THE TFTP AGREEMENT, SCHREMS RIGHTS, AND THE SAUGMANDSGAARD REQUIREMENTS

Two important developments have clarified EU law on agreements between the European Union and third-countries in the field of data protection, national security, and law-enforcement: (1) the *Schrems* case[1] by the Court of Justice of the European Union (CJEU) and (2) the opinion of EU Advocate General Saugmandsgaard øe on the joined cases of *Post-och telestyrelsen* and *Tom Watson*.[2] Both have important implications for the EU-US Agreement on Financial Messaging Data for the purpose of the US Terrorist Finance Tracking Program (TFTP Agreement).[3] This article examines some of these implications.

Schrems sets out the basic data protection and redress rights that EU agreements with third countries must make available to EU individuals with regards to the conduct of public bodies, notably where these bodies transfer personal data, including financial messaging data, out of the European Union for law-enforcement or national security purposes (the *Schrems* rights). The opinion of EU Advocate General Saugmandsgaard øe clarifies the mandatory requirements that must be met when European Union measures authorize the generalized retention of personal data and allow public bodies to access this data to combat serious crime or national security threats, such as those related to the financing of terrorism (the Saugmandsgaard requirements).

The compatibility of EU-US agreements in the field of data protection with *Schrems* has been examined widely. There has been particular focus on the recent, EU-US Privacy Shield, which regulates the transfer of EU personal data to the United States for commercial, law-enforcement and national security purposes. Other recent

agreements, such as the Umbrella Agreement, have received less attention while others, such as the TFTP Agreement, have been left largely unexamined. This article will remedy this by evaluating the compatibility of the TFTP Agreement with *Schrems* and the opinion of Saugmandsgaard[4] on the joined case of *Post-och telestyrelsen* and *Tom Watson and others* (C-698/15).

The Regulatory Scope of the TFTP Agreement

The TFTP Agreement regulates how the US Department of the Treasury (US Treasury) can request the transfer of the financial messaging data of EU individuals to the United States.[5] It makes available to EU individuals certain data protection and redress rights.[6] It governs and places restrictions on how the US Treasury can access this data as part of its Terrorist Finance Tracking Program.[7] The program monitors international financial transactions so as to investigate, prevent, or prosecute offenses related to terrorism or its financing.[8] Specifically, the US Treasury maintains databases with identifiers connected to persons it suspects of having committed offenses related to terrorism or its financing. It then searches for and monitors financial transactions connected to these identifiers by, among other things, collecting data from financial institutions and providers of international financial-messaging and payments processing services.

The TFTP Agreement was signed before the *Schrems* case, the Saugmandsgaard opinion, and importantly, the disclosure of the PRISM program. The program was, among many other things, a secret and classified US program to collect, retain in a generalized way, and provide the means for US national security and law-enforcement bodies to access the personal data of foreign individuals transmitted or stored in the United States.[9] It was justified as a reasonable and lawful means to protect US objectives of general interest, such as the need to protect US national

security, combat serious crime such as international terrorism, and gather foreign intelligence information.[10] However, it did this by retaining and accessing EU personal data that were transferred to the United States by US companies operating in the United States under the terms of an EU-US agreement on data transfers: The Safe Harbor Framework.[11] The public disclosure of PRISM resulted in much criticism of US conduct and the operation of the Safe Harbor Framework from EU civil rights and data protection institutions.[12]

The EU Commission investigated PRISM for its compatibility with the terms of the Framework and deemed the program to have gone "beyond what was strictly necessary and proportionate"[13] under the terms of the Framework; particularly under the terms of the national security and law-enforcement exemptions in the Framework that the United States relied on to justify the program. The CJEU in the *Schrems* case agreed with the EU Commission and invalidated the Safe Harbor Framework because of this criticism and on other grounds, notably because it did not adequately safeguard EU fundamental rights or make available to EU individuals certain data protection and redress rights.[14]

Schrems and the disclosure of PRISM led to the European Union and United States signing a new agreement on the transfer of EU personal data to the United States for commercial, law-enforcement, and national security purposes; the Privacy Shield.[15] The agreement has sought to provide *Schrems* rights to EU individuals and deal with other criticisms made by the CJEU in the *Schrems* judgment about the Safe Harbor Framework. The European Union and the United States also have signed an "Umbrella Agreement"[16] on the transfer of EU personal data to the United States for law-enforcement purposes. It too seeks to provide EU individuals with *Schrems* rights

whenever their personal data is transferred to the United States under the terms of an EU-US agreement for law-enforcement purposes.[17]

The TFTP Agreement is not one of these recent agreements, and it was not signed with *Schrems* rights in mind. It can therefore be argued that it is not appropriate to evaluate it in the light of this case, or for that matter, the Saugmandsgaard requirements. However, given that *Schrems* (and to a lesser extent the Saugmandsgaard opinion) is the current law with regards to EU agreements with third countries in the field of data protection and law-enforcement, this article does examine the TFTP Agreement in the light of *Schrems* and Saugmandsgaard requirements. This is because many of the issues that have influenced the shape and content of the Privacy Shield and Umbrella Agreement, and indeed much of the judgment of the CJEU in *Schrems*, also influenced negotiations concerning the drafting and signing of the TFTP Agreement. As will be shown, the TFTP Agreement came out of the public disclosure of the Terrorist Finance Tracking Program, which, like PRISM, also secretly collected, retained, and accessed the personal data of EU individuals transmitted to the United States.[18]

It is argued that the TFTP Agreement generally makes available to EU individuals the required *Schrems* rights—with the exception of the right of individuals to request access to and the rectification of personal data collected about them, which are not made available in the agreement. It also is suggested that the TFTP meets most of the Saugmandsgaard requirements. However, it is not argued that the noted limitations concerning the TFTP with regards to the absence of access and rectification rights, in of themselves, render the agreement invalid. Instead, it is suggested how the agreement can be made more *Schrems* compliant by giving EU individuals legal standing under the US Privacy Act[19] through the US Judicial Redress Act.[20]

EU Law on Data Protection: *Schrems* Rights and Augmandsgaard Requirements

Personal data is defined in EU law as any information about an identified or identifiable individual. That is, information that allows for individuals to be identified, directly or indirectly, by way of a reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to an individual.[21] The definition is expansive and can therefore encompass "metadata," that is, information about electronic communications, their source, transmission, storage, or routing.[22]

Using the example of a bank account, metadata encompasses information about the owner (*e.g.*, billing and correspondence information) and data about interactions that take place through this account. This might include billing and corresponding information about external accounts and entities that interact with or are connected to this account; such as, information about the time, duration, location, frequency, volume, methods and form of these interactions. This therefore includes information about whether these interactions take place across border, and if so where, for how long, and in what form (*e.g.*, cash, online, card, cheque, credit, debit, and etc.). All such information can be structured, formatted, and retained in massive, searchable, relational databases that allow for algorithmic and automated processing and analysis or, in other words, data mining.[23]

Databases containing the time and location of financial transactions can be related to databases about correspondence and billing information. These databases can be further examined for their relations or connections with other sets of databases containing lists of, for example, names or account numbers associated with individuals or groups which are of interest to law-enforcement or national security bodies.[24]

Relational and searchable databases allow for one personal identifier (say an account number) to be searched for or connected to a wider set of other interconnected databases. Combining many databases together and searching across them can reveal a great deal of information about relationships that are not apparent when each database is examined in isolation.[25] Thus, when combined and examined relationally, especially through automated means and software, these databases and the metadata they contain can reveal much about individuals and their financial connections and social and political networks. Metadata can therefore be as, or even more revealing than content data; that is, the actual numbers and sums that are contained in a bank account in that, as Advocate General Saugmandsgaard øe has noted, the retention of metadata can allow for "the almost instantaneous cataloguing of entire populations" [26] and their electronic activity and relationships.

EU law affords EU individuals certain fundamental rights to data protection and redress. They have the right to consent before their personal data, including metadata, is collected and they have the right to request access to or the rectification or erasure of this data once collected.[27] They also have the right to a remedy and judicial protection when these and other fundamental rights, such as the right to privacy, are infringed;[28] individuals have the right to privacy over their private communications and personal data.[29] EU Member States and institutions are obligated to safeguard, monitor, and enforce compliance with, and provide a mechanism for individuals to make complaints regarding the infringements of these rights.[30] They are recognized as fundamental rights under EU law. Accordingly, all EU measures, including international agreements with third countries, must comply with them.[31]

EU law does not prohibit but regulates the transfer of EU personal data to third countries. The EU Commission has powers under EU law to decide on the adequacy

of data protection in third-countries and, where certain conditions are met, enter into data transfer agreements with them.[32] These decisions and agreements may authorize the transfer of EU personal data to third-countries without the need for national licenses (among other methods, such as binding corporate rules and standard contractual clauses). Such agreements can authorize such transfers for law-enforcement or national security purposes.[33] They must, however, be compatible with EU fundamental rights to privacy, data protection, and redress. Compatibility with these rights is a precondition for the validity of these agreements.[34]

How these agreements can be made compatible with the fundamental rights of EU individuals to data protection and redress was provided in the *Schrems* case. It requires that all EU data transfer agreements with third countries must make available to EU individuals certain fundamental rights. This includes the right to request access to and the rectification of personal data collected about them under the terms of such agreements.[35] It also requires that they have a right to a remedy, administrative appeal, and judicial review where these rights are denied, particularly on grounds of national security or law-enforcement.[36] Additionally, it requires that EU Member States have the power to monitor and investigate complaints from individuals about breaches of their fundamental rights.[37] These are the so-called *Schrems* rights.

Rights to data protection and privacy are not, however, absolute. They are qualified and can be limited for purposes of general interest, such as the need to prevent and prosecute criminal offenses or protect national security.[38] For such purposes, EU Member States and institutions are not prohibited from passing measures that authorize or require providers of electronic communications services, including those dealing with financial payments data, to retain all or some metadata relating to communications effected by the users of their services.[39] Such a measure

could involve the retention of data in a generalized manner of a great many, if not all persons. This would include all means of electronic communication, as well as all traffic data. The retention of such data could result in the persons whose data are retained being placed in a situation which is liable to result in criminal prosecution.[40] It therefore applies even to persons for whom there is no evidence suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.[41] Such measures are subject to strict, mandatory requirements as defined and argued for by EU Advocate General Saugmandsgaard øe on the joined cases of Post-och telestyrelsen and Tom Watson.[42]

According to the Advocate General on his reading of the seminal case of *Digital Rights Ireland*, such measures must be based on a law that is sufficiently clear to allow individuals to regulate their conduct, even if with the need of legal advice.[43] It must be demonstrated that it is strictly necessary for purposes of general interest and must be shown to be the most appropriate and proportionate means of achieving this purpose.[44] It is necessary to demonstrate that a measure is the most effective among viable options in terms of combating *serious* crime or threats to national security. Such measures also must intrude the least on fundamental rights. Proportionality requires a determination as to which objectives of general interest take priority where they are in conflict. It requires such a determination to be made in light of the established, strict necessity of a measure of general interest and the values and expectations of democratic society. Necessity asks whether a measure is relatively effective, in effect whether it has a strong operational case to combat serious crime when compared with other available options. Furthermore, proportionality entails a balancing of this necessity with and against the need to safeguard fundamental rights and the values and expectations of a democratic society. The results of these assessments must,

however, observe the essence of the fundamental rights to privacy and data protection.[45] This means public measures cannot allow for the generalized retention and accessing of personal data, particularly content data. Such generalized access to content does not observe the essence of fundamental rights. [46]

Instead, access to data retained in a generalized way must be subject to strict conditions or mandatory requirements (these are the so-called Saugmandsgaard requirements).[47] Such access is allowed only on the basis of a reasoned request from a law-enforcement and national security body and on prior review carried out by a court or by an independent administrative body.[48] Access to data retained in a generalized way must be authorized externally by an entity independent from the public body seeking access to this data. Such an entity must limit access to what is strictly necessary for the purpose of combating a defined list of serious crime or national security threats. The need for such safeguards is all the greater where personal data are subjected to automatic processing, such as datamining and algorithmic filtering, and where there is a significant risk of unlawful access to that data.[49]

Consequently, the question of when and how public bodies can access data, particularly huge metadata sets, retained in a generalized way in searchable and relational databases is of “decisive importance”[50] when assessing the compatibility of public measures with fundamental rights. Increasingly, the question is not about whether data is collected and retained in a generalized way, but more on how it is accessed or made accessible to public bodies for purposes of generalized interest, such as combating serious crime.

Accordingly, all EU agreements with third-countries in the field of data protection, national security, and law-enforcement (such as the TFTP Agreement)

must ensure that they are compatible with EU fundamental rights. They must particularly ensure that they make available to EU individuals the *Schrems* rights and comply with the Saugmandsgaard requirements. The next sections describe the TFTP Agreement and examine whether it makes available these rights or complies with these requirements.

The History of the TFTP Agreement

Following the September 11, 2001 attacks on the United States by al Qaeda, the US Treasury established a secret, classified Terrorist Finance Tracking Program (TFTP).[51] Its objective was to collect metadata on and monitor the financial transactions of persons and entities the US Treasury suspected of being involved in terrorism-related offenses or their financing. A list of such persons and identifiers associated with them were retained in electronic databases. This was then connected to and used to search other databases that retained metadata about financial transactions collected from providers of international financial messaging and payments processing services. This was mostly done by the US Treasury issuing administrative subpoenas (the so-called national security letters)[52] on the US branch of SWIFT (the Society for Worldwide Interbank Financial Telecommunications). SWIFT was compelled to transfer financial-messaging and payments data to the US treasury.[53] It was not, outside very narrow exceptions, allowed to disclose publically the issuing of these subpoenas.[54]

SWIFT is a company located in Belgium and is the global, market-leader in the provision of international financial messaging services. It runs a telecommunications network, administers datacenters, and owns the proprietary software through which most international financial institutions and payment-clearing providers transmit, route, receive, and exchange their financial messages and payment instructions; some

10,000 organizations across 216 countries subscribe to and use SWIFT's services for these purposes.[55] Prior to 2010, SWIFT stored the content and metadata on electronic transactions through its network in two operational centers or datacenters in the European Union and the United States. Both centers retained identical copies of this metadata and included data on EU-originating messages and instructions. By issuing administrative subpoenas on the US branch and operation center of SWIFT, the US Treasury was thereby able to gain access to EU-originating messages and other global transactions transmitted from outside the European Union, but routed through its SWIFT's operating center in the European Union.[56]

The existence of the Terrorist Finance Tracking Program was disclosed in 2006 in media reports and attracted strong condemnation and much criticism from the EU Parliament. This resulted in the United States making unilateral undertakings (TFTP Representations) in 2007 to the European Union. It undertook to only access EU-originating messages for counter-terrorism purposes and only to access these messages where it had pre-existing information that they had a "terrorism nexus." The Unite States also undertook to not subject EU-originating data to data mining. That is, the random searches of interconnected databases to see what relationships and connections are revealed.[57]

In the following year, the European Union appointed an "eminent European person," Judge Bruguiere, to review US compliance with its undertaking and publish a report on his findings. He published reports in 2009 and 2010. Both of them concluded that the United States complied with its undertaking and found that the Terrorist Finance Tracking Program generated important intelligence leads for the counter-terrorism activities of the United States and, indeed, many EU Member States

(the United States shared some 1400 intelligence leads from the program with these Member States).[58]

In 2009, SWIFT changed its telecommunication architecture so that EU-originating data was no longer mirrored/copied in its US servers or operating centers. Intra-EU data and transactions were instead processed and stored within a "European Zone."[59] The effect was that half of the financial messages that the United States monitored through the Terrorist Finance Tracking Program was placed outside of its subpoenas. The European Union and the United States negotiated an interim agreement to grant the US Treasury access to EU-originated data in 2010. The EU Parliament, however, refused to give its consent to the coming into force of this agreement. It did so because it concluded that the interim agreement did not adequately safeguard EU fundamental rights, particularly the right of EU individuals to privacy, data protection, and redress.[60]

In the same year, the EU Commission was granted the mandate to negotiate an agreement with the United States that would resume US access to SWIFT's messages in the European Union while safeguarding these rights. The result was/is the TFTP Agreement.

Description and Outline of the TFTP Agreement

The TFTP Agreement regulates how the US Treasury can request the transfer of EU-originating data from SWIFT to the United States and regulates how the US Treasury can access this data and use it as part of its Terrorist Finance Tracking Program. It also recognizes EU fundamental rights and the principles of proportionality and necessity concerning the right to respect of privacy and the protection of personal data.[61] It therefore also makes available to EU individuals certain data protection and redress rights.

The US Treasury only can request the transfer of EU-originating data when based on an ongoing investigation concerning, or pre-existing information or evidence about specific conduct related to terrorism offenses or their financing.[62] Such requests must identify as clearly as possible what specific data stored by SWIFT in the European Union is strictly necessary for the prevention, investigation, detection, or prosecution of these offenses.[63] Specific data may include identifiers associated with the originator and/or recipient of a financial transaction, such as a name, account number, address, national identification number, or other personal data related to financial messages. The US Treasury also must substantiate the need for it to acquire this data, and must tailor its requests for data as narrowly as possible so as to minimize the amount and type of data requested.[64]

The US Treasury (specifically, the US Department of Justice on behalf of the Treasury) must draft data requests and submit them to the EU Member States where SWIFT is based or stores the requested data. These requests must be sent simultaneously to Eurojust.[65] States receiving such requests must review them and certify that they comply with the aforementioned requirements and other terms of the TFT agreement. In cases where that is so, they can issue a production order on SWIFT requiring it to transfer the requested data to the US Treasury.

The US Treasury can retain requested data in secure databases as long as the requested data is not subject to any manipulation, alteration, or addition and those databases containing requested data are not interconnected with any other database.[66] The US Treasury only can search this data under strict conditions. Among other things, all searches must be narrowly tailored and cannot involve data mining or any other type of algorithmic or automated profiling or computer filtering.[67] Searches are authorized only when the US Treasury has pre-existing information or evidence

and can demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing.[68] All such searches must be logged, along with the grounds that justified initiating searches.

The TFTP Agreement makes available to EU individuals certain redress rights. They have the right to request, without constraint or excessive delay or expense, confirmation from their data protection authority whether all necessary verifications have taken place within the European Union to ensure that their data protection rights have been respected in compliance with the Agreement.[69] Particularly, they have the right to know whether any processing of their personal data has taken place in breach of the Agreement. This right is however subject to limitations on the basis of objectives of general interest, such as the need to protect national security or investigate and prosecute criminal offenses.[70]

EU individuals have the right, however, to seek the judicial review of the exercise of such limitations under the US Administrative Procedure Act (1946).[71] They can do so in cases where they have suffered a legal wrong resulting from the decision of a US body or where they are adversely affected or aggrieved by such a decision. They also have the right under the Act to seek the setting aside of such a decision on the grounds that it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." They also can seek monetary compensation and other forms of injunctive and equitable relief under the Computer Fraud and Abuse Act[72] for intentional, unlawful interferences with their computers.

It is interesting to note that the TFTP Agreement does not make available to EU individuals the right to request access to or the rectification of personal data collected about them by the US Treasury under the terms of the Agreement. Instead, the Agreement reiterates their right under the US Freedom of Information Act[73] to request,

regardless of nationality, access to certain records maintained by US bodies. This is problematic because this Act does not give individuals the specific right to request access to or the rectification of personal data maintained in "systems in records;" that is, searchable databases in which the US Treasury retains and can retrieve the personal data or financial-messaging data associated with EU individuals. For individuals to have access to this personal data contained in these databases, the Agreement would have had to give EU individuals legal standing under the US Privacy Act.[74]

The US Privacy Act makes available to individuals the right to request access to and the rectification of personal data maintained in systems of records.[75] It subjects these rights to national security and law-enforcement exemptions. These allow databases maintained for certain law-enforcement or national security purposes to be exempted from access and rectification requests. The Act does, however, make available to individuals the right to seek a remedy, administrative appeal and judicial review where these access and rectification rights are denied, especially on grounds of national security and law-enforcement exemptions.[76] These rights, however, only are available to US citizens and foreign nationals permanently resident in the United States.[77] The TFTP Agreement could have extended these rights to EU individuals by giving them legal standing under the Privacy Act (as the recent EU-US Umbrella Agreement aims to do and the US Judicial Redress Act provides).

Does the TFTP Agreement Comply with the *Schrems* Rights?

It is clear that the TFTP Agreement makes available to EU individuals most *Schrems* rights. The agreement is subject to respect for EU fundamental rights and the principles of necessity and proportionality with regards to how EU-originating data is transferred to the United States and accessed by the US Treasury. It makes

available to EU individuals the right to administrative appeal and judicial review with regards to the decisions of the Treasury. It provides them with a means to seek a remedy, particularly monetary compensation and injunctive relief, for unlawful and intentional interference with their devices. The Agreements also provide a means for EU Member States to investigate complaints from EU individuals concerning whether or not their personal data has been transferred to the United States or accessed by US bodies in compliance with the Agreement and EU fundamental rights.

The Agreement does not, however, as required by *Schrems*, provide EU individuals with the right to request access to or rectification or erasure of personal data collected about them by the US Treasury. This deficiency could be resolved through the US Judicial Redress Act and EU-US Umbrella Agreement. The Umbrella Agreement provides for, and the Judicial Redress Act brings into US law, a mechanism for the United States to give EU individuals legal standing under the US Privacy Act. [78] The Judicial Redress Act gives the US Attorney General[79] the power to designate the TFTP Agreement as a measure covered by the Act.[80] If the Attorney General does so, the citizens of EU Member States could have access, rectification, and redress rights against the US Treasury (if it is designated as a US body covered by the Judicial Redress Act) with regards to how it maintains, accesses, and uses EU data retained in its databases.[81] EU individuals could, through the Judicial Redress Act, also have the right to seek the judicial review of decisions by the US Treasury in cases where it denies the access and rectification rights of EU citizens on grounds of national security or law-enforcement exemptions available in the Privacy Act or TFTP Agreement. By doing so, this could address the absence of these access and rectification rights under the TFTP Agreement and make it more *Schrems* compliant.

Does the TFTP Agreement Comply with the Saugmandsgaard Requirements?

The TFTP Agreement is more compliant with the Saugmandsgaard requirements. The retention of EU personal data is based on public law that is clear enough to allow EU individuals to regulate their conduct. As required, the US Treasury's request for EU-originating data and their access to this data through the Agreement is limited to what is strictly necessary for it to combat serious crime, such as those related to terrorism and its financing. Requests for EU data and its accessing are subject to a test of proportionality in that they only are allowed access when it is narrowly tailored to what is strictly necessary to combat terrorism and when the US Treasury has pre-existing information or evidence that they are needed for this purpose. Such measures observe the essence of the fundamental rights to privacy and data protection because they do not allow for the generalized accessing of requested data or the use of data mining to retrieve personal data retained in the US Treasury's databases.

Significantly, the Treasury only can assess EU financial messages on the basis of pre-existing information or evidence and a reasoned request to Eurojust and EU Member States. As required by Saugmandsgaard, they must approve US requests only after reviewing them for their necessity, proportionality, and compatibility with the terms of the TFTP agreement and EU fundamental rights. In terms of the Saugmandsgaard requirements, the TFTP Agreement, therefore, generally is compliant. If the question of how retained data is made accessible to public bodies is of "decisive importance," as Saugmandsgaard has argued, then the TFTP more than meets the requirement.

NOTES

[1] Maximillian Schrems v. Data Protection Commissioner, Case C-362/14 [2015] I-650.
[2] Opinion of Advocate General Saugmandsgaard øe delivered on July 19, 2016 (1). Joined Tele2 Sverige AB v. Post- och telestyrelsen, Case C‑203/15 and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, Case C‑698/15 (Hereinafter Saugmandsgaard Opinion).
[3] Council Decision 2010/412/EU of July 13, 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement).
[4] The Saugmandsgaard requirements are, at the time of writing, the opinion of an EU Advocate General on a case that has not yet been decided by the CJEU. As the CJEU generally follows and gives much weight to the opinions of Advocate Generals, the article relies on the opinion of Saugmandsgaard for its analysis since his opinion is the closest authoritative interpretation currently available on EU law with regards to how public bodies access and use personal data retained in a generalized way to combat serious crime, such as the financing of terrorism. The opinion does not directly address the issue of EU agreements with third countries, but it does speak of the law as it applies to all EU measures. This is taken to include EU agreements, such as the TFTP Agreement with the United States that allow for EU personal data to be retained in a generalized way and accessed by public bodies for objectives of generalized interest.
[5] TFTP Agreement, Art. 1.
[6] *Id.* preamble and Art. 11.
[7] *Id.* Art. 4 and 5.
[8] *Id.* Art. 2.
[9] For a detailed factual and legal analysis of PRISM, see US Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," *https://www.pclob.gov/library/702-Report.pdf* accessed September 20, 2016.
[10] *Id.*
[11] Commission Decision of July 26, 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 harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (2000/520/EC). (Hereinafter the Safe-Harbor Framework).
[12] *See* Communication from the Commission to the European: Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows' European Commission [European Union] (Communication) COM(2013) 846.
[13] *See* point 3.2 of Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the [European Union] (COM (2013) 847 final).
[14] *Schrems*, at 92-98.
[15] Commission Implementing Decision of July 12, 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (hereinafter Privacy Shield), *http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf accessed* September 20, 2016.
[16] Proposal for a Council decision on the conclusion, on behalf of the European Union, of an agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses (8245/16).

[17] *See* Commission of the European Union Press Release, 16/401 (Feb. 4, 2016).
[18] *See* David B. Bulloch, "Tracking Terrorist Finances: The Swift Program and the American Anti-Terrorist Finance Regime," 3(4) *Amsterdam L F* (2011); Valentin Pfisterer, "Second SWIFT Agreement between the European Union and the United States of America—An Overview," 11(10) *German L J,* 1173 (2010); Jeremy S. Shrader, "Secrets Hurt: How SWIFT Shook up Congress, the European Union, and the U.S. Banking Industry," 11 *N C Banking Inst* 397 (2007).
[19] Privacy Act, Pud. L. No. 93-579, 88 Stat. 1896 (1974) [hereinafter Privacy Act].
[20] Judicial Redress Act of 2015, Pub. L. No. 82-414, (2015) [hereinafter Judicial Redress Act].
[21] *See* Art. 4 of Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[22] Saugmandsgaard Opinion, at 234, 257, 259, and 260.
[23] *See* United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism of December 28, 2009, A/HRC/13/37.
[24] *Id.*
[25] *Id.*
[26] Saugmandsgaard Opinion, at 259.
[27] Art.12 of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) (hereinafter Directive 95/46/EC or Data Protection Directive).
[28] *See* Art. 28(3) of Directive 95/46/EC; and 47 of the Charter of Fundamental Rights of the European Union. Art. 47 gives individuals whose rights are infringed a right to an effective remedy before a tribunal under certain circumstances. CJEU sees this right as essential to protect the principle of the rule of law. *See* al Parti écologiste "Les Verts" v. European Parliament, Case 294/83 [1986] ECR I-01339, at 23; Johnston v. Chief Constable of the Royal Ulster Constabulary, Case 222/84 [1986], ECR I- 1986:206, at 18, 19.
[29] *See* Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ.T.S. No. 5; 213 U.N.T.S. 221; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ.T.S. 108; *see also* Art. 7 of Charter of Fundamental Rights of the European Union [2012] (OJ. C 326/02) (the Charter); and Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Cases C-293/12 and C-594/12 [2014] ECR I-238, at 53. (Hereinafter Digital Ireland case).
[30] *See* Art. 8(3) of the Charter and Art. 28 of Directive 95/46.
[31] *See* Joined Cases C-402/05 P and C-415/05 P Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities [2008] ECR I-461, at 66 (Kadi case); Inuit Tapiriit Kanatami and Others v. European Parliament and Council of the European Union, Case C-583/11 [2013] ECR I-625, at 91.
[32] *See* Directive 95/46, Art.s 25(6) and 31(2). *See also Schrems*, at 73, 76.
[33] *Schrems*, at 73, 76.
[34] *Supra* n.31.
[35] *Schrems*, at 96.
[36] *Id.* at 95.

[37] *Id.* at 101.
[38] *Supra* n.31.
[39] Saugmandsgaard Opinion, at 263.
[40] *Digital Rights Ireland*, at 57, 58.
[41] *Id.*
[42] *See* Saugmandsgaard Opinion.
[43] *See* Leander v. Sweden, Series A no. 116 (1987); Rotaru v. Romania, no. 28341/95 (1995); Weber and Saravia v. Germany, no. 54934/00 (2006).
[44] *Digital Rights Ireland*, at 39.
[45] *Id.* at 186.
[46] *Digital Rights Ireland*, at 39.
[47] Saugmandsgaard Opinion, at 262.
[48] Saugmandsgaard Opinion, at 233.
[49] *Digital Rights Ireland*, at 55
[50] *Id.* at 125.
[51] *Supra* n.18.
[52] *See* Brett A. Shumate, "Thou Shalt Not Speak: The Nondisclosure Provisions of the National Security Letter Statutes and the First Amendment Challenge," 41(1) *GonzLRev* 151 (2005).
[53] *Id.*
[54] *Supra* n.52.
[55] *See* EU Commission. Explanatory Memorandum on a proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (COM(2010) 316 final) (2010/0178 (NLE).
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Supra* n.6.
[62] TFTP Agreement, Art. 4(1).
[63] *Id.*
[64] *Id.* Art. 4(2)
[65] TFTP Agreement, Art. 4(4).
[66] TFTP Agreement, Art. 5(2)(g)
[67] TFTP Agreement, Art. 5(2).
[68] TFTP Agreement, Art. 5(2)(a).
[69] TFTP Agreement, Art. 11(1).
[70] TFTP Agreement, Art. 11(1).
[71]Administrative Procedure Act, Pub.L. No. 79–404, 60 Stat. 237 (1946).
[72] 18 U.S.C. § 1030.
[73] *See* Congressional Research Service, "Freedom of Information Act Legislation in the 114th Congress: Issue Summary and Side-by-Side Analysis," study by Wendy Ginsberg (2016).
[74] *See* Congressional Research Service, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping," study by Gina Stevens and Charles Doyle (2012).
[75] *Id.*
[76] *Id.*

[77] *Id.*
[78] Umbrella Agreement, Art. 16(4) and Art. 17(3); Judicial Redress Act, §§ 2(d)(1), 2(d)(2).
[79] With the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security.
[80] Judicial Redress Act, § 2(d).
[81] Judicial Redress Act § 2(a).