriminate' but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets") and p. 13, n. 36 (with reference to a 2014 FISC Opinion); NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.04.2014. Even in the case of UPSTREAM, the NSA may only request the interception of electronic communications to, from, or about tasked selectors.

53 ODNI Representations (Annex VI), p. 18. See also p. 6, according to which the applicable procedures "demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information, and to implement – from the highest levels of our Government – the principle of reasonableness."

both individually and together, only concern a relatively small number of targets when compared to the overall flow of data on the internet.[54] Moreover, the U.S. government has assured the Commission that "any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet."[55] This statement also covers possible access to the transatlantic cables (which the U.S. government neither confirms nor denies is taking place).

(70) As regards *access* to collected data and *data security*, PPD-28 requires that access "shall be limited to authorized personnel with a need to know the information to perform their mission" and that personal information "shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information". Intelligence personnel receive appropriate and adequate training in the principles set forth in PPD-28.[56]

(71) Finally, as regards the *storage* and further *dissemination* of personal data from EU data subjects collected by U.S. intelligence authorities, PPD-28 states that all persons (including non-U.S. persons) should be treated with dignity and respect, that all persons have legitimate privacy interests in the handling of their personal data and that Intelligence Community elements therefore have to establish policies providing appropriate safeguards for such data "reasonably designed to minimize the[ir] dissemination and retention".

(72) The U.S. government has explained that this reasonableness requirement signifies that Intelligence Community elements will not have to adopt "any measure theoretically possible", but will need to "balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities."[57] In this respect, non-U.S. persons will be treated in the same way as U.S. persons, based on procedures approved by the Attorney-General.[58]

(73) According to these rules, retention is generally limited to a maximum of five years, unless there is a specific determination in law or an express determination by the

---

[54] See Statistical Transparency Report Regarding Use of National Security Authorities, 22.04.2015. For the overall flow of data on the internet, see for example Fundamental Rights Agency, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), at pp. 15-16. As regards the UPSTREAM program, according to a declassified FISC opinion of 2011, over 90% of the electronic communications acquired under Sec. 702 FISA came from the PRISM program, whereas less than 10% came from UPSTREAM. See FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (available at: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

[55] ODNI Representations (Annex VI), p. 4.

[56] See Sec. 4(a)(ii) of PPD-28. See also ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, July 2014, p. 5, according to which "Intelligence Community element policies should reinforce existing analytic practices and standards whereby analysts must seek to structure queries or other search terms and techniques to identify intelligence information relevant to a valid intelligence or law enforcement task; focus queries about persons on the categories of intelligence information responsive to an intelligence or law enforcement requirement; and minimize the review of personal information not pertinent to intelligence or law enforcement requirements." See e.g. CIA, Signals Intelligence Activities, p. 5; FBI, Presidential Policy Directive 28 Policies and Procedures, p. 3. According to the 2016 Progress Report on the Signals Intelligence Reform, IC elements (including the FBI, CIA and NSA) have taken steps to sensitise their personnel to the requirements of PPD-28 by creating new or modifying existing training policies.

[57] ODNI Representations (Annex VI), p. 4.

[58] See Sec. 4(a)(i) of PPD-28 with Sec 2.3 of E.O. 12333.

Director of National Intelligence after careful evaluation of privacy concerns – taking into account the views of the ODNI Civil Liberties Protection Officer as well as agency privacy and civil liberties officials – that continued retention is in the interest of national security.[59] Dissemination is limited to cases where the information is relevant to the underlying purpose of the collection and thus responsive to an authorised foreign intelligence or law enforcement requirement.[60]

(74) According to the assurances given by the U.S. government, personal information may not be disseminated solely because the individual concerned is a non-U.S. person and "signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement."[61]

(75) The Commission therefore concludes that there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question.

3.1.2. Effective legal protection

(76) The Commission has assessed both the oversight mechanisms that exist in the United States with regard to any interference by U.S. intelligence authorities with personal data transferred to the United States and the avenues available for EU data subjects to seek individual redress.

Oversight

(77) First, intelligence activities by U.S. authorities are subject to extensive oversight from within the executive branch.

(78) According to PPD-28, Section 4(a)(iv), the policies and procedures of Intelligence Community elements "shall include appropriate measures to facilitate oversight over

[59] Sec. 4(a)(i) of PPD-28; ODNI Representations (Annex VI), p. 7. For instance, for personal information collected under Sec. 702 FISA, the NSA's FISC-approved minimization procedures foresee as a rule that the metadata and unevaluated content for PRISM is retained for no more than five years, whereas UPSTREAM data is retained for no more than two years. The NSA complies with these storage limits through an automated process that deletes collected data at the end of the respective retention period. See NSA Sec. 702 FISA Minimization Procedures, Sec. 7 with Sec. 6(a)(1); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014. Likewise, retention under Sec. 501 FISA (ex-Sec. 2015 U.S. PATRIOT ACT) is limited to five years, unless the personal data form part of properly approved dissemination of foreign intelligence information, or if the DOJ advises the NSA in writing that the records are subject to a preservation obligation in pending or anticipated litigation. See NSA, CLOP, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016.

[60] In particular, in case of Sec. 501 FISA (ex-Sec. 215 U.S. PATRIOT ACT), dissemination of personal information may take place only for counterterrorism purposes or as evidence of a crime; in case of Sec. 702 FISA only if there is a valid foreign intelligence or law enforcement purpose. Cf. NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.01.2016. See also NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014.

[61] ODNI Representations (Annex VI), p. 7 (with reference to Intelligence Community Directive (ICD) 203).

the implementation of safeguards protecting personal information"; these measures should include periodic auditing.[62]

(79) Multiple oversight layers have been put in place in this respect, including civil liberties or privacy officers, Inspector Generals, the ODNI Civil Liberties and Privacy Office, the PCLOB, and the President's Intelligence Oversight Board. These oversight functions are supported by compliance staff in all the agencies.[63]

(80) As explained by the U.S. government[64], *civil liberties or privacy officers* with oversight responsibilities exist at various departments with intelligence responsibilities and intelligence agencies.[65] While the specific powers of these officers may vary somewhat depending on the authorising statute, they typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated (and in some cases, like the ODNI, may themselves have the power to investigate complaints[66]). The head of the department/agency in turn has to ensure that the officer receives all the information and is given access to all material necessary to carry out his functions. Civil liberties and privacy officers periodically report to Congress and the PCLOB, including on the number and nature of the complaints received by the department/agency and a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the officer.[67]

(81) In addition, each Intelligence Community element has its own *Inspector General* with responsibility, among others, to oversee foreign intelligence activities.[68] This includes, within the ODNI, an Office of the Inspector General with comprehensive jurisdiction over the entire Intelligence Community and authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority, in connection with ODNI and/or Intelligence Community programs and activities.[69] Inspectors General are statutorily independent[70] units responsible for conducting

---

62 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, p. 7. See e.g. CIA, Signals Intelligence Activities, p. 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 8.1, 8.6(c).

63 For instance, the NSA employs more than 300 compliance staff in the Directorate for Compliance. See ODNI Representations (Annex VI), p. 7.

64 See Ombudsperson Mechanism (Annex III), Sec. 6(b) (i) to (iii).

65 See 42 U.S.C. § 2000ee-1. This includes for instance the Department of State, the Department of Justice (including the FBI), the Department of Homeland Security, the Department of Defense, the NSA, CIA and the ODNI.

66 According to the U.S. government, if the ODNI Civil Liberties and Privacy Office receives a complaint, it will also coordinate with other Intelligence Community elements on how that complaint should be further processed within the IC. See Ombudsperson Mechanism (Annex III), Sec. 6(b) (ii).

67 See 42 U.S.C. § 2000ee-1 (f)(1),(2).

68 ODNI Representations (Annex VI), p. 7. See e.g. NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 8.1; CIA, Signals Intelligence Activities, p. 7 (Responsibilities).

69 This IG (which was created in October 2010) is appointed by the President, with Senate confirmation, and can be removed only by the President, not the DNI.

70 These IGs have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal. This does not necessarily mean that they are completely free from instructions. In some cases, the head of the department may prohibit the Inspector General from initiating, carrying out, or completing an audit or investigation where this is considered necessary to preserve important national (security) interests. However, Congress must be informed of the exercise of this authority and on this basis could hold the respective director responsible. See, e.g., Inspector

audits and investigations relating to the programs and operations carried out by the respective agency for national intelligence purposes, including for abuse or violation of the law.[71] They are authorised to have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony.[72] While the Inspectors General can only issue non-binding recommendations for corrective action, their reports, including on follow-up action (or the lack thereof) are made public and moreover sent to Congress which can on this basis exercise its oversight function.[73]

(82) Furthermore, the *Privacy and Civil Liberties Oversight Board*, an independent agency within the executive branch composed of members[74] appointed by the President with Senate approval, is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. For these purposes, it may access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony. It receives reports from the civil liberties and privacy officers of several federal departments/agencies[75], may issue recommendations to them, and regularly reports to Congressional committees and the President.[76] The PCLOB is also tasked, within the confines of its mandate, to prepare a report assessing the implementation of PPD-28.

(83) Finally, the aforementioned oversight mechanisms are complemented by the *Intelligence Oversight Board* established within the President's Intelligence Advisory Board which oversees compliance by US intelligence authorities with the Constitution and all applicable rules.

(84) To facilitate the oversight, Intelligence Community elements are encouraged to design information systems to allow for the monitoring, recording and reviewing of queries or other searches of personal information.[77] Oversight and compliance bodies will periodically check the practices of Intelligence Community elements for protecting personal information contained in signals intelligence and their compliance with those procedures.[78]

(85) These oversight functions are moreover supported by extensive reporting requirements with respect to non-compliance. In particular, agency procedures must ensure that, when a significant compliance issue occurs involving personal information of any

---

General Act of 1978, § 8 (IG of the Department of Defense); § 8E (IG of the DOJ), § 8G (d)(2)(A),(B) (IG of the NSA); 50. U.S.C. § 403q (b) (IG for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (IG for the Intelligence Community).

71 See ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, as amended, Pub. L. 113-126 of 7.07.2014.

72 See Inspector General Act of 1978, § 6.

73 See ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, §§ 4(5), 5. According to Sec. 405(b)(3),(4) of the Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 of 7.10.2010, the IG for the Intelligence Community will keep the DNI as well as Congress informed of the necessity for, and the progress of, corrective actions.

74 In addition, the PCLOB employs some 20 regular staff. See https://www.pclob.gov/about-us/staff.html.

75 These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, the Director of National Intelligence and the Central Intelligence Agency, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

76 See 42 U.S.C. § 2000ee. See also Ombudsperson Mechanism (Annex III), Sec. 6(b) (iv).

77 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, pp. 7-8.

78 Id. at p. 8. See also ODNI Representations (Annex VI), p. 9.

person, regardless of nationality, collected through signals intelligence, such issue shall be promptly reported to the head of the Intelligence Community element, which in turn will notify the Director of National Intelligence who, under PPD-28, shall determine if any corrective actions are necessary.[79] Moreover, according to E.O. 12333, all Intelligence Community elements are required to report to the Intelligence Oversight Board on non-compliance incidents.[80] These mechanisms ensure that the issue will be addressed at the highest level in the Intelligence Community. Where it involves a non-U.S. person, the Director of National Intelligence, in consultation with the Secretary of State and the head of the notifying department or agency, shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.[81]

(86) Second, in addition to these oversight mechanisms within the executive branch, the U.S. Congress, specifically the *House and Senate Intelligence and Judiciary Committees*, have oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence. According to the National Security Act, "[t]he President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter."[82] Also, "[t]he President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity."[83] Members of these committees have access to classified information as well as intelligence methods and programs.[84]

(87) Later statutes have extended and refined the reporting requirements, both regarding the Intelligence Community elements, the relevant Inspector Generals and the Attorney-General. For instance, FISA requires the Attorney General to "fully inform" the Senate and House Intelligence and Judiciary Committees regarding the government's activities under certain sections of FISA.[85] It also requires the government to provide the Congressional committees with copies of "all decisions, orders, or opinions of the FISC or that include significant construction or interpretation" of FISA provisions. In particular, as regards surveillance under Section 702 FISA, oversight is exercised through statutorily required reports to the Intelligence and Judiciary Committees, as well as frequent briefings and hearings. These include a semi-annual report by the Attorney General describing the use of Section 702 FISA, with supporting documents including notably the Department of Justice and ODNI compliance reports and a description of any incidents of non-compliance,[86] and a separate semi-annual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures

---

79 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, p. 7. See, e.g., NSA, PPD-28 Section 4 Procedures, 12.01.2015, Sec. 7.3, 8.7(c),(d); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III.(A)(4), (B)(4); CIA, Signals Intelligence Activities, p. 6 (Compliance) and p. 8 (Responsibilities).

80 See E.O. 12333, Sec. 1.6(c).

81 PPD-28, Sec. 4(a)(iv).

82 See Sec. 501(a)(1) (50 U.S.C. § 413(a)(1)). This provision contains the general requirements as regards Congressional oversight in the area of national security.

83 See Sec. 501(b) (50 U.S.C. § 413(b)).

84 Cf. Sec. 501(d) (50 U.S.C. § 413(d)).

85 See 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

86 See 50 U.S.C. § 1881f.

designed to ensure that collection is for a valid foreign intelligence purpose.[87] Congress also receives reports by the Inspector Generals who are authorised to evaluate the agencies' compliance with targeting and minimization procedures and Attorney General Guidelines.

(88) According to the USA FREEDOM Act of 2015, the U.S. government must disclose to Congress (and the public) each year the number of FISA orders and directives sought and received, as well as estimates of the number of U.S. and non-U.S. persons targeted by surveillance, among others.[88] The Act also requires additional public reporting about the number of NSL issued, again both with regard to U.S. and non-U.S. persons (while at the same time allowing the recipients of FISA orders and certifications, as well as NSL requests, to issue transparency reports under certain conditions).[89]

(89) Third, intelligence activities by U.S. public authorities based on FISA allow for review, and in some cases prior authorisation of the measures, by the *FISA Court* (FISC)[90], an independent tribunal[91] whose decisions can be challenged before the Foreign Intelligence Court of Review (FISCR)[92] and, ultimately, the Supreme Court of the United States.[93] In case of prior authorisation, the requesting authorities (FBI, NSA, CIA, etc.) will have to submit a draft application to lawyers at the National Security Department of the Department of Justice who will scrutinise it and, if necessary, request additional information.[94] Once the application has been finalised, it will have to be approved by the Attorney General, Deputy Attorney General or the Assistant Attorney General for National Security.[95] The Department of Justice will then submit the application to the FISC that will assess the application and make a

87 See 50 U.S.C. § 1881a(l)(1).

88 See USA FREEDOM Act of 2015, Pub. L. No. 114-23, Sec. 602(a). In addition, according to Sec 402, "the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion."

89 USA FREEDOM Act, Sec. 602(a), 603(a).

90 For certain types of surveillance, alternatively a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States may have the power to hear applications and grant orders.

91 The FISC is comprised of eleven judges appointed by the Chief Justice of the United States from among sitting U.S. district court judges, who previously have been appointed by the President and confirmed by the Senate. The judges have life tenure, can only be removed for good cause and serve on the FISC for staggered seven-year terms. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits. See Sec 103 FISA (50 U.S.C. 1803 (a)); PCLOB, Sec. 215 Report, pp. 174-187. The judges are supported by experienced judicial law clerks that constitute the court's legal staff and prepare legal analysis on collection requests. See PCLOB, Sec. 215 Report, p. 178; Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (July 29, 2013) ("Walton Letter"), pp. 2-3.

92 The FISCR is composed of three judges appointed by the Chief Justice of the United States and drawn from U.S. district courts or courts of appeals, serving for a staggered seven year term. See Sec. 103 FISA (50 U.S.C. § 1803 (b)).

93 See 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

94 For instance, additional factual details about the target of the surveillance, technical information about the surveillance methodology, or assurances about how the information acquired will be used and disseminated. See PCLOB, Sec. 215 Report, p. 177.

95 50 U.S.C. §§ 1804 (a), 1801 (g).

preliminary determination on how to proceed.[96] Where a hearing takes place, the FISC has the authority to take testimony which may include expert advice.[97]

(90) The FISC (and FISCR) are supported by a standing panel of five individuals that have an expertise in national security matters as well as civil liberties.[98] From this group the court shall appoint an individual to serve as *amicus curiae* to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate.[99] This shall in particular ensure that privacy considerations are properly reflected in the court's assessment. The court may also appoint an individual or organisation to serve as *amicus curiae*, including providing technical expertise, whenever it deems this appropriate or, upon motion, permit an individual or organisation leave to file an *amicus curiae* brief.[100]

(91) As regards the two legal authorisations for surveillance under FISA that are most important for data transfers under the EU-U.S. Privacy Shield, oversight by the FISC differs.

(92) Under Section 501 FISA[101], which allows the collection of "any tangible things (including books, records, papers, documents, and other items)", the application to the FISC must contain a statement of facts showing that there are reasonable grounds to believe that the tangible things sought for are relevant to an authorised investigation (other than a threat assessment) conducted to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Also, the application must contain an enumeration of the minimisation procedures adopted by the Attorney General for the retention and dissemination of the collected intelligence. [102]

(93) Conversely, under Section 702 FISA[103], the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence. Section 702 FISA allows the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[104] Such targeting is carried out by the NSA in two steps: First, NSA analysts will identify non-U.S. persons located abroad whose surveillance will lead, based on the analysts' assessment, to the relevant foreign intelligence

---

96 The FISC may approve the application, request further information, determine the necessity of a hearing or indicate a possible denial of the application. On the basis of this preliminary determination, the government will make its final application. The latter may include substantial changes to the original application on the basis of the judge's preliminary comments. Although a large percentage of final applications are approved by the FISC, a substantial part of these contain substantive changes to the original application, e.g. 24% of applications approved for the period from July to September 2013. See PCLOB, Sec. 215 Report, p.179; Walton Letter, p. 3.

97 PCLOB, Sec. 215 Report, p.179, n. 619.

98 50 U.S.C. § 1803 (i)(1),(3)(A). This new legislation implemented recommendations by the PCLOB to establish a pool of privacy and civil liberties experts that can serve as *amicus curiae*, in order to provide the court with legal arguments to the advancement of privacy and civil liberties. See PCLOB, Sec. 215 Report, pp. 183-187.

99 50 U.S.C. § 1803 (i)(2)(A). According to information by the ODNI, such appointments have already taken place. See Signals Intelligence Reform, 2016 Progress Report.

100 50 U.S.C. § 1803 (i)(2)(B).

101 50 U.S.C. § 1861

102 50 U.S.C. § 1861 (b).

103 50 U.S.C. § 1881.

104 50 U.S.C. § 1881a (a).

specified in the certification. Second, once these individualised persons have been identified and their targeting has been approved by an extensive review mechanism within the NSA[105], selectors identifying communication facilities (such as email addresses) used by the targets will be "tasked".[106] As indicated, the certifications to be approved by the FISC contain no information about the individual persons to be targeted but rather identify categories of foreign intelligence information.[107] While the FISC does not assess – under a probable cause or any other standard – that individuals are properly targeted to acquire foreign intelligence information,[108] its control extends to the condition that "a significant purpose of the acquisition is to obtain foreign intelligence information"[109]. Indeed, under Section 702 FISA, the NSA is allowed to collect communications of non-U.S. persons outside the U.S. only if it can be reasonably believed that a given means of communication is being used to communicate foreign intelligence information (e.g. related to international terrorism, nuclear proliferation or hostile cyber activities). Determinations to this effect are subject to judicial review.[110] Certifications also need to provide for targeting and minimization procedures.[111] The Attorney General and the Director of National Intelligence verify compliance and the agencies have the obligation to report any incidents of non-compliance to the FISC[112] (as well as the Congress and the President's Intelligence Oversight Board), which on this basis can modify the authorisation.[113]

(94) Furthermore, to increase the efficiency of the oversight by the FISC, the U.S. Administration has agreed to implement a recommendation by the PCLOB to supply to the FISC documentation of Section 702 targeting decisions, including a random sample of tasking sheets, so as to allow the FISC to assess how the foreign intelligence purpose requirement is being met in practice.[114] At the same time, the U.S.

---

105 PCLOB, Sec. 702 Report, p. 46.

106 50 U.S.C. § 1881a (h).

107 50 U.S.C. § 1881a (g). According to the PCLOB, these categories have so far mainly concerned international terrorism and topics such as the acquisition of weapons of mass destruction. See PCLOB, Sec. 702 Report, p. 25.

108 PCLOB, Sec. 702 Report, p. 27.

109 50 U.S.C. § 1881a.

110 "Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12.12.2013, p. 152.

111 50 U.S.C.1881a (i).

112 Rule 13(b) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented in a manner that does not comply with the Court's authorization or approval, or with applicable law. It also requires the government to notify the Court in writing of the facts and circumstances relevant to such non-compliance. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. See Walton Letter, p. 10.

113 50 U.S.C. § 1881 (l). See also PCLOB, Sec. 702 Report, pp. 66-76; NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.04.2014. The collection of personal data for intelligence purposes under Sec 702 FISA is subject to both internal and external oversight within the executive branch. Among others, the internal oversight includes internal compliance programs to evaluate and oversee compliance with targeting and minimization procedures; reporting of non-compliance incidents, both internally and externally to the ODNI, Department of Justice, Congress and the FISC; and annual reviews sent to the same bodies. As for external oversight, it mainly consists in targeting and minimization reviews conducted by the ODNI, DOJ and Inspectors General, which in turn report to Congress and the FISC, including on non-compliance incidents. Significant compliance incidents must be reported to the FISC immediately, others in a quarterly report. See PCLOB, Sec. 702 Report, pp. 66-77.

114 PCLOB, Recommendations Assessment Report, 29.01.2015, p. 20.

Administration accepted and has taken measures to revise NSA targeting procedures to better document the foreign intelligence reasons for targeting decisions.[115]

Individual redress

(95) A number of avenues are available under U.S. law to EU data subjects if they have concerns whether their personal data have been processed (collected, accessed, etc.) by U.S. Intelligence Community elements, and if so, whether the limitations applicable in U.S. law have been complied with. These relate essentially to three areas: interference under FISA; unlawful, intentional access to personal data by government officials; and access to information under Freedom of Information Act (FOIA).[116]

(96) First, the Foreign Intelligence Surveillance Act provides a number of remedies, available also to non-U.S. persons, to challenge unlawful electronic surveillance. This includes the possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed (18 U.S.C. § 2712); to sue U.S. government officials in their personal capacity ("under colour of law") for money damages (50 U.S.C. § 1810); and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States (50 U.S.C. § 1806).[117]

(97) Second, the U.S. government referred the Commission to a number of additional avenues that EU data subjects could use to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes (i.e. the Computer Fraud Abuse Act, 18 U.S.C. § 1030; Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712; and Right to Financial Privacy Act, 12 U.S.C. § 3417). All of these causes of action concern specific data, targets and/or types of access (e.g. remote access of a Computer via the Internet) and are available under certain conditions (e.g. intentional/wilful conduct, conduct outside of official capacity, harm suffered).[118]

(98) Finally, the U.S. government has pointed to the FOIA as a means for non-U.S. persons to seek access to existing federal agency records, including where these contain the individual's personal data (5 U.S.C. § 552).[119] Given its focus, the FOIA does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. Even in this respect the possibilities appear to be limited as agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations.[120] This being

---

115 PCLOB, Recommendations Assessment Report, 29.01.2015, p.16.

116 In addition, Sec. 10 of the Classified Information Procedures Act provides that, in any prosecution in which the United States must establish that material constitutes classified information (e.g. because it requires protection against unauthorized disclosure for reasons of national security), the United States shall notify the defendant of the portions of the material that it reasonably expects to rely upon to establish the classified information element of the offense.

117 ODNI Representations (Annex VI), p. 16.

118 ODNI Representations (Annex VI), p. 17.

119 Similar laws exist at State level.

120 If this is the case, the individual will normally only receive a standard reply by which the agency declines either to confirm or deny the existence of any records. See *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

said, the use of such exceptions by national intelligence agencies can be challenged by individuals who can seek both administrative and judicial review.

(99) While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available courses of action are limited[121] and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing"[122], which restricts access to ordinary courts.[123]

(100) In order to provide for an additional avenue accessible for all EU data subjects, the U.S. government has decided to create a new mechanism, the Privacy Shield Ombudsperson, as set out in the letter from the U.S. Secretary of State to the Commission which is contained in Annex III to this decision. This mechanism builds on the designation, under PPD-28, of a Senior Coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond. In particular, according to the binding commitments from the U.S. government, the Privacy Shield Ombudsperson will guarantee that individual complaints are investigated and individuals receive independent confirmation that U.S. laws have been complied with or, in case of a violation of such laws, the non-compliance has been remedied.

(101) This mechanism contributes to ensuring individual redress and independent oversight.

(102) First, differently from a pure government-to-government mechanism, the Privacy Shield Ombudsperson will receive and respond to individual complaints. Such complaints can be addressed to the Member States bodies competent for the oversight of national security services and, eventually, a centralised EU individual complaint handling body that will channel them to the Privacy Shield Ombudsperson.[124] This will in fact benefit EU data subjects who can turn to a national (as well as a European) body 'close to home' and in their own language. It will be the task of such body to support the individual in making a request to the Privacy Shield Ombudsperson that contains the basic information and thus can be considered "complete". Importantly, the

---

121 See ODNI Representations (Annex VI), p. 16. According to the explanations provided, the available courses of action either require the existence of *damage* (18 U.S.C. § 2712; 50 U.S.C. § 1810) or a showing that the *government intends to use or disclose information* obtained or derived from electronic surveillance of the person concerned against that person *in judicial or administrative proceedings* in the United States (50 U.S.C. § 1806). However, as the Court of Justice has repeatedly stressed, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the person concerned has suffered any adverse consequences on account of that interference. See *Schrems*, paragraph 89 with further references.

122 This admissibility criterion stems from the 'case or controversy' requirement of the U.S. Const., Art. III.

123 See *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). As regards the use of NSLs, the USA FREEDOM Act (Sec. 502(f)-503) provides that non-disclosure requirements must be periodically reviewed, and that *recipients* of NSL be notified when the facts no longer support a non-disclosure requirement (see ODNI Representations (Annex VI), p. 13). However, this does not ensure that the *EU data subject* would be informed that (s)he has been the target of an investigation.

124 According to the Ombudsperson Mechanism (Annex III), Sec. 4(f), the Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of the "underlying processes" that may provide the requested relief (e.g. a FOIA access request, see Sec. 5), those communications will take place in accordance with the applicable procedures.

individual does not have to demonstrate that his/her personal data has in fact been accessed by the U.S. government through signals intelligence activities.

(103) Second, in carrying out her functions, the Privacy Shield Ombudsperson will be able to rely on the independent oversight and compliance review mechanisms existing in U.S. law that involve bodies with the power to investigate the respective request and address non-compliance, such as the Inspector Generals and Civil Liberties and Privacy Officers.[125] Also, the Privacy Shield Ombudsperson will be able to refer matters to the PCLOB for its consideration.[126]

(104) Finally, the Privacy Shield Ombudsperson will be independent and thus free from instructions by the U.S. Intelligence Community. This is of significant importance, given that the Ombudsperson will have to "confirm" that the complaint has been properly investigated and that U.S. law – including the limitations and safeguards set out in the representations by the ODNI – has been complied with or, in the event of non-compliance, such violation has been remedied.[127] In order to be able to provide that independent confirmation, the Privacy Shield Ombudsperson will have to receive sufficient information to make an own assessment, both as regards the investigation carried out and the compliance of the respective national intelligence activities with U.S. law.

(105) The Commission therefore concludes that the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield.

3.2. Access and use by U.S. public authorities for law enforcement and public interest purposes

(106) As regards interference with personal data transferred under the EU-U.S. Privacy Shield for law enforcement purposes, the U.S. government (through the Department of Justice) has provided assurance on the applicable limitations and safeguards which in the Commission's assessment demonstrate an adequate level of protection.

(107) According to this information, under the Fourth Amendment of the U.S. Constitution searches and seizures by law enforcement authorities principally require a court-ordered warrant upon a showing of "probable cause". In the few specifically established and exceptional cases where the warrant requirement does not apply[128],

[125] See Ombudsperson Mechanism (Annex III), Sec. 2(a). See also recitals (80)-(81).

[126] See Ombudsperson Mechanism (Annex III), Sec. 2(c). According to the explanations provided by the U.S. government, the PCLOB shall continually review the policies and procedures, as well as their implementation, of those U.S. authorities responsible for counterterrorism to determine whether their actions "appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties." It also shall "receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities."

[127] Given that the Privacy Shield Ombudsperson "will neither confirm nor deny whether the individual has been the target of surveillance" (nor the specific remedy that was applied), the Commission considers that the caveat that any response will be "subject to the continuing obligation to protect information under applicable laws and policies" will not undermine the obligation to provide an appropriate response. The Commission will monitor, including through the Annual Joint Review, that this is indeed the case.

[128] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

law enforcement is subject to a "reasonableness" test.[129] Whether a search or seizure is reasonable is "determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[130] More generally, the Fourth Amendment guarantees privacy, dignity, and protects against arbitrary and invasive acts by officers of the Government.[131] These concepts capture the idea of necessity and proportionality in Union law.

(108) While the protection under the Fourth Amendment does not extend to non-U.S. persons that are not resident in the United State, the latter nevertheless benefit indirectly through the protection afforded to the U.S. companies holding the personal data and who are the recipients of law enforcement requests. Further protections are provided by special statutory authorities, as well as the Department of Justice Guidelines which limit law enforcement access to data on grounds equivalent to necessity and proportionality (e.g. by requiring that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties).[132] According to the representations made by the U.S. government, the same or higher protections apply to law enforcement investigations at State level (with respect to investigations carried out under State laws).[133]

(109) Although a prior judicial authorisation by a court or grand jury (an investigate arm of the court impanelled by a judge or magistrate) is not required in all cases[134], administrative subpoenas are limited to specific cases and will be subject to independent judicial review at least where the government seeks enforcement in court.[135]

(110) The same applies for the use of administrative subpoenas for public interest purposes. In addition, according to the representations from the U.S. government, similar substantive limitations apply in that agencies may only seek access to data that is relevant to matters falling with their scope of authority and have to respect the standard of reasonableness.

(111) The Commission therefore concludes that there are rules in place in the United States designed to limit any interference for law enforcement or other public interest purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question, and that ensure effective legal protection against such interference.

---

129 PCLOB, Sec. 215 Report, p. 107, referring to *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

130 PCLOB, Sec. 215 Report, p.107, referring to *Samson v. California*, 547 U.S. 843, 848 (2006).

131 *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

132 DOJ Representations (Annex VII), p. 4 with further references.

133 DOJ Representations (Annex VII), n. 2.

134 According to the information the Commission has received, and leaving aside specific areas likely not relevant for data transfers under the EU-U.S. Privacy Shield (e.g. investigations into health care fraud, child abuse or controlled substances cases), this concerns mainly certain authorities under the Electronic Communications Privacy Act (ECPA), namely requests for subscriber information (18 U.S.C. § 2703(c)(1)) and for the content of emails more than 180 days old (18 U.S.C. § 2703(b)). In the latter case, however, the individual concerned has to be notified and thus has the opportunity to challenge the request in court. See *Bignami*, The U.S. legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens, p.18.

135 According to the representations by the U.S. government, recipients of administrative subpoenas may challenge them in court on the grounds that they are unreasonable, i.e. overboard, oppressive of burdensome. See DOJ Representations (Annex VII), p. 2.

4. Adequate level of protection under the EU-U.S. Privacy Shield

(112) In the light of the those findings, the Commission considers that the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield.

(113) In particular, the Commission considers that the Privacy Principles issued by the U.S. Department of Commerce as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the basic principles laid down in Directive 95/46.

(114) In addition, the effective application of the Privacy Principles is guaranteed by the transparency obligations and the administration of the Privacy Shield by the Department of Commerce.

(115) Moreover, the Commission considers that, taken as a whole, the oversight and recourse mechanisms provided for by the Privacy Shield enable infringements of the Privacy Principles by Privacy Shield organisations to be identified and punished in practice and offer legal remedies to the data subject to gain access to personal data relating to him and, eventually, to obtain the rectification or erasure of such data.

(116) Finally, on the basis of the available information about the U.S. legal order, including the representations and assurances from the U.S. government, the Commission considers that any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Privacy Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference. The Commission concludes that this meets the standards of Article 25 of Directive 95/46/EC, interpreted in light of the Charter of Fundamental Rights of the European Union, as explained by the Court of Justice in particular in the *Schrems* judgment.

5. Action of Data Protection Authorities and information to the Commission

(117) In the *Schrems* judgment, the Court of Justice clarified that the Commission has no competence to restrict the powers that DPAs derive from Article 28 of Directive 95/46 (including the power to suspend data transfers) where a person, in bringing a claim under that provision, calls into question the compatibility of a Commission adequacy decision with the protection of the fundamental right to privacy and data protection.[136]

(118) In order to effectively monitor the functioning of the Privacy Shield, the Commission should be informed by Member States about relevant action undertaken by DPAs.

(119) The Court of Justice furthermore considered that, in line with the second subparagraph of Article 25(6) of Directive 95/46, Member States and their organs must take the measures necessary to comply with acts of the Union institutions, as the latter are in principle presumed to be lawful and accordingly produce legal effects until such time

[136] *Schrems*, paragraphs 40 et seq., 101-103.

as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality. Consequently, a Commission adequacy decision adopted pursuant to Article 25(6) of Directive 95/46 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities.[137] Where such an authority has received a complaint putting in question the compliance of a Commission adequacy decision with the protection of the fundamental right to privacy and data protection and considers the objections advanced to be well founded, national law must provide it with a legal remedy to put those objections before a national court which, in case of doubts, must stay proceedings and make a reference for a preliminary ruling to the Court of Justice.[138]

6. Periodic review of adequacy finding

(120) In the light of the fact that the level of protection afforded by the U.S. legal order may be liable to change, the Commission, following adoption of this decision, will check periodically whether the finding relating to the adequacy of the level of protection ensured by the EU-U.S. Privacy Shield is still factually and legally justified. Such a check is required, in any event, when the Commission acquires any information giving rise to a justified doubt in that regard.[139]

(121) Therefore, the Commission will continuously monitor the overall framework for the transfer of personal data created by the EU-U.S. Privacy Shield as well as compliance by U.S. authorities with the representations and commitments contained in the documents attached to this decision. Moreover, this decision will be subject to an Annual Joint Review which will cover all aspects of the functioning of the EU-U.S. Privacy Shield, including the operation of the national security and law enforcement exceptions to the Privacy Principles.

(122) To perform the Annual Joint Review referred to in Annexes I, II and VI, the Commission will meet with the Department of Commerce and FTC, accompanied, if appropriate, by other departments and agencies involved in the implementation of the Privacy Shield arrangements, as well as, for matters pertaining to national security, representatives of the ODNI, other Intelligence Community elements and the Ombudsperson. The participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party.

(123) In the framework of the Annual Joint Review, the Commission will request that the Department of Commerce provides comprehensive information on all relevant aspects of the functioning of the EU-U.S. Privacy Shield, including referrals received by the Department of Commerce from DPAs and the results of *ex officio* compliance reviews. The Commission will also seek explanations concerning any questions or matters concerning the EU-U.S. Privacy Shield and its operation arising from any information available, including transparency reports allowed under the USA FREEDOM Act, public reports by U.S. national intelligence authorities, the DPAs, privacy groups, media reports, or any other possible source. Moreover, in order to facilitate the Commission's task in this regard, the Member States should inform the Commission of

[137] *Schrems*, paragraphs 51, 52 and 62.
[138] *Schrems*, paragraph 65.
[139] *Schrems*, paragraph 76.

cases where the actions of bodies responsible for ensuring compliance with the Privacy Principles in the United States fail to secure compliance and of any indications that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection.

(124) On the basis of the annual joint review, the Commission will prepare a public report to be submitted to the European Parliament and the Council.

7. Suspension of the adequacy decision

(125) Where, on the basis of the checks or of any other information available, the Commission concludes that there are clear indications that effective compliance with the Privacy Principles in the United States might no longer be ensured, or that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection, it will inform the Department of Commerce thereof and request that appropriate measures are taken to swiftly address any potential non-compliance with the Privacy Principles within a specified, reasonable timeframe. If, after the expiration of the specified timeframe, the U.S. authorities fail to demonstrate satisfactorily that the EU-U.S. Privacy Shield continues to guarantee effective compliance and an adequate level of protection, the Commission will initiate the procedure leading to the partial or complete suspension or repeal of this decision.[140] Alternatively, the Commission may propose to amend this decision, for instance by limiting the scope of the adequacy finding only to data transfers subject to additional conditions.

(126) In particular, the Commission will initiate the procedure for suspension or repeal in case of:

(a) indications that the U.S. authorities do not comply with the representations and commitments contained in the documents annexed to this decision, including as regards the conditions and limitations for access by U.S. public authorities for law enforcement, national security and other public interest purposes to personal data transferred under the Privacy Shield;

(b) failure to effectively address complaints by EU data subjects; in this respect, the Commission will take into account all circumstances having an impact on the possibility for EU data subjects to have their rights enforced, including, in particular, the voluntary commitment by self-certified U.S. companies to cooperate with the DPAs and follow their advice; or

(c) failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects.

[140] As of the date of application of the General Data Protection Regulation, the Commission will make use of its powers to adopt, on duly justified imperative grounds of urgency, an implementing act suspending the present decision which shall apply immediately without its prior submission to the relevant comitology committee and shall remain in force for a period not exceeding six months

(127) The Commission will also consider to initiate the procedure leading to the amendment, suspension, or repeal of this decision if, in the context of the Annual Joint Review of the functioning of the EU-U.S. Privacy Shield or otherwise, the Department of Commerce or other departments or agencies involved in the implementation of the Privacy Shield, or, for matters pertaining to national security, representatives of the U.S. Intelligence Community or the Ombudsperson, fail to provide information or clarifications necessary for the assessment of compliance with the Privacy Principles, the effectiveness of complaint handling procedures, or any lowering of the required level of protection as a consequence of actions by U.S. national intelligence authorities, in particular as a consequence of the collection and/or access to personal data that is not limited to what is strictly necessary and proportionate. In this respect, the Commission will take into account the extent to which the relevant information can be obtained from other sources, including through reports from self-certified U.S. companies as allowed under the USA FREEDOM Act.

(128) [The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46 has delivered a favourable opinion on the adequate level of protection provided by the United States for personal data transferred under the EU-U.S. Privacy Shield from the European Union to self-certified organisations in the United States[141], which has been taken into account in the preparation of this Decision.]

(129) [The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31(1) of Directive 95/46[142],]

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.

2. The EU-U.S. Privacy Shield is constituted by the Privacy Principles issued by the U.S. Department of Commerce on [Date] as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I, III to VII.

3. For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the "Privacy Shield List", maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Privacy Principles set out in Annex II.

[141] [Reference]
[142] [Reference]

Article 2

This Decision does not affect the application of the provisions of Directive 95/46/EC other than Article 25(1) that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

Article 3

Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive 95/46/EC leading to the suspension or definitive ban of data flows to an organisation in the United States that is included in the Privacy Shield List in accordance with Sections I and III of the Privacy Principles set out in Annex II in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall inform the Commission without delay.

Article 4

1. The Commission will continuously monitor the functioning of the EU-U.S. Privacy Shield with a view to assessing whether the United States continues to ensure an adequate level of protection of personal data transferred thereunder from the Union to organisations in the United States.

2. The Member States and the Commission shall inform each other of cases where it appears that the government bodies in the United States with the statutory power to enforce compliance with the Privacy Principles set out in Annex II fail to provide effective detection and supervision mechanisms enabling infringements of the Privacy Principles to be identified and punished in practice.

3. The Member States and the Commission shall inform each other of any indications that the interferences by U.S. public authorities responsible for national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go beyond what is strictly necessary, and/or that there is no effective legal protection against such interferences.

4. Within one year from the date of the notification of this Decision to the Member States and on a yearly basis thereafter, the Commission will evaluate the finding in Article 1(1) on the basis of all available information, including the information received as part of the Annual Joint Review referred to in Annexes I, II and VI.

5. The Commission will report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC.

6. The Commission will present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC with a view to suspending, amending or repealing this Decision or limiting its scope, among others, where there are indications:

– that the U.S. public authorities do not comply with the representations and commitments contained in the documents annexed to this Decision, including as regards the conditions

and limitations for access by U.S. public authorities for law enforcement, national security and other public interest purposes to personal data transferred under the EU-U.S. Privacy Shield;

– of a systematic failure to effectively address complaints by EU data subjects; or

– of a systematic failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects in accordance with his functions as set out in Annex III.

The Commission will also present such draft measures if the lack of cooperation of the bodies involved in ensuring the functioning of the EU-U.S. Privacy Shield in the United States prevents the Commission from determining whether the finding in Article 1(1) is affected.

Article 5

Member States shall take all the measures necessary to comply with this Decision.

Article 6

This Decision is addressed to the Member States.

Done at Brussels,

For the Commission
[…]

Member of the Commission

ANNEXES

ANNEX I: Letter from U.S. Secretary of Commerce Penny Pritzker
Annex 1: Letter from Under Secretary for International Trade Stefan Selig
ANNEX II: EU-U.S. Privacy Shield Principles
Annex I: Arbitral Model
ANNEX III: Letter from U.S. Secretary of State John Kerry
Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism
ANNEX IV: Letter from Federal Trade Commission Chairwoman Edith Ramirez
ANNEX V: Letter from U.S. Secretary of Transportation Anthony Foxx
ANNEX VI: Letter from General Counsel Robert Litt, Office of the Director of National Intelligence
ANNEX VII: Letter from Deputy Assistant Attorney General Bruce Swartz, U.S. Department of Justice

ANNEX I

UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

February 23, 2016

Ms. Věra Jourová
Commissioner for Justice, Consumers
and Gender Equality
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Privacy Shield materials that is the product of two years of productive discussions among our teams. This package, along with other materials available to the Commission from public sources, provides a very strong basis for a new adequacy finding by the European Commission.

We should both be proud of the improvements to the Framework. The Privacy Shield is based on Principles that have strong consensus support on both sides of the Atlantic, and we have strengthened their operation. Through our work together, we have the real opportunity to improve the protection of privacy around the world.

The Privacy Shield Package includes the Privacy Shield Principles, along with a letter, attached as Annex 1, from the International Trade Administration (ITA) of the Department of Commerce, which administers the program, describing the commitments that our Department has made to ensure that the Privacy Shield operates effectively. The Package also includes Annex 2, which includes other Department of Commerce commitments relating to the new arbitral model available under the Privacy Shield.

I have directed my staff to devote all necessary resources to implement the Privacy Shield Framework expeditiously and fully and to ensure the commitments in Annex 1 and Annex 2 are met in a timely fashion.

The Privacy Shield Package also includes other documents from other United States agencies, namely:

- A letter from the Federal Trade Commission (FTC) describing its enforcement of the Privacy Shield;
- A letter from the Department of Transportation describing its enforcement of the Privacy Shield;

- A letter prepared by the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to U.S. national security authorities;
- A letter from the Department of State and accompanying memorandum describing the State Department's commitment to establish a new Privacy Shield Ombudsperson for submission of inquiries regarding the United States' signals intelligence practices; and
- A letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

You can be assured that the United States takes these commitments seriously.

Within 30 days of final approval of the adequacy determination, the full Privacy Shield Package will be delivered to the *Federal Register* for publication.

We look forward to working with you as the Privacy Shield is implemented and as we embark on the next phase of this process together.

Sincerely,

Penny Pritzker

FEB 2 3 2016

UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for International Trade
Washington, D.C. 20230

The Honorable Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

On behalf of the International Trade Administration, I am pleased to describe the enhanced protection of personal data that the EU-U.S. Privacy Shield Framework ("Privacy Shield" or "Framework") provides and the commitments the Department of Commerce ("Department") has made to ensure that the Privacy Shield operates effectively. Finalizing this historic arrangement is a major achievement for privacy and for businesses on both sides of the Atlantic. It offers confidence to EU individuals that their data will be protected and that they will have legal remedies to address any concerns. It offers certainty that will help grow the transatlantic economy by ensuring that thousands of European and American businesses can continue to invest and do business across our borders. The Privacy Shield is the result of over two years of hard work and collaboration with you, our colleagues in the European Commission ("Commission"). We look forward to continuing to work with the Commission to ensure that the Privacy Shield functions as intended.

We have worked with the Commission to develop the Privacy Shield to allow organizations established in the United States to meet the adequacy requirements for data protection under EU law. The new Framework will yield several significant benefits for both individuals and businesses. First, it provides an important set of privacy protections for the data of EU individuals. It requires participating U.S. organizations to develop a conforming privacy policy, publicly commit to comply with the Privacy Shield Principles so that the commitment becomes enforceable under U.S. law, annually re-certify their compliance to the Department, provide free independent dispute resolution to EU individuals, and be subject to the authority of the U.S. Federal Trade Commission ("FTC"), Department of Transportation ("DOT"), or another enforcement agency. Second, the Privacy Shield will enable thousands of companies in the United States and subsidiaries of European companies in the United States to receive personal data from the European Union to facilitate data flows that support transatlantic trade. The transatlantic economic relationship is already the world's largest, accounting for half of global economic output and nearly one trillion dollars in goods and services trade, supporting millions of jobs on both sides of the Atlantic. Businesses that rely on transatlantic data flows come from all industry sectors and include major Fortune 500 firms as well as many small and medium-sized enterprises (SMEs). Transatlantic data flows allow U.S. organizations to process data required to offer goods, services, and employment opportunities to European individuals. The Privacy Shield supports shared privacy principles, bridging the differences in our legal approaches, while furthering trade and economic objectives of both Europe and the United States.

INTERNATIONAL TRADE ADMINISTRATION

While a company's decision to self-certify to this new Framework will be voluntary, once a company publicly commits to the Privacy Shield, its commitment is enforceable under U.S. law by either the Federal Trade Commission or Department of Transportation, depending on which authority has jurisdiction over the Privacy Shield organization.

Enhancements under the Privacy Shield Principles

The resulting Privacy Shield strengthens the protection of privacy by:

- requiring additional information be provided to individuals in the Notice Principle, including a declaration of the organization's participation in the Privacy Shield, a statement of the individual's right to access personal data, and the identification of the relevant independent dispute resolution body;
- strengthening protection of personal data that is transferred from a Privacy Shield organization to a third party controller by requiring the parties to enter into a contract 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;
- strengthening protection of personal data that is transferred from a Privacy Shield organization to a third party agent, including by requiring a Privacy Shield organization to: 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; upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request;
- providing that a Privacy Shield organization is responsible for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf, and that the Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage;
- clarifying that Privacy Shield organizations must limit personal information to the information that is relevant for the purposes of processing;
- requiring an organization to annually certify with the Department its commitment to apply the Principles to information it received while it participated in the Privacy Shield if it leaves the Privacy Shield and chooses to keep such data;
- requiring that independent recourse mechanisms be provided at no cost to the individual;
- requiring organizations and their selected independent recourse mechanisms to respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield;
- requiring organizations to respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department; and
- requiring a Privacy Shield organization to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC if it becomes subject to an FTC or court order based on non-compliance.

Administration and Supervision of the Privacy Shield Program by the Department of Commerce

The Department reiterates its commitment to maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles (the "Privacy Shield List"). The Department will keep the Privacy Shield List up to date by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the Department's procedures, or are found to persistently fail to comply. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List, including those that were removed for persistent failure to comply with the Principles. The Department will identify the reason each organization was removed.

In addition, the Department commits to strengthening the administration and supervision of the Privacy Shield. Specifically, the Department will:

Provide Additional Information on the Privacy Shield Website

- maintain the Privacy Shield List, as well as a record of those organizations that previously self-certified their adherence to the Principles, but which are no longer assured of the benefits of the Privacy Shield;
- include a prominently placed explanation clarifying that all organizations removed from the Privacy Shield List are no longer assured of the benefits of the Privacy Shield, but must nevertheless continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield for as long as they retain such information; and
- provide a link to the list of Privacy Shield-related FTC cases maintained on the FTC website.

Verify Self-Certification Requirements

- prior to finalizing an organization's self-certification (or annual re-certification) and placing an organization on the Privacy Shield List, verify that the organization has:

    - provided required organization contact information;
    - described the activities of the organization with respect to personal information received from the EU;
    - indicated what personal information is covered by its self-certification;
    - if the organization has a public website, provided the web address where the privacy policy is available and the privacy policy is accessible at the web address provided, or if an organization does not have a public website, provided where the privacy policy is available for viewing by the public;
    - included in its relevant privacy policy a statement that it adheres to the Principles and if the privacy policy is available online, a hyperlink to the Department's Privacy Shield website;

- identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- if the organization elects to satisfy the requirements in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the appropriate EU data protection authorities ("DPAs"), indicated its intention to cooperate with DPAs in the investigation and resolution of complaints brought under the Privacy Shield, notably to respond to their inquiries when EU data subjects have brought their complaints directly to their national DPAs;
- identified any privacy program in which the organization is a member;
- identified the method of verification of assuring compliance with the Principles (*e.g.*, in-house, third party);
- identified, both in its self-certification submission and in its privacy policy, the independent recourse mechanism that is available to investigate and resolve complaints;
- included in its relevant privacy policy, if the policy is available online, a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints; and
- if the organization has indicated that it intends to receive human resources information transferred from the EU for use in the context of the employment relationship, declared its commitment to cooperate and comply with DPAs to resolve complaints concerning its activities with regard to such data, provided the Department with a copy of its human resources privacy policy, and provided where the privacy policy is available for viewing by its affected employees.

- work with independent recourse mechanisms to verify that the organizations have in fact registered with the relevant mechanism indicated in their self-certification submissions, where such registration is required.

Expand Efforts to Follow Up with Organizations That Have Been Removed from the Privacy Shield List

- notify organizations that are removed from the Privacy Shield List for "persistent failure to comply" that they are not entitled to retain information collected under the Privacy Shield; and
- send questionnaires to organizations whose self-certifications lapse or who have voluntarily withdrawn from the Privacy Shield 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, and if personal information will be retained, verify who within the organization will serve as an ongoing point of contact for Privacy Shield-related questions.

Search for and Address False Claims of Participation

- review the privacy policies of organizations that have previously participated in the Privacy Shield program, but that have been removed from the Privacy Shield List to identify any false claims of Privacy Shield participation;
- on an ongoing basis, when an organization: (a) withdraws from participation in the Privacy Shield, (b) fails to recertify its adherence to the Principles, or (c) is removed as a participant in the Privacy Shield notably for "persistent failure to comply," undertake, on an *ex officio* basis, to verify that the organization has removed from any relevant published privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits. Where the Department finds that such references have not been removed, the Department will warn the organization that the Department will, as appropriate, refer matters to the relevant agency for potential enforcement action if it continues to make the claim of Privacy Shield certification. If the organization neither removes the references nor self-certifies its compliance under the Privacy Shield, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency or, in appropriate cases, take action to enforce the Privacy Shield certification mark;
- undertake other efforts to identify false claims of Privacy Shield participation and improper use of the Privacy Shield certification mark, including by conducting Internet searches to identify where images of the Privacy Shield certification mark are being displayed and references to Privacy Shield in organizations' privacy policies;
- promptly address any issues that we identify during our *ex officio* monitoring of false claims of participation and misuse of the certification mark, including warning organizations misrepresenting their participation in the Privacy Shield program as described above;
- take other appropriate corrective action, including pursuing any legal recourse the Department is authorized to take and referring matters to the FTC, DOT, or another appropriate enforcement agency; and
- promptly review and address complaints about false claims of participation that we receive.

The Department will undertake reviews of privacy policies of organizations to more effectively identify and address false claims of Privacy Shield participation. Specifically, the Department will review the privacy policies of organizations whose self-certification has lapsed due to their failure to re-certify adherence to the Principles. The Department will conduct this type of review to verify that such organizations have removed from any relevant published privacy policy any references that imply that the organizations continue to actively participate in the Privacy Shield. As a result of these types of reviews, we will identify organizations that have not removed such references and send those organizations a letter from the Department's Office of General Counsel warning of potential enforcement action if the references are not removed. The Department will take follow-up action to ensure that the organizations either remove the inappropriate references or re-certify their adherence to the Principles. In addition, the Department will undertake efforts to identify false claims of Privacy Shield participation by organizations that have never participated in the Privacy Shield program, and will take similar corrective action with respect to such organizations.

Conduct Periodic *ex officio* Compliance Reviews and Assessments of the Program

- on an ongoing basis, monitor effective compliance, including through sending detailed questionnaires to participating organizations, to identify issues that may warrant further follow-up action. In particular, such compliance reviews shall take place when: (a) the Department has received specific non-frivolous complaints about an organization's compliance with the Principles, (b) an organization does not respond satisfactorily to inquiries by the Department for information relating to the Privacy Shield, or (c) there is credible evidence that an organization does not comply with its commitments under the Privacy Shield. The Department shall, when appropriate, consult with the competent data protection authorities about such compliance reviews; and
- assess periodically the administration and supervision of the Privacy Shield program to ensure that monitoring efforts are appropriate to address new issues as they arise.

The Department has increased the resources that will be devoted to the administration and supervision of the Privacy Shield program, including doubling the number of staff responsible for the administration and supervision of the program. We will continue to dedicate appropriate resources to such efforts to ensure effective monitoring and administration of the program.

Tailor the Privacy Shield Website to Targeted Audiences

The Department will tailor the Privacy Shield website to focus on three target audiences: EU individuals, EU businesses, and U.S. businesses. The inclusion of material targeted directly to EU individuals and EU businesses will facilitate transparency in a number of ways. With regard to EU individuals, it will clearly explain: (1) the rights the Privacy Shield provides to EU individuals; (2) the recourse mechanisms available to EU individuals when they believe an organization has breached its commitment to comply with the Principles; and (3) how to find information pertaining to an organization's Privacy Shield self-certification. With regard to EU businesses, it will facilitate verification of: (1) whether an organization is assured of the benefits of the Privacy Shield; (2) the type of information covered by an organization's Privacy Shield self-certification; (3) the privacy policy that applies to the covered information; and (4) the method the organization uses to verify its adherence to the Principles.

Increase Cooperation with DPAs

To increase opportunities for cooperation with DPAs, the Department will establish a dedicated contact at the Department to act as a liaison with DPAs. In instances where a DPA believes that an organization is not complying with the Principles, including following a complaint from an EU individual, the DPA can reach out to the dedicated contact at the Department to refer the organization for further review. The contact will also receive referrals regarding organizations that falsely claim to participate in the Privacy Shield, despite never having self-certified their adherence to the Principles. The contact will assist DPAs seeking information related to a specific organization's self-certification or previous participation in the program, and the contact will respond to DPA inquiries regarding the implementation of specific Privacy Shield requirements. Second, the Department will provide DPAs with material

regarding the Privacy Shield for inclusion on their own websites to increase transparency for EU individuals and EU businesses. Increased awareness regarding the Privacy Shield and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Facilitate Resolution of Complaints about Non-Compliance

The Department, through the dedicated contact, will receive complaints referred to the Department by a DPA that a Privacy Shield organization is not complying with the Principles. The Department will make its best effort to facilitate resolution of the complaint with the Privacy Shield organization. Within 90 days after receipt of the complaint, the Department will provide an update to the DPA. To facilitate the submission of such complaints, the Department will create a standard form for DPAs to submit to the Department's dedicated contact. The dedicated contact will track all referrals from DPAs received by the Department, and the Department will provide in the annual review described below a report analyzing in aggregate the complaints it receives each year.

Adopt Arbitral Procedures and Select Arbitrators in Consultation with the Commission

The Department will fulfill its commitments under Annex I and publish the procedures after agreement has been reached.

Joint Review Mechanism of the Functioning of the Privacy Shield

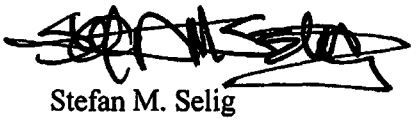
The Department of Commerce, the FTC, and other agencies, as appropriate, will hold annual meetings with the Commission, interested DPAs, and appropriate representatives from the Article 29 Working Party, where the Department will provide updates on the Privacy Shield program. The annual meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield, including referrals received by the Department from DPAs, the results of *ex officio* compliance reviews, and may also include discussion of relevant changes of law.

National Security Exception

With respect to the limitations to the adherence to the Privacy Shield Principles for national security purposes, the General Counsel of the Office of the Director of National Intelligence, Robert Litt, has also sent a letter addressed to Justin Antonipillai and Ted Dean of the Department of Commerce, and this has been forwarded to you. This letter extensively discusses, among other things, the policies, safeguards, and limitations that apply to signals intelligence activities conducted by the U.S. In addition, this letter describes the transparency provided by the Intelligence Community about these matters. As the Commission is assessing the Privacy Shield Framework, the information in this letter provides assurance to conclude that the Privacy Shield will operate appropriately, in accordance with the Principles therein. We understand that you may raise information that has been released publicly by the Intelligence Community, along with other information, in the future to inform the annual review of the Privacy Shield Framework.

On the basis of the Privacy Shield Principles and the accompanying letters and materials, including the Department's commitments regarding the administration and supervision of the Privacy Shield Framework, our expectation is that the Commission will determine that the EU-U.S. Privacy Shield Framework provides adequate protection for the purposes of EU law and data transfers from the European Union will continue to organizations that participate in the Privacy Shield.

Sincerely,



Stefan M. Selig

ANNEX II

EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES
ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

I. OVERVIEW

1. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences and to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries, the Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles (collectively "the Principles") under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission, and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union. They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission's adequacy decision. The Principles do not affect the application of national provisions implementing Directive 95/46/EC ("the Directive") that apply to the processing of personal data in the Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.

2. In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) ("the Department"). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the "FTC"), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles (other U.S. statutory bodies recognized by the EU may be included as an annex in the future); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

3. The Department of Commerce will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Privacy Shield List"). Privacy Shield benefits are assured from the date that the Department places the organization on the Privacy Shield List. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the Department. An organization's removal from the Privacy Shield List means it may no longer benefit from the European Commission's adequacy decision to receive personal information from the EU. The organization must continue to apply the Principles to the personal information it received while it participated in the Privacy Shield, and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide "adequate" protection for the information by another authorized means. The Department will also remove from the Privacy Shield List those organizations that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete the personal information they received under the Privacy Shield.

4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List. The Department will provide a clear warning that these organizations are not participants in the Privacy Shield; that removal from the Privacy Shield List means that such organizations cannot claim to be Privacy Shield compliant and must avoid any statements or misleading practices implying that they participate in the Privacy Shield; and that such organizations are no longer entitled to benefit from the European Commission's adequacy decision that would enable those organizations to receive personal information from the EU. An organization that continues to claim participation in the Privacy Shield or makes other Privacy Shield-related misrepresentations after it has been removed from the Privacy Shield List may be subject to enforcement action by the FTC, the Department of Transportation, or other enforcement authorities.

5. Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is

allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.

7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.

8. Definitions:

   a. "Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.

   b. "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

   c. "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

9. The effective date of the Principles is the date of final approval of the European Commission's adequacy determination.

II. PRINCIPLES

1. NOTICE

a. An organization must inform individuals about:

i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,

ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,

iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,

iv. the purposes for which it collects and uses personal information about them,

v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,

vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

vii. the right of individuals to access their personal data,

viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,

ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,

x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,

xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,

xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

xiii. its liability in cases of onward transfers to third parties.

b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.

c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also 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.

b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the

same level of privacy protection as is required by the Principles; (iii) 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; (iv) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and (v) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

6. ACCESS

a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by

reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

d. In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

e. When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

III. SUPPLEMENTAL PRINCIPLES

1. Sensitive Data

a. An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:

i. in the vital interests of the data subject or another person;

ii. necessary for the establishment of legal claims or defenses;

iii. required to provide medical care or diagnosis;

iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

v. necessary to carry out the organization's obligations in the field of employment law; or

vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

a. Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.

b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Privacy Shield Principles.

3. Secondary Liability

a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Privacy Shield Principles when on behalf of another organization they merely transmit, route, switch, or cache information. As is the case with the Directive itself, the Privacy Shield does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.

b. Public stock corporations and closely held companies, including Privacy Shield organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a Privacy Shield organization involved in a potential merger or takeover will need to perform, or be the subject of, a "due diligence" review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Data Protection Authorities

a. Organizations will implement their commitment to cooperate with European Union data protection authorities ("DPAs") as described below. Under the Privacy Shield, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the DPAs.

b. An organization commits to cooperate with the DPAs by declaring in its Privacy Shield self-certification submission to the Department of Commerce (*see* Supplemental Principle on Self-Certification) that the organization:

i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs;

ii. will cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield; and

iii. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

c. Operation of DPA Panels

i. The cooperation of the DPAs will be provided in the form of information and advice in the following way:

1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will *inter alia* help ensure a harmonized and coherent approach.

2. The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Privacy Shield. This advice will be designed to ensure that the Privacy Shield Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.

3. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for Privacy Shield purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.

4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.

5. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.

6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to refer the matter to the Federal Trade Commission, the Department of Transportation, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce so that the Privacy Shield List can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Privacy Shield Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

d. An organization that wishes its Privacy Shield benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (*see* Supplemental Principle on Human Resources Data).

e. Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed USD 500 and will be less for smaller companies.

6. Self-Certification

a. Privacy Shield benefits are assured from the date on which the Department has placed the organization's self-certification submission on the Privacy Shield List after having determined that the submission is complete.

b. To self-certify for the Privacy Shield, an organization must provide to the Department a self-certification submission, signed by a corporate officer on behalf of the organization that is joining the Privacy Shield, that contains at least the following information:

i. name of organization, mailing address, e-mail address, telephone, and fax numbers;

ii. description of the activities of the organization with respect to personal information received from the EU; and

iii. description of the organization's privacy policy for such personal information, including:

1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public;

2. its effective date of implementation;

3. a contact office for the handling of complaints, access requests, and any other issues arising under the Privacy Shield;

4. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);

5. name of any privacy program in which the organization is a member;

6. method of verification (*e.g.*, in-house, third party) (*see* Supplemental Principle on Verification; and

7. the independent recourse mechanism that is available to investigate unresolved complaints.

c. Where the organization wishes its Privacy Shield benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its self-certification submission and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities as applicable and that it will comply with the advice given by such authorities. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.

d. The Department will maintain the Privacy Shield List of organizations that file completed self-certification submissions, thereby assuring the availability of Privacy Shield benefits, and will update such list on the basis of annual self-recertification submissions and notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such self-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Privacy Shield List and Privacy Shield benefits will

no longer be assured. Both the Privacy Shield List and the self-certification submissions by the organizations will be made publicly available. All organizations that are placed on the Privacy Shield List by the Department must also state in their relevant published privacy policy statements that they adhere to the Privacy Shield Principles. If available online, an organization's privacy policy must include a hyperlink to the Department's Privacy Shield website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.

e. The Privacy Principles apply immediately upon certification. Recognizing that the Principles will impact commercial relationships with third parties, organizations that certify to the Privacy Shield Framework in the first two months following the Framework's effective date shall bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible, and in any event no later than nine months from the date upon which they certify to the Privacy Shield. During that interim period, where organizations transfer data to a third party, they shall (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles.

f. An organization must subject to the Privacy Shield Principles all personal data received from the EU in reliance upon the Privacy Shield. The undertaking to adhere to the Privacy Shield Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the Privacy Shield. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Privacy Shield for any reason. An organization that withdraws from the Privacy Shield but wants to retain such data must affirm to the Department on an annual basis its commitment to continue to apply the Principles or provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission); otherwise, the organization must return or delete the information. An organization that withdraws from the Privacy Shield must remove from any relevant privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits.

g. An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (i) continue to be bound by the Privacy Shield Principles by the operation of law governing the takeover or merger or (ii) elect to self-certify its

adherence to the Privacy Shield Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Privacy Shield Principles. Where neither (i) nor (ii) applies, any personal data that has been acquired under the Privacy Shield must be promptly deleted.

h. When an organization leaves the Privacy Shield for any reason, it must remove all statements implying that the organization continues to participate in the Privacy Shield or is entitled to the benefits of the Privacy Shield. The EU-U.S. Privacy Shield certification mark, if used, must also be removed. Any misrepresentation to the general public concerning an organization's adherence to the Privacy Shield Principles may be actionable by the FTC or other relevant government body. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

a. Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.

b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.

c. Under the self-assessment approach, such verification must indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It must also indicate that its privacy policy conforms to the Privacy Shield Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

d. Where the organization has chosen outside compliance review, such a review must demonstrate that its privacy policy regarding personal information received from the EU conforms to the Privacy Shield Principles, that it is being complied with, and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include, without limitation,

auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

e. Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles.

8. Access

a. The Access Principle in Practice

i. Under the Privacy Shield Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:

1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;[1]

2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and

3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.

ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with or about the nature

[1] The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

of the information or its use that is the subject of the access request.

iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

b. Burden or Expense of Providing Access

i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.

ii. For example, if the personal information is used for decisions that will significantly affect the individual (*e.g.*, the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.

ii. Where confidential commercial information can be readily separated from other personal information subject to an access

request, the organization should redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.

ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

e. When Access May be Restricted

i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the Directive, an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;

2. disclosure where the legitimate rights or important interests of others would be violated;

3. breaching a legal or other professional privilege or obligation;

4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or

5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.

ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.

f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access

i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.

ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.

iii. Access may not be refused on cost grounds if the individual offers to pay the costs.

g. Repetitious or Vexatious Requests for Access

i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

h. Fraudulent Requests for Access

i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

i. Timeframe for Responses

i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. Human Resources Data

a. Coverage by the Privacy Shield

i. Where an organization in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Privacy Shield, the transfer enjoys the benefits of the Privacy Shield. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

ii. The Privacy Shield Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.

b. Application of the Notice and Choice Principles

i. A U.S. organization that has received employee information from the EU under the Privacy Shield may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

iii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

iv. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

c. Application of the Access Principle

i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Privacy Shield requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

d. Enforcement

i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Privacy Shield Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

ii. A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.

e. Application of the Accountability for Onward Transfer Principle

i. For occasional employment-related operational needs of the Privacy Shield organization with respect to personal data transferred under the Privacy Shield, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the Privacy Shield organization has complied with the Notice and Choice Principles.

10. Obligatory Contracts for Onward Transfers

a. Data Processing Contracts

i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.

ii. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in

the Privacy Shield. The purpose of the contract is to make sure that the processor:

1. acts only on instructions from the controller;

2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access, and understands whether onward transfer is allowed; and

3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.

iii. Because adequate protection is provided by Privacy Shield participants, contracts with Privacy Shield participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the EU Member States), as would be required for contracts with recipients not participating in the Privacy Shield or otherwise not providing adequate protection.

b. Transfers within a Controlled Group of Corporations or Entities

i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (*e.g.*, compliance and control programs), ensuring the continuity of protection of personal information under the Privacy Shield Principles. In case of such transfers, the Privacy Shield organization remains responsible for compliance with Privacy Shield Principles.

c. Transfers between Controllers

i. For transfers between controllers, the recipient controller need not be a Privacy Shield organization or have an independent recourse mechanism. The Privacy Shield organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the Privacy Shield, not including the requirement that the third party controller be a Privacy Shield organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. Dispute Resolution and Enforcement

a. The Recourse, Enforcement and Liability Principle sets out the requirements for Privacy Shield enforcement. How to meet the requirements of point (a)(ii) of the Principle is set out in the

Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Privacy Shield Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.

b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts, or another law or regulation prohibiting such acts.

c. In order to help ensure compliance with their Privacy Shield commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the Privacy Shield when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.

d. Recourse Mechanisms

   i. Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to a consumer within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be

transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Privacy Shield Principles. They should also cooperate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

ii. Independent recourse mechanisms must include on their public websites information regarding the Privacy Shield Principles and the services that they provide under the Privacy Shield. This information must include: (1) information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Privacy Shield website; (3) an explanation that their dispute resolution services under the Privacy Shield are free of charge to individuals; (4) a description of how a Privacy Shield-related complaint can be filed; (5) the timeframe in which Privacy Shield-related complaints are processed; and (6) a description of the range of potential remedies.

iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.

iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles[2] or with respect to an allegation about the adequacy of the Privacy Shield. Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return

[2] Section I.5 of the Principles.

of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

i. The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.[3] Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

f. FTC Action

ii. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. This includes false claims of adherence to the Privacy Shield Principles or participation in the Privacy Shield by organizations, which either are no longer

[3] Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Privacy Shield Principles.

on the Privacy Shield List or have never self-certified to the Department. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Privacy Shield Principles.

g. Persistent Failure to Comply

i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the Privacy Shield. Organizations that have persistently failed to comply with the Principles will be removed from the Privacy Shield List by the Department and must return or delete the personal information they received under the Privacy Shield.

ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.

iii. The Department will remove an organization from the Privacy Shield List in response to any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a privacy self-regulatory body or another independent dispute resolution body, or from a government body, but only after first providing 30 days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the Privacy Shield List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of Privacy Shield benefits.

iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the Privacy Shield must provide that body with full information about its prior participation in the Privacy Shield.

12. Choice – Timing of Opt Out

a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside the EU in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (i) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (ii) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Privacy Shield provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting these conditions or other conditions set out in Article 26 of the Directive. Since the Privacy Shield includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to Privacy Shield participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

a. Application of EU Member State Laws or the Privacy Shield Principles

i. EU Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Privacy Shield Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

b. Future Scientific Research

i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing.

ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

c. Withdrawal from a Clinical Trial

i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

d. Transfers for Regulatory and Supervision Purposes

i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.

e. "Blinded" Studies

i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as "blinded" studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.

ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.

f. Product Safety and Efficacy Monitoring

i. A pharmaceutical or medical device company does not have to apply the Privacy Shield Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

g. Key-coded Data

i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (*e.g.*, if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way would not constitute a transfer of personal data that would be subject to the Privacy Shield Principles.

15. Public Record and Publicly Available Information

a. An organization must apply the Privacy Shield Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records, *i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general.

b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Privacy Shield.

d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, Privacy Shield organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public

authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.

b. The information provided by the Privacy Shield organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the annual joint review of the functioning of the Privacy Shield in accordance with the Principles.

c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.

ANNEX I

This Annex I provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain "residual" claims as to data covered by the EU-U.S. Privacy Shield. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of claimed violations of the Principles not resolved by any of the other Privacy Shield mechanisms, if any.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles[1] or with respect to an allegation about the adequacy of the Privacy Shield.

B. Available Remedies

Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in Section III.11(d)(i) of the Principles; (2) make use of the independent recourse mechanism under the Principles, which is at no cost to the individual; and (3) raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual.

This arbitration option may not be invoked if the individual's same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if an EU Data Protection

---

[1] Section I.5 of the Principles.

Authority (1) has authority under Sections III.5 or III.9 of the Principles; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA's authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.[2] Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the Privacy Shield organization.

---

[2] Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")]." 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select the arbitrators from the list of arbitrators discussed below.

Consistent with applicable law, the U.S. Department of Commerce and the European Commission will develop a list of at least 20 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

(1) will remain on the list for a period of 3 years, absent exceptional circumstances or for cause, renewable for one additional period of 3 years;
(2) shall not be subject to any instructions from, or be affiliated with, either party, or any Privacy Shield organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
(3) must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law.

G. Arbitration Procedures

Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.

6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing as well as translation of arbitral materials will be provided at no cost to the individual, unless the panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

Subject to applicable law, the Department of Commerce will facilitate the establishment of a fund, into which Privacy Shield organizations will be required to pay an annual contribution, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts ("caps"), in consultation with the European Commission. The fund will be managed by a third party, which will report regularly on the operations of the fund. At the annual review, the Department of Commerce and European Commission will review the operation of the fund, including the need to adjust the amount of the contributions or of the caps, and will consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the mutual understanding that there will be no excessive financial burden imposed on Privacy Shield organizations. Attorney's fees are not covered by this provision or any fund under this provision.

ANNEX III

THE SECRETARY OF STATE
WASHINGTON

February 22, 2016

Dear Commissioner Jourová,

I am pleased we have reached an understanding on the European Union-United States Privacy Shield that will include an Ombudsperson mechanism through which authorities in the EU will be able to submit requests on behalf of EU individuals regarding U.S. signals intelligence practices.

On January 17, 2014, President Barack Obama announced important intelligence reforms included in Presidential Policy Directive 28 (PPD-28). Under PPD-28, I designated Under Secretary of State Catherine A. Novelli, who also serves as Senior Coordinator for International Information Technology Diplomacy, as our point of contact for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. Building on this role, I have established a Privacy Shield Ombudsperson mechanism in accordance with the terms set out in Annex A. I have directed Under Secretary Novelli to perform this function. Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me.

I have directed my staff to devote the necessary resources to implement this new Ombudsperson mechanism, and am confident it will be an effective means to address EU individuals' concerns.

Sincerely,

John F. Kerry

EU-U.S. PRIVACY SHIELD OMBUDSPERSON MECHANISM REGARDING SIGNALS INTELLIGENCE

In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with Presidential Policy Directive 28 (PPD-28), regarding signals intelligence.

On January 17, 2014, President Obama gave a speech announcing important intelligence reforms. In that speech, he pointed out that "[o]ur efforts help protect not only our nation, but our friends and allies as well. Our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too." President Obama announced the issuance of a new presidential directive—PPD-28—to "clearly prescribe what we do, and do not do, when it comes to our overseas surveillance."

Section 4(d) of PPD-28 directs the Secretary of State to designate a "Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) "to ... serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States." As of January 2015, Under Secretary C. Novelli has served as the Senior Coordinator.

This Memorandum describes a new mechanism that the Senior Coordinator will follow to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), "Derogations,"[1] or "Possible Future Derogations,"[2] through

[1] "Derogations" in this context mean a commercial transfer or transfers that take place on the condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

[2] "Possible Future Derogations" in this context mean a commercial transfer or transfers that take place on one of the following conditions, to the extent the condition constitutes lawful grounds for transfers of personal data from the EU to the U.S.: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate

established avenues under applicable United States laws and policy, and the response to those requests.

1. **The Privacy Shield Ombudsperson.** The Senior Coordinator will serve as the Privacy Shield Ombudsperson and designate additional State Department officials, as appropriate to assist in her performance of the responsibilities detailed in this memorandum. (Hereinafter, the Coordinator and any officials performing such duties will be referred to as "Privacy Shield Ombudsperson.") The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Under Secretary reports directly to the Secretary of State, and is independent from the Intelligence Community.

2. **Effective Coordination.** The Privacy Shield Ombudsperson will be able to effectively use and coordinate with the mechanisms and officials described below, in order to ensure appropriate response to communications from submitting EU individual complaint handing body.

    a. The Privacy Shield Ombudsperson will work closely with other United States Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies. In particular, the Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers.

    b. The United States Government will rely on mechanisms for coordinating and overseeing national security matters across departments and agencies to help ensure that the Privacy Shield Ombudsperson is able to respond within the meaning of Section 4(e) to completed requests under Section 3(b).

    c. The Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

---

safeguards; or (b) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (c) where a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data.

3. **Submitting Requests.**

   a. A request will initially be submitted to the Member States bodies competent for the oversight of national security services. The EU reserves the possibility to designate a centralized EU individual complaint handling body to which a request can also be submitted (hereafter together or alternatively: the "EU individual complaint handling body").

   b. The EU individual complaint handling body will ensure, in compliance with the following actions, that the request is complete:

      (i) Verifying the identity of the individual, and that the individual is acting on his/her own behalf, and not as a representative of a governmental or intergovernmental organization.
      (ii) Ensuring the request is made in writing, and that it contains the following basic information:
         - any information that forms the basis for the request,
         - the nature of information or relief sought,
         - the United States Government entities believed to be involved, if any, and
         - the other measures pursued to obtain the information or relief requested and the response received through those other measures.
      (iii) Verifying that the request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to the Privacy Shield, SCCs, BCRs, Derogations, or Possible Future Derogations.
      (iv) Making an initial determination that the request is not frivolous, vexatious, or made in bad faith.

   c. To be completed for purposes of further handling by the Privacy Shield Ombudsperson under this memorandum, the request need not demonstrate that the requester's data has in fact been accessed by the United States Government through signal intelligence activities.

4. **Commitments to Communicate with Submitting EU Individual Complaint Handling Body.**

   a. The Privacy Shield Ombudsperson will acknowledge receipt of the request to the submitting EU individual complaint handling body.

   b. The Privacy Shield Ombudsperson will conduct an initial review to verify that the request has been completed in conformance with Section 3(b). If the Privacy Shield Ombudsperson notes any deficiencies or has any questions regarding the completion of the request, the Privacy Shield Ombudsperson will seek to address and resolve those concerns with the submitting EU individual complaint handling body.

c. If, to facilitate appropriate processing of the request, the Privacy Shield Ombudsperson needs more information about the request, or if specific action is needed to be taken by the individual who originally submitted the request, the Privacy Shield Ombudsperson will so inform the submitting EU individual complaint handling body.

d. The Privacy Shield Ombudsperson will track the status of requests and provide updates as appropriate to the submitting EU individual complaint handling body.

e. Once a request has been completed as described in Section 3 of this Memorandum, the Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policies. The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed as provided under that statute and applicable regulations.

f. The Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of one of the underlying processes described below, then those communications will take place in accordance with existing procedures.

g. Commitments in this Memorandum will not apply to general claims that the EU-U.S. Privacy Shield is inconsistent with European Union data protection requirements. The commitments in this Memorandum are made based on the common understanding by the European Commission and the U.S. government that given the scope of commitments under this mechanism, there may be resource constraints that arise, including with respect to Freedom of Information Act (FOIA) requests. Should the carrying-out of the Privacy Shield Ombudsperson's functions exceed reasonable resource constraints and impede the fulfillment of these commitments, the U.S. government will discuss with the European Commission any adjustments that may be appropriate to address the situation.

5. **Requests for Information.** Requests for access to United States Government records may be made and processed under the Freedom of Information Act (FOIA).

a. FOIA provides a means for any person to seek access to existing federal agency records, regardless of the nationality of the requester. This statute is codified in the United States Code at 5 U.S.C. § 552. The statute, together with additional information about FOIA, is available at www.FOIA.gov and http://www.justice.gov/oip/foia-resources. Each agency has a Chief FOIA Officer, and has provided information on its public website about how to submit a FOIA request to the agency. Agencies have processes for consulting with one another on FOIA requests that involve records held by another agency.

b. By way of example:

   (i) The Office of the Director of National Intelligence (ODNI) has established the ODNI FOIA Portal for the ODNI: http://www.dni.gov/index.php/about-this-site/foia. This portal provides information on submitting a request, checking on the status of an existing request, and accessing information that has been released and published by the ODNI under FOIA. The ODNI FOIA Portal includes links to other FOIA websites for IC elements: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

   (ii) The Department of Justice's Office of Information Policy provides comprehensive information about FOIA: http://www.justice.gov/oip. This includes not only information about submitting a FOIA request to the Department of Justice, but also provides guidance to the United States government on interpreting and applying FOIA requirements.

c. Under FOIA, access to government records is subject to certain enumerated exemptions. These include limits on access to classified national security information, personal information of third parties, and information concerning law enforcement investigations, and are comparable to the limitations imposed by each EU Member State with its own information access law. These limitations apply equally to Americans and non-Americans.

d. Disputes over the release of records requested pursuant to FOIA can be appealed administratively and then in federal court. The court is required to make a *de novo* determination of whether records are properly withheld, 5 U.S.C. § 552(a)(4)(B), and can compel the government to provide access to records. In some cases courts have overturned government assertions that information should be withheld as classified. Although no monetary damages are available, courts can award attorney's fees.

6. **Requests for Further Action.** A request alleging violation of law or other misconduct will be referred to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance as described below.

a. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions.

(i) The Inspector General Act of 1978, as amended, statutorily established the Federal Inspectors General (IG) as independent and objective units within most agencies whose duties are to combat waste, fraud, and abuse in the programs and operations of their respective agencies. To this end, each IG is responsible for conducting audits and investigations relating to the programs and operations of its agency. Additionally, IGs provide leadership and coordination and recommend policies for activities designed to promote economy, efficiency, and effectiveness, and prevent and detect fraud and abuse, in agency programs and operations.

(ii) Each element of the Intelligence Community has its own Office of the Inspector General with responsibility for oversight of foreign intelligence activities, among other matters. A number of Inspector General reports about intelligence programs have been publicly released.

(iii) By way of example:

- The Office of the Inspector General of the Intelligence Community (IC IG) was established pursuant to Section 405 of the Intelligence Authorization Act of Fiscal Year 2010. The IC IG is responsible for conducting IC-wide audits, investigations, inspections, and reviews that identify and address systemic risks, vulnerabilities, and deficiencies that cut across IC agency missions, in order to positively impact IC-wide economies and efficiencies. The IC IG is authorized to investigate complaints or information concerning allegations of a violation of law, rule, regulation, waste, fraud, abuse of authority, or a substantial or specific danger to public health and safety in connection with ODNI and/or IC intelligence programs and activities. The IC IG provides information on how to contact the IC IG directly to submit a report: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

- The Office of the Inspector General (OIG) in the U.S. Department of Justice (DOJ) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The OIG investigates alleged violations of criminal and civil laws by DOJ employees and also audits and inspects DOJ programs. The OIG has jurisdiction over all complaints of misconduct against Department of Justice employees, including the Federal Bureau of Investigation; Drug Enforcement Administration; Federal Bureau of Prisons; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; United States Attorneys Offices; and employees who work in other

Divisions or Offices in the Department of Justice. (The one exception is that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorney's authority to investigate, litigate, or provide legal advice are the responsibility of the Department's Office of Professional Responsibility.) In addition, section 1001 of the USA Patriot Act, signed into law on October 26, 2001, directs the Inspector General to review information and receive complaints alleging abuses of civil rights and civil liberties by Department of Justice employees. The OIG maintains a public website – https://www.oig.justice.gov – which includes a "Hotline" for submitting complaints – https://www.oig.justice.gov/hotline/index.htm.

b. Privacy and Civil Liberties offices and entities in the United States Government also have relevant responsibilities. By way of example:

(i) Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified in the United States Code at 42 U.S.C. § 2000-ee1, establishes privacy and civil liberties officers at certain departments and agencies (including the Department of State, Department of Justice, and ODNI). Section 803 specifies that these privacy and civil liberties officers will serve as the principal advisor to, among other things, ensure that such department, agency, or element has adequate procedures to address complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties.

(ii) The ODNI's Civil Liberties and Privacy Office (ODNI CLPO) is led by the ODNI Civil Liberties Protection Officer, a position established by the National Security Act of 1948, as amended. The duties of the ODNI CLPO include ensuring that the policies and procedures of the elements of the Intelligence Community include adequate protections for privacy and civil liberties, and reviewing and investigating complaints alleging abuse or violation of civil liberties and privacy in ODNI programs and activities. The ODNI CLPO provides information to the public on its website, including instructions for how to submit a complaint: www.dni.gov/clpo. If the ODNI CLPO receives a privacy or civil liberties complaint involving IC programs and activities, it will coordinate with other IC elements on how that complaint should be further processed within the IC. Note that the National Security Agency (NSA) also has a Civil Liberties and Privacy Office, which provides information about its responsibilities on its website – https://www.nsa.gov/civil_liberties/. If information indicates that an agency is out of compliance with privacy requirements (*e.g.*, a requirement under Section 4 of PPD-28), then agencies have compliance mechanisms to review and remedy the incident. Agencies are required to report compliance incidents under PPD-28 to the ODNI.

(iii) The Office of Privacy and Civil Liberties (OPCL) at the Department of Justice supports the duties and responsibilities of the Department's Chief Privacy and Civil Liberties Officer (CPCLO). The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the Department's privacy compliance, including compliance with the Privacy Act of 1974, the privacy provisions of both the E-Government Act of 2002 and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties. OPCL provides information to the public about its responsibilities at http://www.justice.gov/opcl.

(iv) According to 42 U.S.C. § 2000ee *et seq.*, the Privacy and Civil Liberties Oversight Board shall continually review (i) the policies and procedures, as well as their implementation, of the departments, agencies and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected, and (ii) other actions by the executive branch relating to such efforts to determine whether such actions appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties. It shall receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified at 42 U.S.C. § 2000ee-1, directs the privacy and civil liberties officers of eight federal agencies (including the Secretary of Defense, Secretary of Homeland Security, Director of National Intelligence, and Director of the Central Intelligence Agency), and any additional agency designated by the Board, to submit periodic reports to the PCLOB, including the number, nature, and disposition of the complaints received by the respective agency for alleged violations. The PCLOB's enabling statute directs the Board to receive these reports and, when appropriate, make recommendations to the privacy and civil liberties officers regarding their activities.

ANNEX IV

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

OFFICE OF CHAIRWOMAN
EDITH RAMIREZ

February 23, 2016

VIA EMAIL

Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

The United States Federal Trade Commission ("FTC") appreciates the opportunity to describe its enforcement of the new EU-U.S. Privacy Shield Framework (the "Privacy Shield Framework" or "Framework"). We believe the Framework will play a critical role in facilitating privacy-protective commercial transactions in an increasingly interconnected world. It will enable businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections. The FTC has long committed to protecting privacy across borders and will make enforcement of the new Framework a high priority. Below, we explain the FTC's history of strong privacy enforcement generally, including our enforcement of the original Safe Harbor program, as well as the FTC's approach to enforcement of the new Framework.

The FTC first publicly expressed its commitment to enforce the Safe Harbor program in 2000. At that time, then-FTC Chairman Robert Pitofsky sent the European Commission a letter outlining the FTC's pledge to vigorously enforce the Safe Harbor Privacy Principles. The FTC has continued to uphold this commitment through nearly 40 enforcement actions, numerous additional investigations, and cooperation with individual European data protection authorities ("EU DPAs") on matters of mutual interest.

After the European Commission raised concerns in November 2013 about the administration and enforcement of the Safe Harbor program, we and the U.S. Department of Commerce began consultations with officials from the European Commission to explore ways to strengthen it. While those consultations were proceeding, on October 6, 2015, the European Court of Justice issued a decision in the *Schrems* case that, among other things, invalidated the European Commission's decision on the adequacy of the Safe Harbor program. Following the decision, we continued to work closely with the Department of Commerce and the European

Commission in an effort to strengthen the privacy protections provided to EU citizens. The Privacy Shield Framework is a result of these ongoing consultations. As was the case with the Safe Harbor program, the FTC hereby commits to vigorous enforcement of the new Framework. This letter memorializes that commitment.

Notably, we affirm our commitment in four key areas: (1) referral prioritization and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation with EU DPAs. We provide below detailed information about each of these commitments and relevant background about the FTC's role in protecting consumer privacy and enforcing Safe Harbor, as well as the broader privacy landscape in the United States.[1]

I. Background

A. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[2] A representation, omission, or practice is deceptive if it is material and likely to mislead consumers acting reasonably under the circumstances.[3] An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers or outweighed by countervailing benefits to consumers or competition.[4] The FTC also enforces targeted statutes that protect information relating to health, credit and other financial matters, as well as children's online information, and has issued regulations implementing each of these statutes.

The FTC's jurisdiction under the FTC Act applies to matters "in or affecting commerce." The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC's jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers. The FTC also does not have jurisdiction over most non-profit organizations, but it does have jurisdiction over sham charities or other non-profits that in actuality operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members.[5] In some instances, the FTC's jurisdiction is concurrent with that of other law enforcement agencies.

---

[1] We provide additional information about U.S. federal and state privacy laws in Attachment A, and a summary of our recent privacy and security enforcement actions in Attachment B. This summary is also available on the FTC's website at https://www.ftc.gov/reports/privacy-data-security-update-2015.

[2] 15 U.S.C. § 45(a).

[3] *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[4] *See* 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[5] *See California Dental Ass'n v. FTC*, 526 U.S. 756 (1999).

We have developed strong working relationships with federal and state authorities and work closely with them to coordinate investigations or make referrals where appropriate.

Enforcement is the lynchpin of the FTC's approach to privacy protection. To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information. This body of cases covers both offline and online information and includes enforcement actions against companies large and small, alleging that they failed to properly dispose of sensitive consumer data, failed to secure consumers' personal information, deceptively tracked consumers online, spammed consumers, installed spyware or other malware on consumers' computers, violated Do Not Call and other telemarketing rules, and improperly collected and shared consumer information on mobile devices. The FTC's enforcement actions—in both the physical and digital worlds—send an important message to companies about the need to protect consumer privacy.

The FTC has also pursued numerous policy initiatives aimed at enhancing consumer privacy that inform its enforcement work. The FTC has hosted workshops and issued reports recommending best practices aimed at improving privacy in the mobile ecosystem; increasing transparency of the data broker industry; maximizing the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers; and highlighting the privacy and security implications of facial recognition and the Internet of Things, among other areas.

The FTC also engages in consumer and business education to enhance the impact of its enforcement and policy development initiatives. The FTC has used a variety of tools—publications, online resources, workshops, and social media—to provide educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. Most recently, the Commission launched its "Start With Security" initiative, which includes new guidance for businesses drawing on lessons learned from the agency's data security cases, as well as a series of workshops across the country. In addition, the FTC has long been a leader in educating consumers about basic computer security. Last year, our OnGuard Online site and its Spanish language counterpart, Alerta en Línea, had more than 5 million page views.

B. U.S. Legal Protections Benefiting EU Consumers

The Framework will operate in the context of the larger U.S. privacy landscape, which protects EU consumers in a number of ways.

The FTC Act's prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies, including restitution, that are available to protect domestic consumers when protecting foreign consumers.

Indeed, the FTC's enforcement work significantly benefits both U.S. and foreign consumers. For example, our cases enforcing Section 5 of the FTC Act have protected the privacy of U.S. and foreign consumers alike. In a case against an information broker, Accusearch, the FTC alleged that the company's sale of confidential telephone records to third

parties without consumers' knowledge or consent was an unfair practice in violation of Section 5 of the FTC Act. Accusearch sold information relating to both U.S. and foreign consumers.[6] The court granted injunctive relief against Accusearch prohibiting, among other things, the marketing or sale of consumers' personal information without written consent, unless it was lawfully obtained from publicly available information, and ordered disgorgement of almost $200,000.[7]

The FTC's settlement with TRUSTe is another example. It ensures that consumers, including those in the European Union, can rely on representations that a global self-regulatory organization makes about its review and certification of domestic and foreign online services.[8] Importantly, our action against TRUSTe also strengthens the privacy self-regulatory system more broadly by ensuring the accountability of entities that play an important role in self-regulatory schemes, including cross-border privacy frameworks.

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children's Online Privacy Protection Act ("COPPA"). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under the age of 13, provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. In addition to the U.S. federal laws enforced by the FTC, certain other federal and state consumer protection and privacy laws may provide additional benefits to EU consumers.

C. Safe Harbor Enforcement

As part of its privacy and security enforcement program, the FTC has also sought to protect EU consumers by bringing enforcement actions that involved Safe Harbor violations. The FTC has brought 39 Safe Harbor enforcement actions: 36 alleging false certification claims, and three cases—against Google, Facebook, and Myspace—involving alleged violations of Safe Harbor Privacy Principles.[9] These cases demonstrate the enforceability of certifications and the repercussions for non-compliance. Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products

---

[6] *See* Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. The Office of the Privacy Commissioner of Canada filed an *amicus curiae* brief in the appeal of the FTC action and conducted its own investigation, concluding that Accusearch's practices also violated Canadian law.

[7] *See FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

[8] *See In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (decision and order), *available at* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

[9] *See In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), *available at* https://www ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* https://www ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new Privacy Shield Framework. The FTC can enforce these orders by seeking civil penalties. In fact, Google paid a record $22.5 million civil penalty in 2012 to resolve allegations it had violated its order. Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.

The FTC's cases have also focused on false, deceptive, or misleading claims of Safe Harbor participation. The FTC takes these claims seriously. For example, in *FTC v. Karnani*, the FTC brought an action in 2011 against an Internet marketer in the United States alleging that he and his company tricked British consumers into believing that the company was based in the United Kingdom, including by using .uk web extensions and referencing British currency and the UK postal system.[10] However, when consumers received the products, they discovered unexpected import duties, warranties that were not valid in the United Kingdom, and charges associated with obtaining refunds. The FTC also charged that the defendants deceived consumers about their participation in the Safe Harbor program. Notably, all of the consumer victims were in the United Kingdom.

Many of our other Safe Harbor enforcement cases involved organizations that joined the Safe Harbor program but failed to renew their annual certification while they continued to represent themselves as current members. As discussed further below, the FTC also commits to addressing false claims of participation in the Privacy Shield Framework. This strategic enforcement activity will complement the Department of Commerce's increased actions to verify compliance with program requirements for certification and re-certification, its monitoring of effective compliance, including through the use of questionnaires to Framework participants, and its increased efforts to identify false Framework membership claims and misuse of any Framework certification mark.[11]

II. Referral Prioritization and Investigations

As we did under the Safe Harbor program, the FTC commits to give priority to Privacy Shield referrals from EU Member States. We will also prioritize referrals of non-compliance with self-regulatory guidelines relating to the Privacy Shield Framework from privacy self-regulatory organizations and other independent dispute resolution bodies.

---

[10] *See FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (stipulated final order), *available at* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *see also* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways (June 9, 2011).

[11] Letter from Stefan M. Selig, Under Secretary of Commerce for International Trade, International Trade Administration, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality (Feb. 23, 2016).

To facilitate referrals under the Framework from EU Member States, the FTC is creating a standardized referral process and providing guidance to EU Member States on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC will designate an agency point of contact for EU Member State referrals. It is most useful when the referring authority has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of a referral from an EU Member State or self-regulatory organization, the FTC can take a range of actions to address the issues raised. For example, we may review the company's privacy policies, obtain further information directly from the company or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether consumer and business education would be helpful, and, as appropriate, initiate an enforcement proceeding.

The FTC also commits to exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with EU DPAs to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially similar to those prohibited by laws the FTC enforces.[12] As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on behalf of the EU DPA conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the DPA's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.[13]

---

[12] In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, inter alia: "(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons." 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

[13] In fiscal years 2012-2015, for example, the FTC used its U.S. SAFE WEB Act authority to share information in response to almost 60 requests from foreign agencies and it issued nearly 60 civil investigative demands (equivalent to administrative subpoenas) to aid 25 foreign investigations.

In addition to prioritizing Privacy Shield referrals from EU Member States and privacy self-regulatory organizations,[14] the FTC commits to investigating possible Framework violations on its own initiative where appropriate using a range of tools.

For well over a decade, the FTC has maintained a robust program of investigating privacy and security issues involving commercial organizations. As part of these investigations, the FTC routinely examined whether the entity at issue was making Safe Harbor representations. If the entity was making such representations and the investigation revealed apparent violations of the Safe Harbor Privacy Principles, the FTC included allegations of Safe Harbor violations in its enforcement actions. We will continue this proactive approach under the new Framework. Importantly, the FTC conducts many more investigations than ultimately result in public enforcement actions. Many FTC investigations are closed because staff does not identify an apparent law violation. Because FTC investigations are non-public and confidential, the closing of an investigation is often not made public.

The nearly 40 enforcement actions initiated by the FTC involving the Safe Harbor program evidence the agency's commitment to proactive enforcement of cross-border privacy programs. The FTC will look for potential Framework violations as part of the privacy and security investigations we undertake on a regular basis.

III. Addressing False or Deceptive Privacy Shield Membership Claims

As referenced above, the FTC will take action against entities that misrepresent their participation in the Framework. The FTC will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of the Framework or using any Framework certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the Privacy Shield Principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from FTC enforcement of those Framework commitments.

IV. Order Monitoring

The FTC also affirms its commitment to monitor enforcement orders to ensure compliance with the Privacy Shield Framework.

We will require compliance with the Framework through a variety of appropriate injunctive provisions in future FTC Framework orders. This includes prohibiting

[14] Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize Privacy Shield referrals from EU DPAs. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. EU citizens can use the same complaint system available to U.S. citizens to submit a complaint to the FTC at www.ftc.gov/complaint. For individual Privacy Shield complaints, however, it may be most useful for EU citizens to submit complaints to their Member State DPA or alternative dispute resolution provider.

misrepresentations regarding the Framework and other privacy programs when these are the basis for the underlying FTC action.

The FTC's cases enforcing the original Safe Harbor program are instructive. In the 36 cases involving false or deceptive claims of Safe Harbor certification, each order prohibits the defendant from misrepresenting its participation in Safe Harbor or any other privacy or security program and requires the company to make compliance reports available to the FTC. In cases that involved violations of Safe Harbor Privacy Principles, companies have been required to implement comprehensive privacy programs and obtain independent third-party assessments of those programs every other year for twenty years, which they must provide to the FTC.

Violations of the FTC's administrative orders can lead to civil penalties of up to $16,000 per violation, or $16,000 per day for a continuing violation,[15] which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with Safe Harbor orders, as it does with all of its orders. The FTC takes enforcement of its privacy and data security orders seriously and brings actions to enforce them when necessary. For example, as noted above, Google paid a $22.5 million civil penalty to resolve allegations it had violated its FTC order. Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints.

Finally, the FTC will continue to maintain an online list of companies subject to orders obtained in connection with enforcement of both the Safe Harbor program and the new Privacy Shield Framework.[16] In addition, the Privacy Shield Principles now require companies subject to an FTC or court order based on non-compliance with the Principles to make public any relevant Framework-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality laws and rules.

V. Engagement With EU DPAs and Enforcement Cooperation

The FTC recognizes the important role that EU DPAs play with respect to Framework compliance and encourages increased consultation and enforcement cooperation. In addition to any consultation with referring DPAs on case-specific matters, the FTC commits to participate in periodic meetings with designated representatives of the Article 29 Working Party to discuss in general terms how to improve enforcement cooperation with respect to the Framework. The FTC will also participate, along with the Department of Commerce, the European Commission, and Article 29 Working Party representatives, in the annual review of the Framework to discuss its implementation.

---

[15] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

[16] *See* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251.

The FTC also encourages the development of tools that will enhance enforcement cooperation with EU DPAs, as well as other privacy enforcement authorities around the world. In particular, the FTC, along with enforcement partners in the European Union and around the globe, last year launched an alert system within the Global Privacy Enforcement Network ("GPEN") to share information about investigations and promote enforcement coordination. This GPEN Alert tool could be particularly useful in the context of the Privacy Shield Framework. The FTC and EU DPAs could use it to coordinate with respect to the Framework and other privacy investigations, including as a starting point for sharing information in order to deliver coordinated and more effective privacy protection for consumers. We look forward to continuing to work with participating EU authorities to deploy the GPEN Alert system more broadly and develop other tools to improve enforcement cooperation in privacy cases, including those involving the Framework.

***

The FTC is pleased to affirm its commitment to enforcing the new Privacy Shield Framework. We also look forward to continuing engagement with our EU colleagues as we work together to protect consumer privacy on both sides of the Atlantic.

Sincerely,

Edith Ramirez
Chairwoman

ANNEX V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

February 19, 2016

Commissioner Věra Jourová
European Commission
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
Belgium

Re: EU-U.S. Privacy Shield Framework

Dear Commissioner Jourová:

The United States Department of Transportation ("Department" or "DOT") appreciates the opportunity to describe its role in enforcing the EU-U.S. Privacy Shield Framework. This Framework plays a critical role in protecting personal data provided during commercial transactions in an increasingly interconnected world. It enables businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the Safe Harbor Framework in a letter sent to the European Commission over 15 years ago. The DOT pledged to vigorously enforce the Safe Harbor Privacy Principles in that letter. The DOT continues to uphold this commitment and this letter memorializes that commitment.

Notably, the DOT renews its commitment in the following key areas: (1) prioritization of investigation of alleged Privacy Shield violations; (2) appropriate enforcement action against entities making false or deceptive Privacy Shield certification claims; and (3) monitoring and making public enforcement orders concerning Privacy Shield violations. We provide information about each of these commitments and, for necessary context, pertinent background about the DOT's role in protecting consumer privacy and enforcing the Privacy Shield Framework.

I. Background

A. DOT's Privacy Authority

The Department is strongly committed to ensuring the privacy of information provided by consumers to airlines and ticket agents. The DOT's authority to take action in this area is found in 49 U.S.C. 41712, which prohibits a carrier or ticket agent from engaging in "an unfair or deceptive practice or an unfair method of competition" in the sale of air transportation that results or is likely to result in consumer harm. Section 41712 is patterned after Section 5 of the Federal Trade Commission (FTC) Act (15 U.S.C. 45). We interpret our unfair or deceptive practice statute as prohibiting an airline or ticket agent from: (1) violating the terms of its

privacy policy; or (2) gathering or disclosing private information in a way that violates public policy, is immoral, or causes substantial consumer injury not offset by any countervailing benefits. We also interpret section 41712 as prohibiting carriers and ticket agents from: (1) violating any rule issued by the Department that identifies specific privacy practices as unfair or deceptive; or (2) violating the Children's Online Privacy Protection Act (COPPA) or FTC rules implementing COPPA. Under federal law, the DOT has exclusive authority to regulate the privacy practices of airlines, and it shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation.

As such, once a carrier or seller of air transportation publicly commits to the Privacy Shield Framework's privacy principles the Department is able to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier or ticket agent that has committed to honoring the Privacy Shield Framework's privacy principles, any failure to do so by the carrier or ticket agent would be a violation of section 41712.

B. Enforcement Practices

The Department's Office of Aviation Enforcement and Proceedings (Aviation Enforcement Office) investigates and prosecutes cases under 49 U.S.C. 41712. It enforces the statutory prohibition in section 41712 against unfair and deceptive practices primarily through negotiation, preparing cease and desist orders, and drafting orders assessing civil penalties. The office learns of potential violations largely from complaints it receives from individuals, travel agents, airlines, and U.S. and foreign government agencies. Consumers may use the DOT's website to file privacy complaints against airlines and ticket agents.[1]

If a reasonable and appropriate settlement in a case is not reached, the Aviation Enforcement Office has the authority to institute an enforcement proceeding involving an evidentiary hearing before a DOT administrative law judge (ALJ). The ALJ has the authority to issue cease-and-desist orders and civil penalties. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to $27,500 for each violation of section 41712.

The Department does not have the authority to award damages or provide pecuniary relief to individual complainants. However, the Department does have the authority to approve settlements resulting from investigations brought by its Aviation Enforcement Office that directly benefit consumers (e.g., cash, vouchers) as an offset to monetary penalties otherwise payable to the U.S. Government. This has occurred in the past, and may also occur in the context of the Privacy Shield Framework principles when circumstances warrant. Repeated violations of section 41712 by an airline would also raise questions regarding the airline's compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority.

[1] http://www.transportation.gov/airconsumer/privacy-complaints.

To date, the DOT has received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated according to the principles set forth above.

C. DOT Legal Protections Benefiting EU Consumers

Under section 41712, the prohibition on unfair or deceptive practices in air transportation or the sale of air transportation applies to U.S. and foreign air carriers as well as ticket agents. The DOT frequently takes action against U.S. and foreign airlines for practices that affect both foreign and U.S. consumers on the basis that the airline's practices took place in the course of providing transportation to or from the United States. The DOT does and will continue to use all remedies that are available to protect both foreign and U.S. consumers from unfair or deceptive practices in air transportation by regulated entities.

The DOT also enforces, with respect to airlines, other targeted laws whose protections extend to non-U.S. consumers such as COPPA. Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under 13 provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. To the extent that U.S. or foreign airlines doing business in the United States violate COPPA, the DOT would have jurisdiction to take enforcement action.

II. Privacy Shield Enforcement

If an airline or ticket agent chooses to participate in the Privacy Shield Framework and the Department receives a complaint that such an airline or ticket agent had allegedly violated the Framework, the Department would take the following steps to vigorously enforce the Framework.

A. Prioritizing Investigation of Alleged Violations

The Department's Aviation Enforcement Office will investigate each complaint alleging Privacy Shield violations (including complaints received from EU Data Protection Authorities) and take enforcement action where there is evidence of a violation. Further, the Aviation Enforcement Office will cooperate with the FTC and Department of Commerce and give priority consideration to allegations that the regulated entities are not complying with privacy commitments made as part of the Privacy Shield Framework.

Upon receipt of an allegation of a violation of the Privacy Shield Framework, the Department's Aviation Enforcement Office may take a range of actions as part of its investigation. For example, it may review the ticket agent or airline's privacy policies, obtain further information from the ticket agent or airline or from third parties, follow up with the referring entity, and assess whether there is a pattern of violations or significant number of consumers affected. In

addition, it would determine whether the issue implicates matters within the purview of the Department of Commerce or FTC, assess whether consumer education and business education would be helpful, and as appropriate, initiate an enforcement proceeding.

If the Department becomes aware of potential Privacy Shield violations by ticket agents, it will coordinate with the FTC on the matter. We will also advise the FTC and the Department of Commerce of the outcome of any Privacy Shield enforcement action.

B. Addressing False or Deceptive Membership Claims

The Department remains committed to investigating Privacy Shield violations, including false or deceptive claims of membership in the Privacy Shield Program. We will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of Privacy Shield or using the Privacy Shield Framework certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the substantive Privacy Shield principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from DOT enforcement of those commitments.

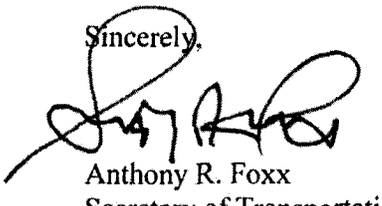
C. Monitoring and Making Public Enforcement Orders Concerning Privacy Shield Violations

The Department's Aviation Enforcement Office also remains committed to monitoring enforcement orders as needed to ensure compliance with the Privacy Shield program. Specifically, if the office issues an order directing an airline or ticket agent to cease and desist from future violations of Privacy Shield and section 41712, it will monitor the entity's compliance with the cease-and-desist provision in the order. In addition, the office will ensure that orders resulting from Privacy Shield cases are available on its website.

We look forward to our continued work with our federal partners and EU stakeholders on Privacy Shield matters.

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,



Anthony R. Foxx
Secretary of Transportation

ANNEX VI

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
OFFICE OF GENERAL COUNSEL
WASHINGTON, DC 20511

FEB 22 2016

Mr. Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Mr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Dear Mr. Antonipillai and Mr. Dean:

Over the last two and a half years, in the context of negotiations for the EU-U.S. Privacy Shield, the United States has provided substantial information about the operation of U.S. Intelligence Community signals intelligence collection activity. This has included information about the governing legal framework, the multi-layered oversight of those activities, the extensive transparency about those activities, and the overall protections for privacy and civil liberties, in order to assist the European Commission in making a determination about the adequacy of those protections as they relate to the national security exception to the Privacy Shield principles. This document summarizes the information that has been provided.

I. PPD-28 and the Conduct of U.S. Signals Intelligence Activity

The U.S. Intelligence Community collects foreign intelligence in a carefully controlled manner, in strict accordance with U.S. laws and subject to multiple layers of oversight, focusing on important foreign intelligence and national security priorities. A mosaic of laws and policies governs U.S. signals intelligence collection, including the U.S. Constitution, the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 *et seq.*) (FISA), Executive Order 12333 and its implementing procedures, Presidential guidance, and numerous procedures and guidelines, approved by the FISA Court and the Attorney General, that establish additional rules limiting the collection, retention, use, and dissemination of foreign intelligence information.[1]

a. PPD 28 Overview

In January 2014, President Obama gave a speech outlining various reforms to U.S. signals intelligence activities, and issued Presidential Policy Directive 28 (PPD-28) concerning

[1] Further information concerning U.S. foreign intelligence activities is posted online and publicly accessible through IC on the Record (www.icontherecord.tumblr.com), the ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the government.

those activities.[2] The President emphasized that U.S. signals intelligence activities help secure not only our country and our freedoms, but also the security and freedoms of other countries, including EU Member States, that rely on the information U.S. intelligence agencies obtain to protect their own citizens.

PPD-28 sets out a series of principles and requirements that apply to all U.S. signals intelligence activities and for all people, regardless of nationality or location. In particular, it sets certain requirements for procedures to address the collection, retention, and dissemination of personal information about non-U.S. persons acquired pursuant to U.S. signals intelligence. These requirements are set forth in more detail below, but in summary:

- The PPD reiterates that the United States collects signals intelligence only as authorized by statute, executive order, or other Presidential directive.
- The PPD establishes procedures to ensure that signals intelligence activity is conducted only in furtherance of legitimate and authorized national security purposes.
- The PPD also requires that privacy and civil liberties be integral concerns in the planning of signals intelligence collection activities. In particular, the United States does not collect intelligence to suppress or burden criticism or dissent; in order to disadvantage persons based on their ethnicity, race, gender, sexual orientation, or religion; or to afford a competitive commercial advantage to U.S. companies and U.S. business sectors.
- The PPD directs that signals intelligence collection be as tailored as feasible and that signals intelligence collected in bulk can only be used for specific enumerated purposes.
- The PPD directs that the Intelligence Community adopt procedures "reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities," and in particular extending certain protections afforded to the personal information of U.S. persons to non-US person information.
- Agency procedures implementing PPD-28 have been adopted and made public.

The applicability of the procedures and protections set out herein to the Privacy Shield is clear. When data has been transferred to corporations in the United States pursuant to the Privacy Shield, or indeed by any means, U.S. intelligence agencies can seek that data from those corporations only if the request complies with FISA or is made pursuant to one of the National Security Letter statutory provisions, which are discussed below.[3] In addition, without confirming or denying media reports alleging that the U.S. Intelligence Community collects data from transatlantic cables while it is being transmitted to the United States, were the U.S. Intelligence Community to collect data from transatlantic cables, it would do so subject to the limitations and safeguards set out herein, including the requirements of PPD-28.

b. Collection Limitations

PPD-28 sets out a number of important general principles that govern the collection of signals intelligence:

---

[2] *Available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[3] Law enforcement or regulatory agencies may request information from corporations for investigative purposes in the United States pursuant to other criminal, civil, and regulatory authorities that are beyond the scope of this paper, which is limited to national security authorities.

- The collection of signals intelligence must be authorized by statute or Presidential authorization, and must be undertaken in accordance with the Constitution and law.
- Privacy and civil liberties must be integral considerations in planning signals intelligence activities.
- Signals intelligence will be collected only when there is a valid foreign intelligence or counterintelligence purpose.
- The United States will not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent.
- The United States will not collect signals intelligence to disadvantage people based on their ethnicity, race, gender, sexual orientation, or religion.
- The United States will not collect signals intelligence to afford a competitive commercial advantage to U.S. companies and business sectors.
- U.S. signals intelligence activity must *always* be as tailored as feasible, taking into account the availability of other sources of information. This means, among other things, that whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk.

The requirement that signals intelligence activity be "as tailored as feasible" applies to the manner in which signals intelligence is collected, as well as to what is actually collected. For example, in determining whether to collect signals intelligence, the Intelligence Community must consider the availability of other information, including diplomatic or public sources, and prioritize collection through those means, where appropriate and feasible. Moreover, Intelligence Community element policies should require that wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (*e.g.*, specific facilities, selection terms and identifiers).

It is important to view the information provided to the Commission as a whole. Decisions about what is "feasible" or "practicable" are not left to the discretion of individuals but are subject to the policies that agencies have issued under PPD-28 – which have been made publicly available – and to the other processes described therein.[4] As PPD-28 says, bulk collection of signals intelligence is collection that "due to technical or operational considerations, is acquired without the use of discriminants (*e.g.*, specific identifiers, selection terms, etc.)." In this respect, PPD-28 recognizes that Intelligence Community elements must collect bulk signals intelligence in certain circumstances in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications. It also recognizes the privacy and civil liberties concerns raised when bulk signals intelligence is collected. PPD-28 therefore directs the Intelligence Community to prioritize alternatives that would allow the conduct of targeted signals intelligence rather than bulk signals intelligence collection. Accordingly, Intelligence Community elements should conduct targeted signals intelligence collection activities rather than bulk signal intelligence

[4] *Available at* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. These procedures implement the targeting and tailoring concepts discussed in this letter in a manner specific to each IC element.

collection activities whenever practicable.[5] These principles ensure that the exception for bulk collection will not swallow the general rule.

As for the concept of "reasonableness," it is a bedrock principle of U.S. law. It signifies that Intelligence Community elements will not be required to adopt any measure theoretically possible, but rather will have to balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities. Here again, the agencies' policies have been made available, and can provide assurance that the term "reasonably designed to minimize the dissemination and retention of personal information" does not undermine the general rule.

PPD-28 also provides that signals intelligence collected in bulk can only be used for six specific purposes: detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion. The President's National Security Advisor, in consultation with the Director for National Intelligence (DNI), will annually review these permissible uses of signals intelligence collected in bulk to see whether they should be changed. The DNI will make this list publicly available to the maximum extent feasible, consistent with national security. This provides an important and transparent limitation on the use of bulk signals intelligence collection.

Additionally, the Intelligence Community elements implementing PPD-28 have reinforced existing analytic practices and standards for querying unevaluated signals intelligence.[6] Analysts must structure their queries or other search terms and techniques to ensure that they are appropriate to identify intelligence information relevant to a valid foreign intelligence or law enforcement task. To that end, IC elements must focus queries about persons on the categories of signals intelligence information responsive to a foreign intelligence or law enforcement requirement, so as to prevent the use of personal information not pertinent to foreign intelligence or law enforcement requirements.

It is important to emphasize that any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet. Additionally, the use of targeted queries, as described above, ensures that only those items believed to be of potential intelligence value are ever presented for analysts to examine. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

The United States has elaborate processes to ensure that signals intelligence activities are conducted only in furtherance of appropriate national security purposes. Each year the President sets the nation's highest priorities for foreign intelligence collection after an extensive, formal interagency process. The DNI is responsible for translating these intelligence priorities into the

---

[5] To cite but one example, the NSA's procedures implementing PPD-28 state that "[w]henever practicable, collection will occur through the use of one or more selection terms in order to focus the collection on specific foreign intelligence targets (*e.g.*, a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (*e.g.*, the proliferation of weapons of mass destruction by a foreign power or its agents)."

[6] *Available at* http://www.dni.gov/files/documents/1017/PPD-28 Status Report Oct 2014.pdf.

National Intelligence Priorities Framework, or NIPF. PPD-28 strengthened and enhanced the interagency process to ensure that all of the IC's intelligence priorities are reviewed and approved by high-level policymakers. Intelligence Community Directive (ICD) 204 provides further guidance on the NIPF and was updated in January 2015 to incorporate the requirements of PPD-28.[7] Although the NIPF is classified, information related to specific U.S. foreign intelligence priorities is reflected annually in the DNI's unclassified *Worldwide Threat Assessment*, which is also readily available on the ODNI website.

The priorities in the NIPF are at a fairly high level of generality. They include topics such as the pursuit of nuclear and ballistic missile capabilities by particular foreign adversaries, the effects of drug cartel corruption, and human rights abuses in specific countries. And they apply not just to signals intelligence, but to all intelligence activities. The organization that is responsible for translating the priorities in the NIPF into actual signals intelligence collection is called the National Signals Intelligence Committee, or SIGCOM. It operates under the auspices of the Director of the National Security Agency (NSA), who is designated by Executive Order 12333 as the "functional manager for signals intelligence," responsible for overseeing and coordinating signals intelligence across the Intelligence Community under the oversight of both the Secretary of Defense and the DNI. The SIGCOM has representatives from all elements of the IC and, as the United States fully implements PPD-28, also will have full representation from other departments and agencies with a policy interest in signals intelligence.

All U.S. departments and agencies that are consumers of foreign intelligence submit their requests for collection to the SIGCOM. The SIGCOM reviews those requests, ensures that they are consistent with the NIPF, and assigns them priorities using criteria such as:

- Can signals intelligence provide useful information in this case, or are there better or more cost-effective sources of information to address the requirement, such as imagery or open source information?
- How critical is this information need? If it is a high priority in the NIPF, it will most often be a high signal intelligence priority.
- What type of signals intelligence could be used?
- Is the collection as tailored as feasible? Should there be time, geographic, or other limitations?

The U.S. signals intelligence requirements process also requires explicit consideration of other factors, namely:

- Is the target of the collection, or the methodology used to collect, particularly sensitive? If so, it will require review by senior policymakers.
- Will the collection present an unwarranted risk to privacy and civil liberties, regardless of nationality?
- Are additional dissemination and retention safeguards necessary to protect privacy or national security interests?

---

[7] *Available at* http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

Finally, at the end of the process, trained NSA personnel take the priorities validated by the SIGCOM and research and identify specific selection terms, such as telephone numbers or email addresses, which are expected to collect foreign intelligence responsive to these priorities. Any selector must be reviewed and approved before it is entered into NSA's collection systems. Even then, however, whether and when actual collection takes place will depend in part on additional considerations such as the availability of appropriate collection resources. This process ensures that U.S. signals intelligence collection targets reflect valid and important foreign intelligence needs. And, of course, when collection is conducted pursuant to FISA, NSA and other agencies must follow additional restrictions approved by the Foreign Intelligence Surveillance Court. In short, neither NSA nor any other U.S. intelligence agency decides on its own what to collect.

Overall, this process ensures that all U.S. intelligence priorities are set by senior policymakers who are in the best position to identify U.S. foreign intelligence requirements, and that those policymakers take into account not only the potential value of the intelligence collection but also the risks associated with that collection, including the risks to privacy, national economic interests, and foreign relations.

With respect to data transmitted to the United States pursuant to the Privacy Shield, although the United States cannot confirm or deny specific intelligence methods or operations, the requirements of PPD-28 apply to any signals intelligence operations the United States conducts, regardless of the type or source of data that is being collected. Further, the limitations and safeguards applicable to the collection of signals intelligence apply to signals intelligence collected for any authorized purpose, including both foreign relations and national security purposes.

The procedures discussed above demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information, and to implement – from the highest levels of our Government – the principle of reasonableness. PPD-28 and agency implementing procedures clarify new and existing limitations to and describe with greater specificity the purpose for which the United States collects and uses signals intelligence. These should provide assurance that signals intelligence activities are and will continue to be conducted only to further legitimate foreign intelligence goals.

c. Retention and Dissemination Limitations

Section 4 of PPD-28 requires that each element of the Intelligence Community have express limits on the retention and dissemination of personal information about non-U.S. persons collected by signals intelligence, comparable to the limits for U.S. persons. These rules are incorporated into procedures for each IC agency that were released in February 2015 and are publicly available. To qualify for retention or dissemination as foreign intelligence, personal information must relate to an authorized intelligence requirement, as determined in the NIPF process described above; be reasonably believed to be evidence of a crime; or meet one of the other standards for retention of U.S. person information identified in Executive Order 12333, section 2.3.

Information for which no such determination has been made may not be retained for more than five years, unless the DNI expressly determines that continued retention is in the national security interests of the United States. Thus, IC elements must delete non-U.S. person information collected through signals intelligence five years after collection, unless, for example, the information has been determined to be relevant to an authorized foreign intelligence requirement, or if the DNI determines, after considering the views of the ODNI Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security.

In addition, all agency policies implementing PPD-28 now explicitly require that information about a person may not be disseminated solely because an individual is a non-U.S. person, and ODNI has issued a directive to all IC elements[8] to reflect this requirement. Intelligence Community personnel are specifically required to consider the privacy interests of non-U.S. persons when drafting and disseminating intelligence reports. In particular, signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement. This recognizes an important limitation and is responsive to European Commission concerns about the breadth of the definition of foreign intelligence as set forth in Executive Order 12333.

d. Compliance and Oversight

The U.S. system of foreign intelligence oversight provides rigorous and multi-layered oversight to ensure compliance with applicable laws and procedures, including those pertaining to the collection, retention, and dissemination of non-U.S. person information acquired by signals intelligence as set forth in PPD-28. These include:

- The Intelligence Community employs hundreds of oversight personnel. NSA alone has over 300 people dedicated to compliance, and other elements also have oversight offices. In addition, the Department of Justice provides extensive oversight of intelligence activities, and oversight is also provided by the Department of Defense.
- Each element of the Intelligence Community has its own Office of the Inspector General with responsibility for oversight of foreign intelligence activities, among other matters. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions. While Inspector General recommendations are non-binding, the Inspector General's reports are often made public, and in any event are provided to Congress; this includes follow-up reports in case corrective action recommended in previous reports has not yet been completed. Congress is therefore informed of any non-compliance and can exert pressure, including through budgetary means, to achieve corrective action. A number of Inspector General reports about intelligence programs have been publicly released.[9]

---

[8] Intelligence Community Directive (ICD) 203, *available at* http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

[9] *See, e.g.*, U.S. Department of Justice Inspector General Report "A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008" (September 2012), *available at* https://oig.justice.gov/reports/2016/o1601a.pdf.

- ODNI's Civil Liberties and Privacy Office (CLPO) is charged with ensuring that the IC operates in a manner that advances national security while protecting civil liberties and privacy rights.[10] Other IC elements have their own privacy officers.
- The Privacy and Civil Liberties Oversight Board (PCLOB), an independent body established by statute, is charged with analyzing and reviewing counterterrorism programs and policies, including the use of signals intelligence, to ensure that they adequately protect privacy and civil liberties. It has issued several public reports on intelligence activities.
- As discussed more fully below, the Foreign Intelligence Surveillance Court, a court composed of independent federal judges, is responsible for oversight and compliance of any signals intelligence collection activities conducted pursuant to FISA.
- Finally, the U.S. Congress, specifically the House and Senate Intelligence and Judiciary Committees, have significant oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence.

Apart from these formal oversight mechanisms, the Intelligence Community has in place numerous mechanisms to ensure that the Intelligence Community is complying with the limitations on collection described above. For example:

- Cabinet officials are required to validate their signals intelligence requirements each year.
- NSA checks signals intelligence targets throughout the collection process to determine if they are actually providing valuable foreign intelligence responsive to the priorities, and will stop collection against targets that are not. Additional procedures ensure that selection terms are reviewed periodically.
- Based on a recommendation from an independent Review Group appointed by President Obama, the DNI has established a new mechanism to monitor the collection and dissemination of signals intelligence that is particularly sensitive because of the nature of the target or the means of collection, to ensure that it is consistent with the determinations of policymakers.
- Finally, ODNI annually reviews the IC's allocation of resources against the NIPF priorities and the intelligence mission as a whole. This review includes assessments of the value of all types of intelligence collection, including signals intelligence, and looks both backward – how successful has the IC been in achieving its goals? – and forward – what will the IC need in the future? This ensures that signals intelligence resources are applied to the most important national priorities.

As evidenced by this comprehensive overview, the Intelligence Community does not decide on its own which conversations to listen to, try to collect everything, or operate free from scrutiny. Its activities are focused on priorities set by policymakers, through a process that involves input from across the government, and that is overseen both within NSA and by the ODNI, Department of Justice, and Department of Defense.

PPD-28 also contains numerous other provisions to ensure that personal information collected pursuant to signals intelligence is protected, regardless of nationality. For instance,

---

[10] *See* www.dni.gov/clpo.

PPD-28 provides for data security, access, and quality procedures to protect personal information collected through signals intelligence, and provides for mandatory training to ensure that the workforce understands the responsibility to protect personal information, regardless of nationality. The PPD also provides for additional oversight and compliance mechanisms. These include periodic audit and reviews by appropriate oversight and compliance officials of the practices for protecting personal information contained in signals intelligence. The reviews also must examine the agencies' compliance with the procedures for protecting such information.

Additionally, PPD-28 provides that significant compliance issues related to non-U.S. persons will be addressed at senior levels of government. Should a significant compliance issue occur involving the personal information of any person collected as a result of signals intelligence activities, the issue must, in addition to any existing reporting requirements, be reported promptly to the DNI. If the issue involves the personal information of a non-U.S. person, the DNI, in consultation with the Secretary of State and the head of the relevant IC element, will determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel. Moreover, as directed by PPD-28, the Secretary of State has identified a senior official, Under Secretary Catherine Novelli, to serve as a point of contact for foreign governments that wish to raise concerns regarding signals intelligence activities of the United States. This commitment to high-level engagement exemplifies the efforts the U.S. government has made over the past few years to instill confidence in the numerous and overlapping privacy protections in place for U.S. person and non-U.S. person information.

e. ***Summary***

The United States' processes for collecting, retaining, and disseminating foreign intelligence provide important privacy protections for the personal information of all persons, regardless of nationality. In particular, these processes ensure that our Intelligence Community focuses on its national security mission as authorized by applicable laws, executive orders, and presidential directives; safeguards information from unauthorized access, use and disclosure; and conducts its activities under multiple layers of review and oversight, including by congressional oversight committees. PPD-28 and the procedures implementing it represent our efforts to extend certain minimization and other substantial data protection principles to the personal information of all persons regardless of nationality. Personal information obtained through U.S. signals intelligence collection is subject to the principles and requirements of U.S. law and Presidential direction, including the protections set forth in PPD-28. These principles and requirements ensure that all persons are treated with dignity and respect, regardless of their nationality or wherever they might reside, and recognize that all persons have legitimate privacy interests in the handling of their personal information.

II. Foreign Intelligence Surveillance Act – Section 702

Collection under Section 702 of the Foreign Intelligence Surveillance Act[11] is not "mass and indiscriminate" but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets; is clearly authorized by explicit statutory authority; and is subject to both independent judicial supervision and substantial review and oversight within

[11] 50 U.S.C. § 1881a.

the Executive Branch and Congress. Collection under Section 702 is considered signals intelligence subject to the requirements of PPD-28.[12]

Collection under Section 702 is one of the most valuable sources of intelligence protecting both the United States and our European partners. Extensive information about the operation and oversight of Section 702 is publicly available. Numerous court filings, judicial decisions and oversight reports relating to the program have been declassified and released on the ODNI's public disclosure website, www.icontherecord.tumblr.com. Moreover, Section 702 was comprehensively analyzed by the PCLOB, in a report which is available at https://www.pclob.gov/library/702-Report.pdf.[13]

Section 702 was passed as part of the FISA Amendments Act of 2008,[14] after extensive public debate in Congress. It authorizes the acquisition of foreign intelligence information through targeting of non-U.S. persons located outside the United States, with the compelled assistance of U.S. electronic communications service providers. Section 702 authorizes the Attorney General and the DNI – two Cabinet-level officials appointed by the President and confirmed by the Senate – to submit annual certifications to the FISA Court.[15] These certifications identify specific categories of foreign intelligence to be collected, such as intelligence related to counterterrorism or weapons of mass destruction, which must fall within the categories of foreign intelligence defined by the FISA statute.[16] As the PCLOB noted, "[t]hese limitations do *not* permit unrestricted collection of information about foreigners."[17]

The certifications also are required to include "targeting" and "minimization" procedures that must be reviewed and approved by the FISA Court.[18] The targeting procedures are designed to ensure that the collection takes place only as authorized by statute and is within the scope of the certifications; the minimization procedures are designed to limit the acquisition, dissemination, and retention of information about U.S. persons, but also contain provisions that provide substantial protection to information about non-U.S. persons as well, as described below. Moreover, as described above, in PPD-28 the President directed that the Intelligence Community

---

[12] The United States also may obtain court orders pursuant to other provisions of FISA for the production of data, including data transferred pursuant to the Privacy Shield. *See* 50 U.S.C. § 1801 *et seq.* Titles I and III of FISA, which respectively authorize electronic surveillance and physical searches, require a court order (except in emergency circumstances) and always require probable cause to believe that the target is a foreign power or an agent of a foreign power. Title IV of FISA authorizes the use of pen registers and trap and trace devices, pursuant to court order (except in emergency circumstances) in authorized foreign intelligence, counterintelligence, or counterterrorism investigations. Title V of FISA permits the FBI, pursuant to court order (except in emergency circumstances), to obtain business records that are relevant to an authorized foreign intelligence, counterintelligence, or counterterrorism investigations. As discussed below, the USA FREEDOM Act specifically prohibits the use of FISA pen register or business record orders for bulk collection, and imposes a requirement of a "specific selection term" to ensure that those authorities are used in a targeted fashion.

[13] Privacy and Civil Liberties Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (July 2, 2014) ("PCLOB Report").

[14] *See* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[15] *See* 50 U.S.C. § 1881a(a) and (b).

[16] *See id.* § 1801(e).

[17] *See* PCLOB Report at 99.

[18] *See* 50 U.S.C. § 1881a(d) and (e).

provide additional protections for personal information about non-U.S. persons, and those protections apply to information collected under Section 702.

Once the court approves the targeting and minimization procedures, collection under Section 702 is not bulk or indiscriminate, but "consists entirely of targeting specific persons about whom an individualized determination has been made," as the PCLOB said.[19] Collection is targeted through the use of individual selectors, such as email addresses or telephone numbers, which U.S. intelligence personnel have determined are likely being used to communicate foreign intelligence information of the type covered by the certification submitted to the court.[20] The basis for selection of the target must be documented, and the documentation for every selector is subsequently reviewed by the Department of Justice.[21] The U.S. Government has released information showing that in 2014 there were approximately 90,000 individuals targeted under Section 702, a miniscule fraction of the over 3 billion internet users throughout the world.[22]

Information collected under Section 702 is subject to the court-approved minimization procedures, which provide protections to non-U.S. persons as well as U.S. persons, and which have been publicly released.[23] For example, communications acquired under Section 702, whether of U.S. persons or non-U.S. persons, are stored in databases with strict access controls. They may be reviewed only by intelligence personnel who have been trained in the privacy-protective minimization procedures and who have been specifically approved for that access in order to carry out their authorized functions.[24] Use of the data is limited to identification of foreign intelligence information or evidence of a crime.[25] Pursuant to PPD-28, this information may be disseminated only if there is a valid foreign intelligence or law enforcement purpose; the mere fact that one party to the communication is not a U.S. person is not sufficient.[26] And the minimization procedures and PPD-28 also set limits on how long data acquired pursuant to Section 702 may be retained.[27]

Oversight of Section 702 is extensive, and is conducted by all three branches of our government. Agencies implementing the statute have multiple levels of internal review, including by independent Inspectors General, and technological controls over access to the data. The Department of Justice and the ODNI closely review and scrutinize the use of Section 702 to verify compliance with legal rules; agencies are also under an independent obligation to report

---

[19] *See* PCLOB Report at 111.

[20] *Id.*

[21] *Id.* at 8; 50 U.S.C. § 1881a(l); *see also* NSA Director of Civil Liberties and Privacy Report, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (hereinafter "NSA Report") at 4, *available at* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

[22] Director of National Intelligence 2014 Transparency Report, *available at* www.icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

[23] Minimization procedures available at: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf ("NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd 28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[24] *See* NSA Report at 4.

[25] *See, e.g.,* NSA Minimization Procedures at 6.

[26] Intelligence Agency PPD-28 procedures available at www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

[27] *See* NSA Minimization Procedures; PPD-28 Section 4.

potential incidents of noncompliance. Those incidents are investigated, and all compliance incidents are reported to the Foreign Intelligence Surveillance Court, the President's Intelligence Oversight Board, and Congress, and remedied as appropriate. [28] To date, there have been no incidents of willful attempts to violate the law or circumvent legal requirements. [29]

The FISA Court plays an important role in implementing Section 702. It is composed of independent federal judges who serve for a term of seven years on the FISA Court but who, like all federal judges, have life tenure as judges. As noted above, the Court must review the annual certifications and targeting and minimization procedures for compliance with the law. In addition, as also noted above, the Government is required to notify the Court immediately of compliance issues,[30] and several Court opinions have been declassified and released showing the exceptional degree of judicial scrutiny and independence it exercises in reviewing those incidents.

The Court's exacting processes have been described by its former Presiding Judge in a letter to Congress that has been publicly released.[31] And as a result of the USA FREEDOM Act, described below, the Court is now explicitly authorized to appoint an outside lawyer as an independent advocate on behalf of privacy in cases that present novel or significant legal issues.[32] This degree of involvement by a country's independent judiciary in foreign intelligence activities directed at persons who are neither citizens of that country nor located within it is unusual if not unprecedented, and helps ensure that Section 702 collection occurs within appropriate legal limits.

Congress exercises oversight through statutorily required reports to the Intelligence and Judiciary Committees, and frequent briefings and hearings. These include a semiannual report by the Attorney General documenting the use of Section 702 and any compliance incidents; [33] a separate semiannual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures designed to ensure that collection is for a valid foreign intelligence purpose;[34] and an annual report by heads of intelligence elements which includes a certification that collection under Section 702 continues to produce foreign intelligence information.[35]

In short, collection under Section 702 is authorized by law; is subject to multiple levels of review, judicial supervision and oversight; and, as the FISA Court stated in a recently

---

[28] *See* 50 U.S.C. § 1881(l); *see also* PCLOB Report at 66-76.

[29] *See* Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence at 2-3, *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

[30] Rule 13 of the Foreign Intelligence Surveillance Court Rules of Procedures, *available at* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

[31] July 29, 2013 Letter from The Honorable Reggie B. Walton to The Honorable Patrick J. Leahy, *available at* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

[32] *See* Section 401 of the USA FREEDOM Act, P.L. 114-23.

[33] *See* 50 U.S.C. § 1881f.

[34] *See id.* § 1881a(l)(1).

[35] *See id.* § 1881a(l)(3). Some of these reports are classified.

declassified opinion, is "not conducted in a bulk or indiscriminate manner," but "through . . . discrete targeting decisions for individual [communication] facilities."[36]

III. USA FREEDOM Act

The USA FREEDOM Act, signed into law in June 2015, significantly modified U.S. surveillance and other national security authorities, and increased public transparency on the use of these authorities and on decisions of the FISA Court, as set out below.[37] The Act ensures that our intelligence and law enforcement professionals have the authorities they need to protect the Nation, while further ensuring that individuals' privacy is appropriately protected when these authorities are employed. It enhances privacy and civil liberties and increases transparency.

The Act prohibits bulk collection of any records, including of both U.S. and non-U.S. persons, pursuant to various provisions of FISA or through the use of National Security Letters, a form of statutorily authorized administrative subpoenas.[38] This prohibition specifically includes telephone metadata relating to calls between persons inside the U.S. and persons outside the U.S., and would also include collection of Privacy Shield information pursuant to these authorities. The Act requires that the government base any application for records under those authorities on a "specific selection term"—a term that specifically identifies a person, account, address, or personal device in a way that limits the scope of information sought to the greatest extent reasonably practicable.[39] This further ensures that collection of information for intelligence purposes is precisely focused and targeted.

The Act also made significant modifications to proceedings before the FISA Court, which both increase transparency and provide additional assurances that privacy will be protected. As noted above, it authorized creation of a standing panel of security-cleared lawyers with expertise in privacy and civil liberties, intelligence collection, communications technology, or other relevant areas, who may be appointed to appear before the court as *amicus curiae* in cases that involve significant or novel interpretations of law. These lawyers are authorized to make legal arguments that advance the protection of individual privacy and civil liberties, and will have access to any information, including classified information, that the court determines is necessary to their duties.[40]

---

[36] Mem. Opinion and Order at 26 (FISC 2014), *available at* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

[37] *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.

[38] *See id.* §§ 103, 201, 501. National Security Letters are authorized by a variety of statutes and allow the FBI to obtain information contained in credit reports, financial records, and electronic subscriber and transaction records from certain kinds of companies, only to protect against international terrorism or clandestine intelligence activities. *See* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. National Security Letters are typically used by the FBI to gather critical non-content information at the early phases of counterterrorism and counterintelligence investigations – such as the identity of the subscriber to an account who may have been communicating with agents of a terrorist group such as ISIL. Recipients of a National Security Letter have the right to challenge them in court. *See* 18 U.S.C. § 3511.

[39] *See* USA FREEDOM Act § 107.

[40] *See id.* § 401.

The Act also builds on the U.S. Government's unprecedented transparency about intelligence activities by requiring the DNI, in consultation with the Attorney General, to either declassify, or publish an unclassified summary of, each decision, order, or opinion issued by the FISA Court or the Foreign Intelligence Surveillance Court of Review that includes a significant construction or interpretation of any provision of law.

Moreover, the Act provides for extensive disclosures about FISA collection and National Security Letter requests. The United States must disclose to Congress and to the public each year the number of FISA orders and certifications sought and received; estimates of the number of U.S. persons and non-U.S. persons targeted and affected by surveillance; and the number of appointments of *amici curiae*, among other items of information.[41] The Act also requires additional public reporting by the government about the numbers of National Security Letter requests about both U.S. and non-U.S. persons.[42]

With regard to corporate transparency, the Act gives companies a range of options to report publicly the aggregate number of FISA orders and directives or National Security Letters they receive from the Government, as well as the number of customer accounts targeted by these orders.[43] Several companies have already made such disclosures, which have revealed the limited number of customers whose records have been sought.

These corporate transparency reports demonstrate that U.S. intelligence requests affect only a miniscule fraction of data. For example, one major company's recent transparency report shows that it received national security requests (pursuant to FISA or National Security Letters) affecting fewer than 20,000 of its accounts, at a time when it had at least 400 million subscribers. In other words, all U.S. national security requests reported by this company affected fewer than .005% of its subscribers. Even if every one of those requests had concerned Safe Harbor data, which of course is not the case, it is obvious that the requests are targeted and appropriate in scale, and are neither bulk nor indiscriminate.

Finally, while the statutes which authorize National Security Letters already restricted the circumstances under which a recipient of such a letter could be barred from disclosing it, the Act further provided that such non-disclosure requirements must be reviewed periodically; required that recipients of National Security Letters be notified when the facts no longer support a non-disclosure requirement; and codified procedures for recipients to challenge nondisclosure requirements.[44]

In sum, the USA FREEDOM Act's important amendments to U.S. intelligence authorities are clear evidence of the extensive effort taken by the United States to place the protection of personal information, privacy, civil liberties, and transparency at the forefront of all U.S. intelligence practices.

---

[41] *See id.* § 602.
[42] *See id.*
[43] *See id.* § 603.
[44] *See id.* §§ 502, 503.

IV. Transparency

In addition to the transparency mandated by the USA FREEDOM Act, the U.S. Intelligence Community provides the public much additional information, setting a strong example with respect to transparency into its intelligence activities. The Intelligence Community has published many of its policies, procedures, Foreign Intelligence Surveillance Court decisions, and other declassified materials, providing an extraordinary degree of transparency. In addition, the Intelligence Community has substantially increased its disclosure of statistics on the government's use of national security collection authorities. On April 22, 2015, the Intelligence Community issued its second annual report presenting statistics on how often the government uses these important authorities. ODNI also has published, on the ODNI website and on *IC On the Record*, a set of concrete transparency principles[45] and an implementation plan that translates the principles into concrete, measurable initiatives.[46] In October 2015, the Director of National Intelligence directed that each intelligence agency designate an Intelligence Transparency Officer within its leadership to foster transparency and lead transparency initiatives.[47] The Transparency Officer will work closely with each intelligence agency's Privacy and Civil Liberties Officer to ensure that transparency, privacy, and civil liberties continue to remain top priorities.

As an example of these efforts, NSA's Chief Privacy and Civil Liberties Officer has released several unclassified reports over the past few years, including reports on activities under section 702, Executive Order 12333, and the USA FREEDOM Act.[48] In addition, the IC works closely with the PCLOB, Congress, and the U.S. privacy advocacy community to provide further transparency relating to U.S. intelligence activities, wherever feasible and consistent with the protection of sensitive intelligence sources and methods. Taken as a whole, U.S. intelligence activities are as transparent as or more transparent than those of any other nation in the world and are as transparent as it is possible to be consistent with the need to protect sensitive sources and methods.

To summarize the extensive transparency that exists about U.S. intelligence activities:

- The IC has released and posted online thousands of pages of court opinions and agency procedures outlining the specific procedures and requirements of our intelligence activities. We have also released reports on intelligence agencies' compliance with applicable restrictions.
- Senior intelligence officials regularly speak publicly about the roles and activities of their organizations, including descriptions of the compliance regimes and safeguards that govern their work.

---

[45] *Available at* http:\\www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

[46] *Available at* http:\\www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.

[47] *See id.*

[48] *Available at* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

- The IC released numerous additional documents about intelligence activities pursuant to our Freedom of Information Act.
- The President issued PPD-28, publicly setting out additional restrictions on our intelligence activities, and ODNI has issued two public reports on the implementation of those restrictions.
- The IC is now required by law to release significant legal opinions issued by the FISA Court, or summaries of those opinions.
- The government is required to report annually on the extent of its use of certain national security authorities, and companies are authorized to do so as well.
- The PCLOB has issued several detailed public reports on intelligence activities, and will continue to do so.
- The IC provides extensive classified information to Congressional oversight committees.
- The DNI issued transparency principles to govern the activities of the Intelligence Community.

This extensive transparency will continue going forward. Any information that is released publicly will, of course, be available to both the Department of Commerce and the European Commission. The annual review between Commerce and the European Commission on the implementation of the Privacy Shield will provide an opportunity for the European Commission to discuss any questions raised by any new information released, as well as any other matters concerning the Privacy Shield and its operation, and we understand that the Department may, in its discretion, invite representatives of other agencies, including the IC, to participate in that review. This is, of course, in addition to the mechanism provided in PPD-28 for EU Member States to raise surveillance-related concerns with a designated State Department official.

V. Redress

U.S. law provides a number of avenues of redress for individuals who have been the subject of unlawful electronic surveillance for national security purposes. Under FISA, the right to seek relief in U.S. court is not limited to U.S. persons. An individual who can establish standing to bring suit would have remedies to challenge unlawful electronic surveillance under FISA. For example, FISA allows persons subjected to unlawful electronic surveillance to sue U.S. government officials in their personal capacities for money damages, including punitive damages and attorney's fees. *See* 50 U.S.C. § 1810. Individuals who can establish their standing to sue also have a civil cause of action for money damages, including litigation costs, against the United States when information about them obtained in electronic surveillance under FISA has been unlawfully and willfully used or disclosed. *See* 18 U.S.C. § 2712. In the event the government intends to use or disclose any information obtained or derived from electronic surveillance of any aggrieved person under FISA against that person in judicial or administrative proceedings in the United States, it must provide advance notice of its intent to the tribunal and the person, who may then challenge the legality of the surveillance and seek to suppress the information. *See* 50 U.S.C. § 1806. Finally, FISA also provides criminal penalties for individuals who intentionally engage in unlawful electronic surveillance under color of law or who intentionally use or disclose information obtained by unlawful surveillance. *See* 50 U.S.C. § 1809.

EU citizens have other avenues to seek legal recourse against U.S. government officials for unlawful government use of or access to data, including government officials who violate the law in the course of unlawful access to or use of information for purported national security purposes. The Computer Fraud and Abuse Act prohibits intentional unauthorized access (or exceeding authorized access) to obtain information from a financial institution, a U.S. government computer system, or a computer accessed via the Internet, as well as threats to damage protected computers for purposes of extortion or fraud. *See* 18 U.S.C. § 1030. Any person, of whatever nationality, who suffers damage or loss by reason of a violation of this law may sue the violator (including a government official) for compensatory damages and injunctive or other equitable relief under section 1030(g), regardless of whether a criminal prosecution has been pursued, provided the conduct involves at least one of several circumstances set forth in the statute. The Electronic Communications Privacy Act (ECPA) regulates government access to stored electronic communications and transactional records and subscriber information held by third-party communications providers. *See* 18 U.S.C. §§ 2701-2712. ECPA authorizes an aggrieved individual to sue government officials for intentional unlawful access to stored data. ECPA applies to all persons regardless of citizenship and aggrieved persons may receive damages and attorney's fees. The Right to Financial Privacy Act (RFPA) limits the U.S. government's access to the bank and broker-dealer records of individual customers. *See* 12 U.S.C. §§ 3401-3422. Under the RFPA, a bank or broker-dealer customer can sue the U.S. government for statutory, actual, and punitive damages for wrongfully obtaining access to the customer's records, and a finding that such wrongful access was willful automatically triggers an investigation of possible disciplinary action against the relevant government employees. *See* 12 U.S.C. § 3417.

Finally, the Freedom of Information Act (FOIA) provides a means for any person to seek access to existing federal agency records on any topic subject to certain categories of exemptions. *See* 5 U.S.C. § 552(b). These include limits on access to classified national security information, personal information of other individuals and information concerning law enforcement investigations, and are comparable to the limitations imposed by nations with their own information access laws. These limitations apply equally to Americans and non-Americans. Disputes over the release of records requested pursuant to FOIA can be appealed administratively and then in federal court. The court is required to make a de novo determination of whether records are properly withheld, 5 U.S.C. § 552(a)(4)(B), and can compel the government to provide access to records. In some cases courts have overturned government assertions that information should be withheld as classified.[49] Although no monetary damages are available, courts can award attorney's fees.

VI. Conclusion

The United States recognizes that our signals intelligence and other intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or place of residence, and that all persons have legitimate privacy interests in the handling of their personal information. The United States only uses signals intelligence to advance its national security and foreign policy interests and to protect its citizens and the

[49] *See, e.g., New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

citizens of its allies and partners from harm. In short, the IC does not engage in indiscriminate surveillance of anyone, including ordinary European citizens. Signals intelligence collection only takes place when duly authorized and in a manner that strictly complies with these limitations; only after consideration of the availability of alternative sources, including from diplomatic and public sources; and in a manner that prioritizes appropriate and feasible alternatives. And wherever practicable, signals intelligence only takes place through collection focused on specific foreign intelligence targets or topics through the use of discriminants.

U.S. policy in this regard was affirmed in PPD-28. Within this framework, U.S. intelligence agencies do not have the legal authority, the resources, the technical capability or the desire to intercept all of the world's communications. Those agencies are not reading the emails of everyone in the United States, or of everyone in the world. Consistent with PPD-28, the United States provides robust protections to the personal information of non-U.S. persons that is collected through signals intelligence activities. To the maximum extent feasible consistent with the national security, this includes policies and procedures to minimize the retention and dissemination of personal information concerning non-U.S. persons comparable to the protections enjoyed by U.S. persons. Moreover, as discussed above, the comprehensive oversight regime of the targeted Section 702 FISA authority is unparalleled. Finally, the significant amendments to U.S. intelligence law set forth in the USA FREEDOM Act and the ODNI-led initiatives to promote transparency within the Intelligence Community greatly enhance the privacy and civil liberties of all individuals, regardless of their nationality.

Sincerely,

Robert S. Litt

ANNEX VII

U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General *Washington, D.C. 20530*

February 19, 2016

Mr. Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Mr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Dear Mr. Antonipillai and Mr. Dean:

This letter provides a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities.[1] These legal processes are nondiscriminatory in that they are used to obtain information from corporations in the United States, including from companies that will self-certify through the US/EU Privacy Shield framework, without regard to the nationality of the data subject. Further, corporations that receive legal process in the United States may challenge it in court as discussed below.[2]

Of particular note with respect to the seizure of data by public authorities is the Fourth Amendment to the United States Constitution, which provides that "[t]he right of the people to

[1] This overview does not describe the national security investigative tools used by law enforcement in terrorism and other national security investigations, including National Security Letters (NSLs) for certain record information in credit reports, financial records, and electronic subscriber and transaction records, *see* 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, and for electronic surveillance, search warrants, business records, and other collection of communications pursuant to the Foreign Intelligence Surveillance Act, *see* 50 U.S.C. § 1801 *et seq.*

[2] This paper discusses federal law enforcement and regulatory authorities; violations of state law are investigated by states and are tried in state courts. State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to protections provided by State constitutions that exceed those of the U.S. Constitution. State law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment.

be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the United States Supreme Court stated in *Berger v. State of New York*, "[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." 388 U.S. 41, 53 (1967) (*citing Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). In domestic criminal investigations, the Fourth Amendment generally requires law enforcement officers to obtain a court-issued warrant before conducting a search. *See Katz v. United States*, 389 U.S. 347, 357 (1967). When the warrant requirement does not apply, government activity is subject to a "reasonableness" test under the Fourth Amendment. The Constitution itself, therefore, ensures that the U.S. government does not have limitless, or arbitrary, power to seize private information.

Criminal Law Enforcement Authorities:

Federal prosecutors, who are officials of the Department of Justice (DOJ), and federal investigative agents including agents of the Federal Bureau of Investigation (FBI), a law enforcement agency within DOJ, are able to compel production of documents and other record information from corporations in the United States for criminal investigative purposes through several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities.

Grand Jury or Trial Subpoenas: Criminal subpoenas are used to support targeted law enforcement investigations. A grand jury subpoena is an official request issued from a grand jury (usually at the request of a federal prosecutor) to support a grand jury investigation into a particular suspected violation of criminal law. Grand juries are an investigative arm of the court and are impaneled by a judge or magistrate. A subpoena may require someone to testify at a proceeding, or to produce or make available business records, electronically stored information, or other tangible items. The information must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. A recipient can file a motion to challenge a subpoena based on those grounds. *See* Fed. R. Crim. P. 17. In limited circumstances, trial subpoenas for documents may be used after the case has been indicted by the grand jury.

Administrative Subpoena Authority: Administrative subpoena authorities may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorize the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies. If the government seeks to enforce an administrative subpoena in court, the recipient of the administrative subpoena, like the recipient of a grand jury subpoena, can argue that the subpoena is unreasonable because it is overbroad, or because it is oppressive or burdensome.

Court Orders For Pen Register and Trap and Traces: Under criminal pen register and trap-and-trace provisions, law enforcement may obtain a court order to acquire real-time, non-content dialing, routing, addressing, and signaling information about a phone number or email upon certification that the information provided is relevant to a pending criminal investigation. *See* 18 U.S.C. §§ 3121-3127. The use or installation of such a device outside the law is a federal crime.

Electronic Communications Privacy Act (ECPA): Additional rules govern the government's access to subscriber information, traffic data, and stored content of communications held by ISPs, telephone companies, and other third-party service providers, pursuant to Title II of ECPA, also called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712. The SCA sets forth a system of statutory privacy rights that limit law enforcement access to data beyond what is required under constitutional law from customers and subscribers of Internet service providers. The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection. For subscriber registration information, IP addresses and associated time stamps, and billing information, criminal law enforcement authorities must obtain a subpoena. For most other stored, non-content information, such as email headers without the subject line, law enforcement must present specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. To obtain the stored content of electronic communications, generally, criminal law enforcement authorities obtain a warrant from a judge based on probable cause to believe the account in question contains evidence of a crime. The SCA also provides for civil liability and criminal penalties.

Court Orders for Surveillance Pursuant to Federal Wiretap Law: Additionally, law enforcement may intercept in real time wire, oral, or electronic communications for criminal investigative purposes pursuant to the federal wiretap law. *See* 18 U.S.C. §§ 2510-2522. This authority is available only pursuant to a court order in which a judge finds, *inter alia*, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution. The statute provides for civil liability and criminal penalties for violations of the wiretapping provisions.

Search Warrant – Rule 41: Law enforcement can physically search premises in the United States when authorized to do so by a judge. Law enforcement must demonstrate to the judge based on a showing of "probable cause" that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. This authority is often used when a physical search by police of a premise is needed due to the danger that evidence may be destroyed if a subpoena or other production order is served on the corporation. *See* U.S. Const. amend. IV (discussed in further detail above); Fed. R. Crim. P. 41. The subject of a search warrant may move to quash the warrant as overbroad, vexatious, or otherwise improperly obtained, and aggrieved parties with standing may move to suppress any evidence obtained in an unlawful search. *See Mapp v. Ohio*, 367 U.S. 643 (1961).

DOJ Guidelines and Policies: In addition to these Constitutional, statutory, and rule-based limitations on government access to data, the Attorney General has issued guidelines that place further limits on law enforcement access to data, and that also contain privacy and civil

liberty protections. For instance, the Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (September 2008) (hereinafter AG FBI Guidelines), available at http://www.justice.gov/archive/opa/docs/guidelines.pdf, set limits on use of investigative means to seek information related to investigations that involve federal crimes. These guidelines require that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties and the potential damage to reputation. Further, they note that "it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." *See* AG FBI Guidelines at 5. The FBI has implemented these guidelines through the FBI Domestic Investigations and Operations Guide (DIOG), available at https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), a comprehensive manual that includes detailed limits on use of investigative tools and guidance to assure that civil liberties and privacy are protected in every investigation. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the *United States Attorneys' Manual* (USAM), also available online at http://www.justice.gov/usam/united-states-attorneys-manual.

Civil and Regulatory Authorities (Public Interest):

There are also significant limits on civil or regulatory (*i.e.*, "public interest") access to data held by corporations in the United States. Agencies with civil and regulatory responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible items. These agencies are limited in their exercise of administrative or civil subpoena authority not only by their organic statutes, but also by independent judicial review of subpoenas prior to potential judicial enforcement. *See, e.g.*, Fed. R. Civ. P. 45. Agencies may seek access only to data that is relevant to matters within their scope of authority to regulate. Further, a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court by presenting evidence that the agency has not acted in accordance with basic standards of reasonableness, as discussed earlier.

There are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess. For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations. *See* 31 U.S.C. § 5318; 31 C.F.R. Part X. Other businesses can rely on the Fair Credit Reporting Act, *see* 15 U.S.C. § 1681b, or a host of other sector specific laws. Misuse of an agency's subpoena authority can result in agency liability, or personal liability for agency officers. *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422. Courts in the United States thus stand as the guardians against improper regulatory requests and provide independent oversight of federal agency actions.

Finally, any statutory power that administrative authorities have to physically seize records from a company in the United States pursuant to an administrative search must meet the requirements of the Fourth Amendment. *See See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusion:

All law enforcement and regulatory activities in the United States must conform to applicable law, including the U.S. Constitution, statutes, rules, and regulations. Such activities must also comply with applicable policies, including any Attorney General Guidelines governing federal law enforcement activities. The legal framework described above limits the ability of U.S. law enforcement and regulatory agencies to acquire information from corporations in the United States -- whether the information concerns U.S. persons or citizens of foreign countries -- and in addition permits judicial review of any government requests for data pursuant to these authorities.

Sincerely,

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs