EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens

Study for the LIBE Committee

EN

2015

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens

STUDY

Abstract

Upon request by the LIBE Committee, this study surveys the US legal system of data protection in the field of federal law enforcement. It reviews two principal sources of US data protection law, the Fourth Amendment to the US Constitution and the Privacy Act of 1974. It also considers the legally prescribed methods of data collection, together with their associated data protection guarantees, in ordinary criminal investigations and national security investigations. Throughout, the study pays special attention to the rights afforded to EU citizens.

PE 519.215 EN

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (LIBE)

AUTHOR

Prof. Francesca Bignami, George Washington University Law School, Washington, DC, USA

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C - Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@ep.europa.eu

Editorial assistant
Ms. Lucia-Cristina ACHIHAEI

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy Departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny.

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@ep.europa.eu

European Parliament, manuscript completed in May 2015.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

ECPA	Electronic Communications Privacy Act
EO	Executive Order
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
NSL	National Security Letter
PPD	Presidential Policy Directive
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TFTP	Terrorist Finance Tracking Program

EXECUTIVE SUMMARY

In US law, there are a number of different legal sources that govern data protection in the field of federal law enforcement. This study first considers the two most important sources of data protection law—the Fourth Amendment to the US Constitution and the Privacy Act of 1974. It then turns to the most significant methods of information collection that are available for ordinary criminal investigations and national security investigations and the data protection guarantees set down under the laws authorizing and regulating such information collection.

The Fourth Amendment prohibits "unreasonable searches and seizures" by the government. Reasonableness is established if the search or seizure is conducted pursuant to a valid warrant, that is, a judicial order based on a showing of probable cause and on a particular description of the property to be searched and the items to be seized. Reasonableness can also be established if one of the exceptions to the warrant requirements exists. In the data protection context, however, the application of the Fourth Amendment is relatively limited because of the third-party records doctrine which holds that individuals do not have an expectation of privacy in personal data that they voluntarily turn over to third parties like financial institutions and communications providers. With regard to EU citizens, the Supreme Court has held that foreign citizens resident abroad are not covered by the Fourth Amendment.

Among U.S. laws, the Privacy Act of 1974 is the closest analogue to a European data protection law in that it seeks to regulate comprehensively personal data processing, albeit only with respect to federal government departments and agencies. It regulates the collection, use, and disclosure of all types of personal information, by all types of federal agencies, including law enforcement agencies. At a general level, the Privacy Act contains most of the elements of the EU right to personal data protection. However, it only protects US citizens and permanent residents, not EU citizens. Furthermore, there are a number of exemptions available specifically for law enforcement agencies. As a result, the benefits of the proposed legislation on judicial redress for EU citizens are unclear. The proposed legislation contemplates three types of law suits, two of which are designed to protect the right of access to and correction of personal data, and one of which enables individuals to obtain compensation for unlawful disclosures of personal data. Since law enforcement agencies commonly exempt their data bases from the access requirements of the Privacy Act, the right of action for intentional or willful disclosures that cause actual damage is the only one that would be available on a general basis.

In investigations involving ordinary crime, there are at least three different methods of personal data collection available to law enforcement officials: (1) use of private sources like commercial data brokers; (2) court and administrative subpoenas; (3) electronic surveillance and access to electronic communications based on a court order under the Electronic Communications Privacy Act. These information-gathering methods afford the same level of data protection for US and EU citizens. With respect to EU data protection law, however, some of these methods contain relatively few data protection guarantees. In the case of private sources of personal data, this is attributable to the absence of a comprehensive data protection scheme in the private sector and the vast quantities of personal information freely available to market actors and, consequently, also to law enforcement officials. With respect to the subpoena power and access to communications metadata and subscriber records (under the Stored Communications Act and the Pen Register Act), the lack of significant data protection guarantees is associated with the

standard of "relevance" to any type of criminal investigation and the permissive application of that standard by the courts. The law and jurisprudence of "relevance," in turn, is driven by the failure of US law to recognize a robust privacy interest in the personal data held by corporate entities and other third parties.

In investigations involving national security threats, which can involve both an intelligence and a law enforcement component, there are a number of additional means available to the government: (1) a special type of administrative subpoena known as a "national security letter"; (2) surveillance authorized by the Foreign Intelligence Surveillance Act (FISA); (3) any other form of intelligence gathering authorized by Executive Order 12,333 (and not covered by FISA). The information gathered through such methods can be shared with criminal prosecutors if relevant for law enforcement purposes.

Foreign intelligence gathering, both inside and outside the United States, follows a two-track scheme, one for US persons and another for non-US persons. With the exception of FISA electronic and physical surveillance orders, the data protection guarantees afforded to non-US persons are minimal. The stated intent of Presidential Policy Directive 28 is to provide for stronger personal data protection for non-US persons, but it is difficult to come to any conclusions at this point in time on what effect it will have.

More generally, even with respect to US persons, personal data protection under foreign intelligence law raises a couple of questions. The first concerns the point in time when the right to privacy is burdened by government action. The US government has suggested that in the case of bulk collection of personal data, harm to the privacy interest only occurs after the personal data is used to search, or results from a search of, the information included in the data base. This position stands in marked contrast with EU law, where it is well established that bulk collection, even before the personal data is accessed, is a serious interference with the right to personal data protection because of the number of people and the amount of personal data involved. The second question concerns the conditions under which personal data can be shared between intelligence and law enforcement officials. In the realm of data processing by law enforcement and intelligence agencies, the European courts have emphasized that intrusive surveillance can only be conducted to combat serious threats that are carefully defined in law. They have also held that the information that results from such surveillance can only be used to combat those serious threats, whether to take national security measures or to prosecute the associated criminal offenses. In US law, by contrast, the law allows for intelligence to be transferred to the police and criminal prosecutors for any type of law enforcement purpose.

1. SCOPE AND DEFINITIONS

As with most comparative studies, it is important to clarify at the outset the meaning of the key legal terms being used because of the differences in how they are defined in the US and EU legal systems. In this Note, "law enforcement" and "data protection" are employed in line with their definition under EU law.

Law enforcement is taken to mean the government functions of investigating and prosecuting criminal offenses.[1] It covers the public offices of criminal prosecutors and the police, acting under the direction of criminal prosecutors (and, in inquisitorial systems, investigating magistrates). Most often, the state is activated after the criminal offense has been committed, but if there is a suspicion that a crime is imminent, the state can also be activated beforehand, to prevent the crime and to punish the actions involved in plotting the crime, which are often themselves treated as criminal offenses, such as criminal conspiracy. There are many types of information used to investigate and prosecute criminal offenses and it generally is "personal data," in the sense that it can be linked to a specific person.[2] In both the US and the EU, as a general matter, in the law enforcement area, the state tends to be highly circumscribed in how it can acquire, use, and disseminate personal data because of the implications of criminal investigations and prosecutions for personal liberty. There nonetheless tend to be different levels of legally mandated personal data protection depending on the nature of the personal data and the type of government intrusion. To illustrate, in the US, records on substance abuse treatment, which fall into a category of particularly sensitive personal data, cannot be used to "initiate or substantiate any criminal charges against a patient"[3] while in Germany, the use of listening devices in the home, a particularly intrusive form of information gathering, is constitutionally prohibited for certain law enforcement purposes.[4] By contrast, a home address or a report of a sighting of an individual in a public place, if not included in a database or not part of a systematic program of surveillance, receives far less, if any, protection under data protection law.

Under EU law, the right to personal data protection is comprised of a number of legal guarantees, which are defined at a general level under fundamental rights law and apply to all personal data processors regardless of their identity.[5] For purposes of the analysis in this Note, the right to personal data protection can be broken down into two different categories of guarantees, what can be roughly described as substantive and procedural respectively. The substantive guarantees include the following elements: transparency (public disclosure of the existence and terms of the program involving personal data); accuracy and reliability of the data; security of the data to protect against fraudulent and unlawful uses; proportionality (lawful purpose and data processing that is necessary for that purpose, including amount and type of data collected, use of that data, retention period, sharing and further dissemination, and special considerations for sensitive data). The procedural guarantees include the individual right of access to one's personal data and to have that data corrected if incorrect or deleted if the proportionality requirements have been violated. They also include the state duty to establish independent oversight bodies,

[1] Treaty on the Functioning of the European Union, arts. 82-89 ("Judicial Cooperation in Criminal Matters" and "Police Cooperation").
[2] Directive 95/46/EC, art. 2(a).
[3] Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 §333, 42 U.S.C. §290dd-2(c) (2006).
[4] See Stender-Vorwachs J (2004), The Decision of the Bundesverfassungsgericht of March 3, 2004 Concerning Acoustic Surveillance of Housing Space, 5 German L.J. 1337.
[5] Charter of Fundamental Rights of the European Union, art. 8 ("Protection of personal data").

generally in the form of a data protection authority, and to provide for a judicial remedy for data protection violations.

In the US context, there are a couple of difficulties in giving a comprehensive assessment of data protection in the field of law enforcement. Because of the federal system of American government, there are multiple levels of law enforcement—federal, state, and local. State police and criminal prosecutors, organized at the state and local levels, exercise independent authority and are regulated not only by federal law, but also by state law, including state constitutions and state privacy legislation. For the most part, this Note excludes state and local law enforcement. It focuses on federal law enforcement, in particular the most important federal police force (the Federal Bureau of Investigation or FBI[6]) and federal prosecutors (in the Offices of the United States Attorneys and the Department of Justice). This Note considers state and local law enforcement only insofar as some of the federal sources of privacy law, e.g., the Fourth Amendment of the Constitution and the Electronic Communications Protection Act, apply both to state and federal authorities.

With respect to the data protection law that governs federal law enforcement, the main challenge to giving a comprehensive overview is the lack of significant constitutionalization of the policy area, even as regards US citizens. For the reasons discussed below, the constitutional right to privacy (the Fourth Amendment) has not been interpreted to afford a comprehensive right to personal data protection. As a result, it is necessary to examine the particular congressional statutes, presidential executive orders, and administrative regulations that apply to personal data processing in the field of law enforcement. This is a complex universe that has expanded considerably since 9/11 because of the emphasis in national security law on information sharing for purpose of intelligence and law enforcement activities. Although the overt purpose of congressional laws mandating information sharing is to protect national security, and therefore might appear to involve only disclosures by intelligence agencies to criminal police and prosecutors in cases of actual or imminent national security crimes such as terrorism, the scope of information sharing has proven to be significantly broader.[7] As a number of commentators have observed, the practice of information sharing extends well beyond what might be characterized as core national security crimes,[8] and, as the analysis below will demonstrate, the law governing information sharing generally extends to all crimes, not only core national security crimes. Therefore, while in the past, it might have been appropriate to exclude from such a study the personal data processing (and the specific laws governing it) conducted by intelligence agencies such as the Office of Intelligence and Analysis of the Department of the Treasury and the National Security Agency, today it is necessary to make at least passing reference because of the possibility that the personal data collected by such government authorities will eventually be used by the police and prosecutors in a criminal investigation.

Although a complete account of this legal landscape is beyond the scope of this Note, it will give an overview of the most important sources of data protection law, as well as the most

[6] It should be noted, however, that there are numerous federal agencies that can act as the police in federal criminal investigations, including the Drug Enforcement Administration, the U.S. Marshals Service, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF).

[7] See Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title V ("Improving Intelligence and Information Sharing Within the Federal Government and with State, Local, and Tribal Governments") (2007), 121 Stat. 266; Intelligence Reform & Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §1016, 118 Stat. 3638 (2004).

[8] See, e.g., Citron D.K. & Pasquale F (2011), Network Accountability for the Domestic Intelligence Apparatus, 62 Hastings L. J. 1441.

prominent methods—and their associated data protection laws—by which personal data can be collected and processed in the course of a criminal investigation and prosecution. It begins with the two most important legal sources: the Fourth Amendment to the US Constitution, which is the highest law applicable, and the Privacy Act of 1974, which is the Congressional law that most comprehensively regulates personal data protection, including in the field of law enforcement. It then turns to six prominent methods of collection in the context of criminal and national security investigations and their associated legal guarantees for personal data protection.

2. SOURCES OF US DATA PROTECTION LAW

2.1. Fourth Amendment to the US Constitution

The Fourth Amendment prohibits "unreasonable searches and seizures" by the government.[9] Reasonableness is established if the search or seizure is conducted pursuant to a valid warrant, that is, a judicial order based on a showing of probable cause and on a particular description of the property to be searched and the items to be seized. Reasonableness can also be established if one of the exceptions to the warrant requirements exists, as established by the courts, and if the government meets any additional reasonableness test (balancing the government's need for the information against the intrusiveness of the search) applied by the courts in the particular circumstances. The normal remedy for a Fourth Amendment violation is the suppression of the evidence in any ensuing criminal proceeding, although it is also generally possible to sue the government official for civil remedies such as damages.

As has been explained previously in a Note on a related topic, the application of the Fourth Amendment is relatively limited in the data protection context.[10] That is because the Fourth Amendment only covers those places, things, and conduct in which the individual has a "legitimate expectation of privacy."[11] In the 1970s, the Supreme Court found that individuals have no "legitimate expectation of privacy" in information they voluntarily turn over to third parties, including telephone records[12] and banking records,[13] and therefore much government personal data processing, which obtains personal data from third parties, operates entirely outside of the rubric of the Fourth Amendment. Although, as the Second Circuit (a federal court of appeals) recently observed, this is "an issue on which the Supreme Court's jurisprudence is in some turmoil," the Supreme Court has not yet overruled the third-party records doctrine.[14] In addition, specifically with reference to EU citizens, the Supreme Court has found that the Fourth Amendment does not apply to a physical search of a premise overseas, where the person invoking the right was a foreign citizen and resident.[15] While the precise scope of the Supreme Court's holding is a matter of some debate, it is clear that whatever protections are afforded by the Fourth Amendment to EU citizens resident abroad are minimal.[16]

2.2. Privacy Act of 1974

2.2.1. Data Protection Guarantees

Among U.S. laws, the Privacy Act of 1974 is the closest analogue to a European data protection law in that it seeks to regulate comprehensively personal data processing, albeit only with respect to federal government departments and agencies. It regulates the collection, use, and disclosure of all types of personal information, by all types of federal agencies, including law enforcement agencies. At a general level, it contains most of the

[9] See generally Solove D.J. & Schwartz P.M. (2015), Privacy, Law Enforcement, and National Security, New York: Wolters Kluwer, 4.
[10] Bowden C & Bigo D (2013), The US surveillance programmes and their impact on EU citizens' fundamental rights, PE 474.405, at 16-21.
[11] Katz v. United States, 389 U.S. 347 (1967).
[12] Smith v. Maryland, 442 U.S. 735, 742 (1979).
[13] United States v. Miller, 425 U.S. 435 (1976).
[14] ACLU v. Clapper, No. 14-42 (2d Cir. May 7, 2015).
[15] United States v. Verdugo-Urquidez, 494 U.S. 1092 (1990).
[16] Goitein E & Patel F (2015), What Went Wrong with the FISA Court, Brennan Center for Justice at New York University School of Law 12.

elements of the EU right to personal data protection. The Privacy Act requires transparency in personal data processing: the responsible government agency must alert the public to the existence of a personal records system by publishing a notice in the Federal Register (the U.S. equivalent to the EU's Official Journal);[17] when information is collected from individuals, they must be told of the nature of the government database.[18] Personal information stored by government agencies that is used to make determinations about individuals must be maintained with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[19] The Privacy Act requires that agencies establish "rules of conduct" for their employees and "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records . . . ."[20] As for proportionality, the Privacy Act requires that the agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[21] Sharing with other government agencies is, in principle, prohibited without the consent of the individual involved.[22] Special protection is afforded for the sensitive data category of information on how individuals exercise their First Amendment rights (freedom of expression and association).[23] The Privacy Act gives individuals the right of access to their records and the right to request correction of "any portion thereof which the individual believes is not accurate, relevant, timely or complete."[24] Legal oversight under the Privacy Act is conducted largely by private litigants and the courts: the Privacy Act gives individuals the right to sue the government for violations of their Privacy Act rights and to obtain, depending on the circumstances, damages or injunctive relief.[25] In addition, government officials may be criminally prosecuted for certain violations of the Privacy Act.[26] These same provisions afford individuals a judicial remedy for violations of the Privacy Act.

2.2.2. Limitations In General

Notwithstanding these provisions, the Privacy Act also has significant limitations. To begin with, it should be noted that its guarantees apply only to information contained within a "system of records," which is defined by the statute and the courts as only including a system from which the government agency retrieves information based on a personal identifier like a name or social security number.[27] While in the ordinary law enforcement context it might be expected that most records will be retrievable and will actually be retrieved based on personal identifiers, this might not be the case for personal data used exclusively for data-mining purposes.[28] Turning the Privacy Act's proportionality guarantees, there are myriad exceptions to the prohibition on sharing, including for "routine uses" that are disclosed to the public at the time the record system is created,[29]

[17] 5 U.S.C. § 552a(e)(4).
[18] 5 U.S.C. § 552a(e)(3).
[19] 5 U.S.C. § 552a(e)(5).
[20] 5 U.S.C. § 552a(e)(9)-(10).
[21] 5 U.S.C. § 552a(e)(1).
[22] 5 U.S.C. § 552a(b).
[23] 5 U.S.C. § 552a(e)(7).
[24] 5 U.S.C. § 552a(d).
[25] 5 U.S.C. § 552a(g).
[26] 5 U.S.C. § 552a(i).
[27] See, e.g., Henke v. U.S. Department of Commerce, 83 F.3d 1453 (D.C. Cir. 1996).
[28] For instance, a report issued by the Congressional Research Service assumes that the Privacy Act does not apply to data-mining and suggests that Congress consider "the possible application of the Privacy Act to these [data-mining] initiatives." Seifert J.W. (2006), Data-mining and Homeland Security: An Overview, Congressional Research Service Report for Congress 19.
[29] 5 U.S.C. §552a(b)(3).

and for "a civil or criminal law enforcement activity."[30] There are no provisions specifically directed at data retention periods. Personal data related to the exercise of First Amendment rights is the only category of sensitive data identified by the Act. As for oversight, each federal agency generally has an office or officer specifically designated to oversee privacy compliance within the agency. In the law enforcement context, the Privacy Office in the Department of Homeland Security and the Office of Privacy and Civil Liberties in the Department of Justice are particularly relevant.[31] These, however, are not bodies with the structural independence and powers of European Data Protection Authorities. Finally, as has been repeatedly underscored in previous research conducted for the European Parliament, the Privacy Act does not afford any protections for those not defined as an "individual" under the Act, namely those who are not "a citizen of the United States or an alien lawfully admitted for permanent residence," e.g., EU citizens.[32]

2.2.3. Limitations with Respect to Law Enforcement Agencies

There are also a number of exemptions to the Privacy Act available specifically for law enforcement agencies. The protection for the sensitive data category of First Amendment activities does not apply to "an authorized law enforcement activity."[33] Any system of records maintained by an agency which "performs as its principal functions any activity pertaining to the enforcement of criminal laws" may be exempted from most of the duties of the Privacy Act if the agency publishes a rule claiming the exemption ("general exemptions").[34] These include exemptions from the proportionality duty of relevance and necessity, the duty of "accuracy, relevance, timeliness, and completeness," the right of access to, and correction of, personal data, and the availability of a civil remedy against the government. Any system of records involving classified, i.e. national defense or foreign policy, material or investigatory material compiled for law enforcement purposes may also be exempted from Privacy Act duties, in particular the proportionality duty related to relevance and necessity and individual access, if the agency publishes a rule to that effect ("specific exemptions").[35]

The principal federal police force, the FBI, routinely invokes both the general and the specific exemptions.[36] As might be expected, it does so for files connected with specific investigations, contained in its Central Records System.[37] The FBI also does so, however, for data bases involving materials not connected to a specific investigation. And it does so for systems that include personal data that is not necessarily collected through the particularly intrusive and secretive means of electronic surveillance, courts orders, and subpoenas. For instance, the FBI's Data Warehouse System includes information not only from the FBI's investigative files, but also from databases created by other government agencies, broadcast services and the media, and public and commercial data bases.[38] It covers any individuals who might be relevant to a criminal or domestic security investigation or foreign intelligence operation including "subjects, suspects, victims, witnesses, complainants, informants, sources, bystanders, law enforcement personnel,

[30] 5 U.S.C. § 552a(b)(7).
[31] See Schlanger M (2014), Offices of Goodness: Influence Without Authority in Federal Agencies, 36 Cardozo L. Rev. 52, 64.
[32] 5 U.S.C. §552a(a)(2).
[33] 5 U.S.C. §552a(e)(7).
[34] 5 U.S.C. § 552a(j).
[35] 5 U.S.C. § 552a(k).
[36] See 28 C.F.R. § 16.96 (2012) ("Exemption of Federal Bureau of Investigation Systems—limited access") (listing over 10 exempt systems).
[37] 28 C.F.R. § 16.96(a)(1) (2012).
[38] 77 Fed. Reg. 40630-02 (July 10, 2012).

intelligence personnel, other responders, administrative personnel, consultants, relatives, and associations."[39] Among the categories of information included are biographical information such as name, place of birth, and photograph, biometric information, financial information, employment and business information, visa and immigration information, and travel information.[40] All of the exemptions listed above have been asserted, including an exception to the Privacy Act's access and correction rights and its civil remedies provision.[41]

2.2.4. Draft Legislation to Extend Privacy Act Judicial Redress to EU Citizens

The possible benefits of US draft legislation, introduced in March 2015, to give EU citizens a judicial remedy for data protection violations are unclear. As mentioned above, the rights and duties of the Privacy Act apply only to US citizens or permanent residents (hereinafter "US persons"). The proposed legislation would extend the protections of the Privacy Act to EU citizens (once certified as a citizen of a covered country) in a couple of respects. It would entitle EU citizens to sue a federal agency (1) if, after exercising their right of access, a "designated federal agency" refuses to amend personal data that the EU citizen believes is "not accurate, relevant, timely, or complete"; (2) if "a designated federal agency" fails to respond to the EU citizen's access request; or (3) if any agency intentionally or willfully discloses an EU citizen's personal data in violation of the restrictions on disclosure set down under the Privacy Act. As established under the Privacy Act, the remedies would be different in each type of civil action: (1) correction of the record and attorneys fees and costs; (2) right of access to the record and attorneys fees and costs; (3) damages and attorneys fees and costs.

To begin with, it should be said that the structure of the draft legislation is somewhat unconventional. The first paragraph creates a series of remedies for EU citizens, the second paragraph makes those remedies the exclusive ones available to EU citizens, and the third paragraph defines the rights of EU citizens in terms of the remedies made available to EU citizens in the previous two paragraphs. Generally statutes, including the Privacy Act of 1974, are drafted the other way around. They first set down the substantive rights and duties and then establish the types of remedies, if any, that are available to individuals when the rights and duties set down in the statute are violated. Understanding what rights are created by a legislative statute is treated as an analytically different question from understanding the types of remedies, if any, that are available to individuals when the rights created by that statute are violated.[42] Thinking ahead to future statutory construction by a future court, it may be helpful to adopt a more conventional structure that would make absolutely clear that the rights (and duties) recognized in the third paragraph are substantive, not remedial: first specify the substantive rights and duties that are to be extended to EU citizens, i.e.,§§ 552a(b) and (d) or their analogues in bilateral EU-US agreements, and then specify the judicial remedy that is to be available to EU citizens, i.e. three types of civil actions under §552a(g).

Setting aside the structure of the bill, it is important to note a couple of aspects of the proposed legislation. First, by its very terms, it is it not designed to create absolute equality of treatment between US persons and EU citizens: it excludes damages liability for adverse determinations based on inaccurate or otherwise unlawful personal data and it

[39] Id.
[40] Id.
[41] 28 C.F.R. § 16.96(v) (2012).
[42] In the privacy context, see, e.g., Sterk v. Redbox, 672 F.3d 535, 538 (7th Cir. 2012) (finding the private right of action in the Video Privacy Protection Act (VPPA) did not apply to the VPPA's requirement that personal information be destroyed in a timely manner).

excludes damages liability for any "failure to hew to the terms of the Act,"[43] with the exception of unlawful disclosure. Second, as just explained, the "limitations, including exemptions and exceptions" that apply in the law enforcement domain are considerable. To take a concrete example, the FBI's Data Warehouse System mentioned above is exempt from the access and correction, as well as the civil remedies, provisions of the Privacy Act.[44] The exact scope of the permissible civil remedies exemption is a matter of some uncertainty. However, the US Court of Appeals for the District of Columbia has interpreted the Privacy Act to not allow the exemption where the system of records cannot be exempted from one of the substantive duties of the Act. [45] Therefore, since the US District Court for the District of Columbia would have exclusive jurisdiction under the proposed legislation, in the concrete case of the FBI's Data Warehouse System, one type of civil suit could be brought: for intentional or willful disclosures that caused the plaintiff actual damages.

[43] Doe v. Chao, 540 U.S. 614, 619 (2004).
[44] 28 C.F.R. §16.96(w)(3), (w)(9) (2012).
[45] Tijerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987).

3. METHODS OF DATA COLLECTION

To better understand the data protection guarantees that apply in the domain of federal law enforcement, it necessary to examine the different methods that can be used by law enforcement officials to gather personal data in criminal investigations and to understand how particular regulatory schemes, applicable to each of those methods, discipline their collection and use of personal data. This section and the following one employ the distinction commonly made between the methods available when the government is investigating "ordinary crime" and when it is investigating "threats to national security," which can involve both intelligence and law enforcement officials, and which can result in both criminal prosecutions and national security measures (e.g., diplomatic or military actions, removing terrorists from the United States, and freezing the assets of organizations linked to terrorism).[46] In the case of "ordinary crime," there are at least three different methods available to law enforcement officials: (1) use of private data bases and online resources; (2) court and administrative subpoenas; (3) electronic surveillance and access to electronic communications based on a court order under the Electronic Communications Privacy Act.

3.1. Ordinary Criminal Investigations

3.1.1. Private Data Bases and Online Resources

Federal law enforcement officials can obtain personal data from commercial or non-profit services. Among other things, the government can purchase subscriptions to commercial data bases, like data brokers, or consult publicly available online resources, such as social media websites. Even though the firms that collect and provide such information are generally established in the United States, the individuals on whom they collect and process personal data are both US and non-US citizens. To give a sense of the broad array of personal data available to law enforcement through these means, it is worthwhile quoting a passage from an internal government document on government subscriptions to commercial data brokers:

> With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes. The profile includes personal identifying information (name, alias name, date of birth, social security number), all known addresses, drivers license information, vehicle information . . . telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapons permits, liens, judgments, lawsuits, marriages, worker compensation claims, etc.[47]

The government is generally treated as any other private party when it accesses such information, meaning that there are no formal legal restrictions unless the private provider falls into a category specifically regulated by federal legislation, such as telephone companies and Internet service providers, credit reporting agencies, and financial institutions.[48] Once the government has acquired the personal data, the safeguards of the Privacy Act apply, as long as the data meets the threshold requirement of being a record

[46] The Attorney General's Guidelines for Domestic FBI Operations 7-8 (2008).
[47] Hoofnagle C.J. (2004), Big Brother's Little Helpers: How Choicepoint and other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J. Int'l L. & Com. Reg. 595.
[48] For a comprehensive overview of such statutes, see Murphy E (2013), The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions, 111 Mich. L. Rev. 485.

about an individual that is part of a system of records.[49] While private sources of personal data are themselves subject to the law, those data protection guarantees are often minimal, as in the case of commercial data brokers. [50]

3.1.2. Subpoenas

Another way of obtaining information in the law enforcement context is through subpoenas for the production of documents. Subpoenas can be issued either in the course of litigation (civil or criminal) at the initiation of one of the parties or on the authority of an administrative agency, in the course of regulatory enforcement activities. Like a search warrant issued by a court in a criminal investigation, subpoenas are binding orders, but unlike a search warrant, they are not served by a government officer and they can be contested in court before compliance is required. In terms of the sheer amount of personal data collected, administrative subpoenas are probably the most important form of subpoena, since the hundreds of regulatory programs administered by government agencies generally give those agencies a subpoena power in connection with regulatory enforcement. The information obtained through an administrative subpoena can be used in support of any of the sanctions set down by the particular regulatory scheme, including administrative sanctions, such as withdrawing a license or a civil money penalty, a civil action seeking injunctive or monetary remedies in a court of law, or criminal prosecutions. In the latter case, the information must be shared with the federal prosecutors in the Department of Justice or the United States Attorney's Office since administrative agencies generally do not have the power to bring criminal prosecutions. Although the numerous statutory and regulatory provisions defining the administrative subpoena power typically do not address the question of further use and dissemination, it should be recalled that the Privacy Act permits disclosure to other government agencies if it is done for law enforcement purposes.

The standards for administrative subpoenas have been described as "minimal." [51] The courts have found them to be reasonable as long as the investigation is conducted pursuant to a legitimate purpose, set down under the administrative agency's enabling law, and the information requested is relevant to that purpose.[52] There are exceptions to this standard. For instance, information that falls under the Fifth Amendment's privilege against self-incrimination is not required to be disclosed.[53] Personal records have been found to require an "articulable suspicion" before disclosure can be ordered.[54] The most common uses of the administrative subpoena power, however, do not trigger these exceptions because they generally investigate businesses or request data held by third-party corporations. These are circumstances under which there is no privilege against self-incrimination (because corporations do not enjoy the privilege and the privilege is personal) and there are no special Fourth Amendment considerations (because of the third-party doctrine which undermines any reasonable expectation of privacy).

To understand how administrative subpoenas are used to acquire personal data in the law enforcement context, it is useful to examine briefly the operation of the subpoena power in a program of interest to EU-US relations, the Terrorist Finance Tracking Program (TFTP). Although some elements of TFTP are particular to the national security domain, which will

[49] Id. at 622-23.
[50] See, e.g., Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, May 2014.
[51] Doe v. Ashcroft, 334 F. Supp. 2d 471, 484-85 (S.D.N.Y. 2004).
[52] United States v. Morton Salt Co., 338 U.S. 632 (1950); Doe v. Ashcroft, 334 F. Supp. 2d 471, 484-85 (S.D.N.Y. 2004).
[53] See Cass R.A. et al. (2011), Administrative Law: Cases and Materials, 6th ed., New York: Wolters Kluwer, 707.
[54] Resolution Trust Corp v. Wade, 18 F.3d 943, 949 (D.C. Cir. 1994).

be explored below, TFTP is illustrative of the broad scope of personal data that can be acquired through administrative subpoenas and that can subsequently be made available for law enforcement purposes. As is well-known, since 9/11, the Treasury Department has been collecting vast quantities of financial data on bank transfers and other types of operations from the Belgian private entity, the Society for Worldwide Interbank Financial Telecommunications (SWIFT). Before SWIFT moved its operating center to Switzerland, the Treasury Department did so using its administrative subpoena power. As the Treasury Department explained in October 2007, the legitimate purpose for the investigation and the use of the subpoena power was the mandate, set down by Congressional law and Presidential executive order, to block "the property of, and prohibited transactions with, persons who commit, threaten to commit, or support terrorism."[55] The authority for, and broad scope of, the subpoena power was to be found in the same law and executive order, as implemented in Treasury Department regulations.[56] As further explained by Treasury, the information acquired through these administrative subpoenas was used not only by the Treasury, to take administrative action such as freezing terrorist assets, but was also shared with intelligence agencies and law enforcement agencies in support of national security measures and criminal prosecutions.

3.1.3. Court Orders under the Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) is the main federal statute that regulates electronic surveillance in connection with investigating ordinary crimes. It is comprised of three acts: (1) the Wiretap Act; (2) the Stored Communications Act; and (3) the Pen Register Act.[57] The ECPA divides the universe of communications that the government might wish to obtain into three categories: (1) wire communications, which are voice communications that pass, at some point, through a telephone or cable wire; (2) oral communications, which are words or other sounds made by individuals in a context where they have an expectation of privacy; (3) electronic communications, which is a residual category that includes every other type of signal that is communicated by wire, radio, or other type of communications system. Wire communications, e.g., telephone conversations, tend to be afforded the highest level of protection.

The Wiretap Act applies when the government wishes to intercept the content of a communication at the time that it is made. To do so, the criminal prosecutor must obtain an order from a court based on a finding that there is probable cause to believe that a particular criminal offense has been or is about to be committed and that particular communications concerning the offense will be obtained through the interception.[58] The court must also find that normal investigative procedures are unlikely to succeed or to be too dangerous. The wiretap, as regulated by the order, must minimize the likelihood of intercepting communications unrelated to the criminal offense.[59] Disclosure and use of the intercepted communications is permitted for law enforcement as well as for foreign intelligence and national security purposes.[60] The targeted person must receive notice of the surveillance within 90 days after it is completed, and, if determined to be in the interest

[55] Notice: Publication of U.S./EU Exchange of Letters and Terrorist Finance Tracking Program Representations of the United States Department of the Treasury, 72 Fed. Reg. 60054-02 (Oct. 23, 2007).
[56] Global Terrorism Sanctions Regulations, 31 C.F.R. § 594.601 (incorporating by reference 31 C.F.R. § 501.602 which say "Every person is required to furnish . . . complete information relative to any transaction . . . .")
[57] For an overview of the ECPA, see Kerr O.S. (2013), Computer Crime Law, 2nd ed., St. Paul, MN: West, 574-673; Solove D.J. & Schwartz P.M. (2015), Privacy, Law Enforcement, and National Security, New York: Wolters Kluwer, 95-154.
[58] 18 U.S.C. § 2518(3).
[59] 18 U.S.C. § 2518(5).
[60] 18 U.S.C. § 2517.

of justice by the court, portions of the intercepted communications.[61] An official who violates the terms of the Wiretap Act may be subject to criminal penalties or civil damages.[62] Moreover, wire and oral, but not electronic communications, that are illegally intercepted may be excluded from evidence in a court or administrative proceeding.[63]

The Stored Communications Act applies to records and communications held by two types of service providers, providers of "electronic communications service" such as email accounts and providers of "remote computing service," which covers outsourced storage and processing services, what today is commonly referred to as the "cloud."[64] It covers the content of the material in storage, such as the content of emails, metadata, such as the to/from information on emails, and subscriber records, such as the name, address, and payment method of the subscriber to the ISP. The Stored Communications Act provides for different means of collection, corresponding to different levels of privacy protection, for different types of data held by ISPs. The following analysis is based on the example of emails, but the reader should keep in mind that the Stored Communications Act applies to a variety of network providers, including certain social media sites and text messaging services. For the content of unopened (and perhaps opened) emails in electronic storage for 180 days or less, the government must obtain an ordinary criminal search warrant; for emails in electronic storage for more than 180 days and other content files, the government has a choice between a subpoena (administrative or judicial) with notice to the individual, notice plus a court order based on "specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material to an ongoing criminal investigation" (a so-called §2703(d) order), or an ordinary criminal search warrant; for metadata, a §2703(d) order or an ordinary criminal search warrant; and for subscriber records, a subpoena (administrative or judicial), a 2703(d) order, or a search warrant.[65] In marked contrast with the Wiretap Act, there is no duty to narrowly tailor the request for personal data or minimize the personal data once obtained based on its relevance to the particular criminal investigation. [66] The Act does not restrict use and dissemination of that personal data for other law enforcement purposes. While notice to the customer of the request is generally required at some point, the remedies available are more limited than in the case of the Wiretap Act: government officers can be sued in a civil action and can be criminally prosecuted for violating the terms of the Stored Communications Act, but information acquired in violation of the Act is not subject to exclusion in a criminal trial. [67]

The Pen Register Act applies to metadata that is intercepted at the time that the communication is made. It applies to the metadata associated with telephone calls (to/from information) and Internet communications such as email (to/from information) and websites visited (IP addresses). To install an interception device, the government must certify to a court that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation" and the court is then directed to issue an order authorizing such installation and use.[68] Contrary to both the Wiretap Act and the Stored Communications Act, the default rule is that the individual subject to the

[61] 18 U.S.C. § 2818(8)(d).
[62] 18 U.S.C. § 2511; 18 U.S.C. § 2520.
[63] 18 U.S.C. § 2518(10)(a).
[64] Kerr O.S. (2004), A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1213.
[65] Id. at 1218-1224.
[66] Kerr O.S. (2014), The Next Generation Privacy Act, 162 U. Pa. L. Rev. 373, 402-404.
[67] 18 U.S.C. § 2707 (civil action); 18 U.S.C. § 2701 (criminal prosecution).
[68] 18 U.S.C. § 3123(a).

surveillance is not notified of the device, even after the conclusion of the investigation,[69] and the statute contains no particularity and minimization requirements, or use and dissemination restrictions. A government officer who knowingly fails to obtain such an order can be fined or imprisoned.[70]

The protections afforded by the ECPA (i.e. the Wiretap Act, the Stored Communications Act, the Pen Register Act) against unlawful disclosures by telecommunications and Internet service providers do not turn on the nationality of the subscriber to the service. The ECPA is designed to protect the three types of communications outlined above, as long as, in the case of wire and electronic communications they pass through a system "that affects interstate or foreign commerce",[71] or, in the case of oral communications they are "uttered by a person . . . ." [72] Likewise, the statute defines the "user" of an electronic communications service broadly, as including "any person"[73] and defines "remote computing service" as "the provision to the public"[74] of storage and processing services. Based on this statutory language, a federal court of appeals concluded in a recent case that the ECPA "extends its protections to non-citizens."[75] In that case, which was decided in the context of a civil fraud proceeding, a corporation sought access to the emails of an Indian citizen, imprisoned abroad, that were stored on a US server by a US corporation, Microsoft. The court found that the relevant provision of the ECPA, which protected the material from disclosure, applied equally to the Indian citizen abroad. An EU citizen, therefore, would enjoy the same guarantees as a US person under the ECPA.

3.1.4. Key Findings

The information-gathering methods available to law enforcement officials in ordinary criminal investigations afford the same data protection guarantees for US and EU citizens. From the perspective of EU data protection law, the main problem is the fairly minimal level of personal data protection associated with some of these methods. With respect to the use of commercial data brokers and other private sources of personal data, this is attributable to the absence of a comprehensive data protection scheme in the private sector and the vast quantities of personal information freely available to market actors and, consequently, also to law enforcement officials. With respect to the subpoena power and access to content data in storage, metadata, and subscriber records (under the Stored Communications Act and the Pen Register Act), the lack of significant data protection guarantees is associated with the standard of "relevance" to any type of criminal investigation and the permissive application of that standard by the courts. The law and jurisprudence of "relevance," in turn, is driven by the failure of US law to recognize a robust privacy interest in the personal data held by corporate entities and other third parties.

3.2. National Security Investigations

In the case of threats to national security, there a number of means available to the government in addition to those available in an ordinary criminal case: (1) a special type of administrative subpoena known as a "national security letter"; (2) surveillance

[69] 18 U.S.C. § 3123(d).
[70] 18 U.S.C. § 3121(d).
[71] 18 U.S.C. § 2510(1),(12).
[72] 18 U.S.C. § 2510(2).
[73] 18 U.S.C. § 2510(13).
[74] 18 U.S.C. §2711(2).
[75] Suzlon Energy Ltd v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011).

authorized by the Foreign Intelligence Surveillance Act (FISA); (3) any other form of intelligence gathering authorized by Executive Order 12,333 (and not covered by FISA).

At the outset of this discussion, it is helpful to understand the historical background of the legal regulation of surveillance and information gathering in national security investigations. This background drives the different treatment of US persons and non-US persons, including EU citizens, which runs throughout national security law and which is particularly relevant to the data protection rights afforded to the two categories of persons. The starting point for most legal treatments of the subject is the Keith Case, decided by the Supreme Court in 1972.[76] In that case, the government had engaged in warrantless wiretapping of a member of radical domestic group (the "White Panthers") who was eventually prosecuted for bombing a CIA recruitment office.[77] When faced with the issue of whether the warrantless wiretapping was in line with the constitutional requirements of the Fourth Amendment, the Supreme Court acknowledged that there was a difference between surveillance connected to "ordinary crime" and to "national security."[78] The latter was conducted pursuant to the President's constitutional power to "preserve, protect, and defend the Constitution of the United States" and was designed to "protect our Government against those who would subvert or overthrow it by unlawful means."[79] In the Court's analysis, national security could be further divided into two parts: the "domestic aspects of national security," which applied to the defendant, who was involved in purely domestic radicalism, and the "activities of foreign powers or their agents," inside or outside the United States.[80] The Court found that in case of domestic security surveillance, the government was required to follow the warrant requirements of the Fourth Amendment. In so holding, it was driven by the danger that unchecked government surveillance would burden democratic debate and dissent. The Court, however, expressly left open the different question of whether the warrant requirement, or Fourth Amendment protection of any sort, applied in the case of surveillance of foreign powers, which quite obviously were not beneficiaries of the democratic freedoms of the US Constitution.

The regulation of national security surveillance reflects the Supreme Court's two-part scheme and the special concerns raised by domestic, as opposed to foreign, security surveillance.[81] The law is largely designed to exclude domestic security threats from the special framework set out for surveillance (considered foreign because it either involves foreign entities or is conducted abroad) and to protect the speech and privacy rights of US citizens. It does so by setting down standards that will ensure that US persons will be minimally implicated by foreign intelligence surveillance or at least will not be burdened in the exercise of their speech and associational rights. There are two main laws in the

[76] United States v. United States District Court, 407 U.S. 297 (1972).
[77] Morrison T.W. (2008), The Story of United States v. United States District Court (Keith):The Surveillance Power in Schroeder C.H. & Bradley C.A. eds., Presidential Power Stories, New York: Foundation Press.
[78] Id. at 313, 321.
[79] Id. at 310.
[80] Id. at 308, 322.
[81] Besides the distinction between domestic and foreign security threats, there is another distinction important for understanding intelligence activities: affirmative versus protective intelligence. While protective intelligence (also called "counterintelligence" in Executive Order 12,333, 3.5(a)) is largely synonymous with national security, affirmative intelligence (also called "foreign intelligence," in Executive Order 12,333, 3.5(e)) refers to more general intelligence-gathering activities necessary to conduct foreign affairs and national defense. See Kris D.S. & Wilson J.D. (2012), National Security Investigations and Prosecutions 2d §§ 8:31, 8:32, 8:33, 8:34, 8:35. In contrast with protective intelligence, i.e. national security, affirmative intelligence is less likely to be associated with law enforcement. Based on these distinctions, the Attorney General's Guidelines for Domestic FBI Operations identify three areas of authority: federal crimes, threats to the national security, and foreign intelligence. The Guidelines also point out, however, that there is likely to be significantly overlap between these subject areas, giving the example of investigations relating to international terrorism and espionage, both of which cut across all three areas of responsibility. Id. at 6.

area—the Foreign Intelligence Surveillance Act (enacted by Congress and which regulates surveillance inside the United States) and Executive Order 12,333 (promulgated by the President and which regulates surveillance outside the United States as well as other residual forms of surveillance). The Foreign Intelligence Surveillance Act (FISA), adopted in 1978, regulates the category of national security surveillance that the Supreme Court had left open in the Keith Case—surveillance designed to protect against the "activities of foreign powers or their agents." It creates a two-track scheme for the conduct of foreign intelligence surveillance: one standard for US persons and another standard for everyone else, including EU citizens. The same is true of Executive Order ("E.O.") 12,333 on "United States Intelligence Activities," first issued by President Reagan in 1981 and since amended a number of times. In contrast with FISA, which has a relatively narrow focus, E.O. 12,333 is the basic operational charter for the US intelligence community: it sets out the organizational framework for intelligence activities, identifying a total of 17 agencies that together form the intelligence community, lays down their powers, and establishes certain limits on the intelligence collection, retention, and dissemination authorized under the Order. Even more so than FISA, those limits are designed to protect the rights of US persons.

Having laid down the basic framework, this section now turns to the specific methods of personal data collection available in national security investigations and their data protection guarantees.

3.2.1. National Security Letters

National Security Letters ("NSLs") are a special type of administrative subpoena available to the FBI in national security investigations. Although they existed before 9/11, their scope was broadened considerably in the USA PATRIOT Act of 2001. The FBI can use NSLs to obtain personal data under the Stored Communications Act,[82] the Right to Financial Privacy,[83] and the Fair Credit Reporting Act.[84] In other words, they can be used by the FBI to compel telephone companies and ISPs to release customer records and metadata, to compel financial institutions like banks to release personal financial information, and to compel consumer reporting agencies to release financial data and credit reports on individuals.

While the specific requirements of these three types of NSLs vary somewhat, the most important one by far, in terms of FBI usage, has been the NSL under the Store Communications Act. As the Inspector General reported in 2006, the total number of NSL requests between 2003 and 2005 totaled at least 143,074 and, among these requests, "[t]he overwhelming majority . . . sought telephone toll billing records information, subscriber information (telephone or e-mail) or electronic communication transaction records under the ECPA NSL statute." [85] They can be used when the FBI certifies that the information requested is "relevant to an authorized investigation to protect against terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States."[86] Here we see the first example of

[82] 18 U.S.C. §2709.
[83] 12 U.S.C. § 3414(a)(5).
[84] 15 U.S.C. § 1681u(a).
[85] Office of the Inspector General, A Review of the Federal Bureau of Investigations Use of National Security Letters, at x-xiv (Mar. 2007). In the context of national security investigations, the content of communications held by ISPs is generally obtained under the physical search provisions of FISA (which, it will be recalled, track the requirements of electronic surveillance). Kerr O.S. (2013), Computer Crime Law, 2nd ed., St. Paul, MN: West, 811.
[86] 18 U.S.C. § 2709 (b).

the unequal treatment of US persons and EU citizens in the national security domain. There is a so-called "gag rule," under which the FBI can prohibit the recipient from disclosing the subpoena to anyone except to his or her attorney, which affects most obviously the customers and subscribers implicated by the subpoena.[87] Dissemination of the information collected under NSLs is permissible if done in accordance with the Attorney General's Guidelines and, with respect to federal agencies, if "clearly relevant to the authorized responsibilities of such agency."[88] In other words, with respect to the subject of this Note, it can be transferred to the police and criminal prosecutors. NSLs and gag orders can be challenged in court.[89] The NSL applicable to telephone companies and ISPs has been found unconstitutional by a federal district court based on the burden placed by the gag rule on the communications provider's right to speech.[90]

3.2.2. Foreign Intelligence Surveillance Act (FISA)

To understand the type of surveillance available under, and regulated by, FISA it is helpful to analyze the relevant provisions chronologically.[91] When FISA was first adopted it authorized one principal method of information collection: electronic surveillance (so-called "traditional FISA orders").[92] In 1998, it was amended to include a separate set of provisions on metadata surveillance (contemporaneous acquisition of information about telephone calls and electronic communications via the Internet). In the USA PATRIOT Act of 2001, a provision was added on the acquisition of "any tangible things" (Section 215). And, in the FISA Amendments Act of 2008, another provision was added on the acquisition of any type of information on persons reasonably believed to be non-US persons overseas (Section 702). Throughout, US persons (defined as a US citizen, a permanent resident, and certain corporations and associations[93]) and non-US persons are treated differently.[94]

Traditional FISA orders. For the acquisition of personal data that is considered "electronic surveillance" under FISA, the government must meet a couple of requirements. First, foreign intelligence gathering must be a "significant purpose" of the surveillance.[95] As explained above, foreign intelligence includes information that serves to protect national security against foreign threats (including international terrorism) and information that affirmatively advances the foreign affairs and national defense interests of the United States.[96] In the case of US persons, foreign intelligence is defined as information that is "necessary" to the protection of the United States or affirmative intelligence purposes,

[87] 18 U.S.C. § 2709 (c).
[88] 18 U.S.C. § 2709 (d).
[89] 18 U.S.C. § 3511.
[90] In re National Security Letter, 930 F. Supp. 2d 1064 (N.D. Cal. 2013).
[91] This section is based on a number of sources, including the leading treatise in the area, Kris D.S. & Wilson J.D. (2012), National Security Investigations and Prosecutions 2d, and a number of studies and reports that have been issued in since the Snowden revelations, including Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014; Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court; Goitein E & Patel F (2015), What Went Wrong with the FISA Court, Brennan Center for Justice at New York University School of Law; Donohue L.K. (2015), Section 702 and the Collection of International Telephone and Internet Content, 38 Harv. J. L. & Pub. Pol'y; Donohue L.K. (2014), Bulk Metadata Collection: Statutory and Constitutional Considerations, 37 Harv. J. L. & Pub. Pol'y 757.
[92] This Note does not give separate consideration to the procedures that apply to physical searches, which mimic those which apply to electronic surveillance but were adopted somewhat later.
[93] 50 U.S.C §1801(i).
[94] Kris & Wilson, National Security Investigations and Prosecutions 2d §§8:38-8:42.
[95] 50 USC § 1804(6)(B). Prior to the USA PATRIOT Act, foreign intelligence had to be the "primary purpose" of the investigation. Goitein & Patel, What Went Wrong 11.
[96] 50 USC § 1801(e).

while in the case of non-US persons, it is information that "relates" to such purposes.[97] Second, the government must show probable cause that the target of the surveillance is a "foreign power" or an "agent of a foreign power," "foreign power" defined broadly as not just a foreign government, but a number of other entities, including a "group engaged in international terrorism or activities in preparation thereof . . . ."[98] In the case of a US-person "agent of a foreign power," the government also must show probable cause that his or her activities violate or may violate criminal law.[99] With respect to non-US persons, FISA was amended in 2004 to allow for the targeting of "lone-wolf" terrorists, who do not need to be connected to a foreign power.[100] To further ensure that surveillance will not be used to suppress political activity, FISA states that a U.S. person cannot be "considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[101] Third, the government must adopt "minimization procedures" designed to "minimize the acquisition and retention and prohibit the dissemination," of information on US persons, with the exception of information that serves a foreign intelligence purpose or "is evidence of a crime which has been, is being, or is about to committed and that is to be retained or disseminated for law enforcement purposes."[102] Of special relevance for EU citizens, to whom these minimization procedures do not apply, information cannot be used or disclosed "except for lawful purposes."[103] Fourth, based on these showings, the government must obtain an order from a special court known as the FISA Court, composed of federal trial judges appointed for a single, seven-year term, who continue to serve on their trial courts but also hear FISA applications on a rotating basis.[104] FISA provides for criminal penalties for government officials that engage in unlawful surveillance as well as a civil suit for damages for US persons who have been the object of unlawful surveillance (non-US persons are expressly excluded by terms of the provision).[105] Although the FISA Court operates entirely in secret, if information derived from such surveillance is to be used as evidence in a legal proceeding, the person concerned must be notified, and evidence obtained from unlawful surveillance may be suppressed.[106]

Before moving to other methods of information collection under FISA, a couple of words on the scope of "electronic surveillance" are in order. The FISA definition is quite complex because it turns on a combination of the technology by which the communication or information is sent or stored, as well as the identity of the parties, the basic premise being that non-US persons receive less protection than US persons.[107] However, the relevant provision does not seek to parse ISPs in the same fashion as the Stored Communications Act, and therefore it is relatively clear that stored email and voice mail, as well as perhaps other stored content, are covered under the definition, and hence by the procedures outlined above.[108]

[97] 50 USC § 1081(e).
[98] 50 U.S.C. § 1801(a); §1801 (b); §1805(a)(2).
[99] 50 U.S.C. § 1801 (b); §1805(a)(2).
[100] Kris & Wilson, National Security Investigations and Prosecutions 2d §8:14; 50 U.S.C. § 1801(b)(1)(C).
[101] 50 U.S.C. § 1805(a)(2)(A).
[102] 50 U.S.C. § 1801(h)
[103] 50 U.S.C. § 1806(a)
[104] 50 U.S.C. § 1805.
[105] Kris & Wilson, National Security Investigations and Prosecutions 2d, Chapter 14. As explained in the Brennan Report, it has proven very difficult to challenge FISA surveillance, both in the course of legal proceedings based on information acquired in such surveillance and in criminal and civil suits. Goitein & Patel, What Went Wrong 34.
[106] 50 U.S.C. § 1806(c).
[107] See Goitein & Patel, What Went Wrong 15.
[108] Kris & Wilson, National Security Investigations and Prosecutions 2d §7:28.

Metadata Surveillance. Until 1998, the government had to satisfy the requirements for a FISA electronic surveillance order to engage in what is sometimes called "pen/trap surveillance" and what is referred to here as metadata surveillance—interception of metadata associated with telephone calls (to/from information) and Internet communications such as email (to/from information) and websites visited (IP addresses). In 1998, a specific set of less demanding provisions were added to FISA, in the USA PATRIOT Act those standards were relaxed, and in 2006, subscriber records were added to the information available under the relevant provisions.[109] A FISA order authorizing such surveillance will issue if (1) the purpose of the investigation, in the case of non-US persons, is foreign intelligence or, in the case of US persons, the protective category of foreign intelligence covering international terrorism and clandestine foreign intelligence activities; and (2) the information likely to be obtained concerns those purposes.[110] There is no requirement that the target of the surveillance be an agent of a foreign power. The FISA Court, in reviewing the application, only ensures that the required elements of the government certification are present, not that they are true. The provision includes the familiar exception for investigations involving US persons based on activities connected to free expression and association.[111] The information may be disclosed for law enforcement and any other "lawful purposes."[112] Although, unlike electronic surveillance, there are no minimization requirements, the same rules on notification and suppression apply if the information is used in a criminal trial.[113] It should be noted that one of the facts that was brought to light by Snowden was that this provision had been used as the basis for a NSA program involving the bulk collection of Internet metadata (which, however, was terminated in 2011 for operational reasons).[114]

Any Tangible Things. Beginning in 1998, FISA contained a provision specifically allowing the acquisition of certain types of records. With Section 215 of the USA PATRIOT Act (codified at 50 U.S.C. § 1861), that provision was expanded considerably. It allows the government to obtain, for the same purposes as the metadata surveillance just described, "any tangible things (including books, records, papers, documents, and other things)."[115] "Tangible things" has been interpreted by national security agencies, in the communications domain, to cover only non-content data, not the content of communications.[116] In applying for a FISA order, the government must provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation"[117] and the FISA Court must find that the application meets these requirements (representing a more active role for the FISA Court in comparison with orders for metadata surveillance).[118] Minimization procedures are required for retention and dissemination but not acquisition.[119] As with electronic surveillance, minimization is designed to limit the use of information on US persons, and does not apply to intelligence and law enforcement uses of the information. For non-US persons, e.g., EU citizens, the only restriction on use or disclosure is that it be for "lawful purposes."[120] (This is common to all methods of information collection under FISA.) Similar

[109] Id. at §18:4.
[110] 50 U.S.C. § 1842.
[111] 50 U.S.C. § 1842(a)(1).
[112] 50 U.S.C. § 1845.
[113] Id.
[114] See Goitein & Patel, What Went Wrong 22.
[115] 50 U.S.C. § 1861.
[116] Kerr O.S. (2013), Computer Crime Law, 2nd ed., St. Paul, MN: West, 813.
[117] 50 U.S.C. § 1861(b)(2)(A).
[118] Kris & Wilson, National Security Investigations and Prosecutions 2d §19.3.
[119] 50 U.S.C. § 1861(g)
[120] 50 U.S.C. § 1861 (h).

to National Security Letters, the recipient of a tangible things order is barred from disclosing the existence of the order, with certain exceptions, but may challenge the order in court.[121] There are no specific sanctions or remedies that apply if information is acquired without, or without following the terms of, an order for any tangible things. To conclude this discussion, it should be noted that the NSA's telephone record bulk collection program is based on Section 215 and that a federal court of appeals has recently held that it exceeds the legal authority conferred by the provision because of the provision's requirement that the tangible things sought be relevant to a specific investigation.[122]

Information on Persons Reasonably Believed to be Non-US Persons Overseas. As originally enacted, FISA did not apply to information gathering abroad, which was instead conducted pursuant to the President's inherent constitutional powers and was regulated by E.O. 12,333, considered in the next section.[123] The FISA Amendments Act of 2008 made a number of changes that extended FISA's coverage to activities with a significant foreign connection, the most notorious one being Section 702 (codified at 50 U.S.C. §1881a). Under Section 702, the government may collect foreign intelligence information, of any type (e.g. content, metadata, records), on any person reasonably believed to be a non-US persons overseas without making any of the specific showings required for electronic surveillance, metadata surveillance, or tangible things.[124] This includes the omission of the requirement, applicable to traditional FISA orders, that a non-US person be an agent of a foreign power or a lone-wolf terrorist. The government, however, is required to conduct such programs following targeting and minimization procedures approved by the FISA Court: the targeting procedures should be "reasonably designed" to ensure the program is limited to targeting "persons reasonably believed to be located outside of the United States"; and the minimization procedure are identical to the ones described in connection with electronic surveillance, i.e. designed to minimize the collection, use, and dissemination of data on US persons, with the exception of intelligence and law enforcement purposes.[125] A directive issued to an electronic communication service provider may be challenged by that provider before the FISA Court.[126] The same restriction on use and disclosure (only for "lawful purposes") and the same requirement of notice, and possibility of suppression, if the information is to be used in a criminal prosecution apply in the case of Section 702 as in traditional electronic surveillance.[127] Section 702 has been used as the authority for PRISM, the NSA program that collects content and metadata from a variety of Internet companies, as well as for upstream collection, the NSA program which intercepts personal data that transit through cables and switches, and which gathers both Internet traffic and telephone calls, including the content of those calls.[128]

Although less relevant for purposes of this Note, the FISA Amendments Act of 2008 also added Sections 703 (codified at 50 USC §1881b) and 704 (codified at 50 USC §1881c), on the acquisition of foreign intelligence information on US persons located abroad. If a US person is reasonably believed to be abroad, but the acquisition of information occurs inside the United States (acquisition covers "electronic surveillance or stored electronic communications or stored electronic data that requires an order") then the procedure

[121] 50 U.S.C. §1861(d); U.S.C. §1861(f).
[122] ACLU v. Clapper, Docket No. 14-42 (2d Cir. May 7, 2015).
[123] Kris & Wilson, National Security Investigations and Prosecutions 2d §17:1.
[124] Id. § 17.4.
[125] Kris & Wilson, National Security Investigations and Prosecutions 2d § 17:7.
[126] Kris & Wilson, National Security Investigations and Prosecutions 2d § 17:10.
[127] 50 U.S.C. §1881e (incorporating by reference 50 U.S.C. §1806); Kris & Wilson, National Security Investigations and Prosecutions 2d §28:7.
[128] See generally Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014.

required of the government is roughly similar to traditional FISA orders.[129] If a US person is reasonably believed to be abroad, but the acquisition of information occurs outside the United States, the government also must apply for a FISA order, although the standards are less demanding in a number of ways.[130]

Relationship between FISA and Law Enforcement. As explained at the beginning of this Note, even though information gathering by intelligence agencies appears somewhat removed from the domain of law enforcement, developments since 9/11 have led to extensive information sharing between intelligence and law enforcement officials. Therefore, personal data acquired through the intelligence routes outlined above, together with the various data protection guarantees that may or may not whittle down the data, can ultimately be used by the police and prosecutors in a criminal proceeding. Even before 9/11, intelligence gathering regulated by FISA could be passed on to criminal prosecutors if it produced evidence that a crime had been committed.[131] The prevailing interpretation of FISA, however, gave rise to a "wall" between intelligence and law enforcement elements within the Department of Justice and the FBI that significantly limited any involvement of criminal prosecutors in intelligence investigations.[132] With the amendments to FISA made by the USA PATRIOT Act,[133] and the subsequent interpretation of those amendments in an important court decision,[134] there are no longer any restrictions on information sharing; furthermore, criminal prosecutors can be fully involved in foreign intelligence investigations as long as FISA is used to obtain evidence for criminal prosecution of an offense related to a foreign intelligence threat (and not ordinary crimes).[135] The result, in everyday practice, has been that "[w]ith the wall down, dozens of prosecutors in the National Security Division [of the Department of Justice] and in the US Attorneys' Offices now legally enjoy access to FBI intelligence investigations, and in fact they do increasingly work with agents."[136] A number of commentators have pointed to the possible Fourth Amendment problems with this practice—for those individuals covered by the Fourth Amendment, i.e. US persons.[137]

In addition, even though it is true that national security investigations cannot be motivated, at the front end, by the need to collect evidence to prosecute "ordinary crime," there are no significant legal limitations, on the back end, on information sharing if evidence of "ordinary crime" is found. This is true both for US persons and non-US persons. As the review of relevant legal provisions above demonstrates, information collected pursuant to FISA can generally be used and disseminated for law enforcement purposes. Although there certainly are reasons related to the need to protect classified information that might limit data sharing is the context of ordinary crimes, the relevant statutes do not actually impose any such limits. This has emerged as a problem especially with bulk surveillance such as PRISM and upstream collection under Section 702, since the amount of personal data collected through such programs is staggering. One of the Recommendations of the

[129] 50 U.S.C. 1881b; Kris & Wilson, National Security Investigations and Prosecutions 2d §§17:11, 17:12.
[130] 50 U.S.C. §1881c; Kris & Wilson, National Security Investigations and Prosecutions 2d § 17:13
[131] See United States v. Isa, 923 F.2d 1300 (8th Cir. 1991) (holding that information gathered under FISA can be retained and disseminated for purposes of criminal investigation and prosecution).
[132] See Kris & Wilson, National Security Investigations and Prosecutions 2d, Chapter 10.
[133] Most notably the "significant purpose" test in 50 U.S.C. § 1804(a)(7)(B) and the provision for consultation between intelligence officers and law enforcement officers in 50 U.S.C. §1806(k). The USA PATRIOT Act of 2001 amended FISA to permit electronic surveillance orders (which, the reader will recall, involve the interception of communications and emails stored on servers) when a significant—as opposed to primary—purpose of the surveillance is to obtain foreign intelligence information and to allow coordination between law enforcement and intelligence officials in foreign intelligence investigations.
[134] In re Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Court of Review 2002).
[135] Kris & Wilson, National Security Investigations and Prosecutions 2d §10:14.
[136] Id. §11.20
[137] See, e.g., Kris & Wilson, National Security Investigations and Prosecutions 2d §11:11; Donohue, Section 702 and the Collection of International Telephone and Internet Content 202.

President's Review Group, convened in the wake of the Snowden revelations, was to prohibit the use of such information as evidence in proceedings.[138] Although the Administration has not gone this far, the NSA's new Section 702 minimization guidelines released in February 2015 only permit the use of such information as evidence in criminal proceedings involving "serious crimes."[139] It should be recalled, however, that the Section 702 minimization guidelines, as with all minimization under FISA, only apply to US persons.

3.2.3. Executive Order 12,333

The last major source regulating intelligence surveillance is E.O. 12,333, originally issued in 1981.[140] As explained earlier, it is the basic charter for US intelligence activities and constitutes a reservoir of legal authority and set of legal standards for intelligence gathering that is not regulated by FISA. As a result of FISA's operation, outlined above, the most important forms of surveillance regulated by E.O. 12,333 are (1) foreign intelligence surveillance outside of the United States; (2) foreign intelligence surveillance both inside and outside the United States if it does not involve the types of communications and personal data covered by FISA; (3) personal data on US persons incidentally collected in foreign intelligence surveillance.[141] As compared to FISA, the standards set down in E.O. 12,333 are significantly more permissive. Even more so than FISA, the limitations on foreign intelligence surveillance are almost entirely designed to protect US persons.[142]

One of the main data protection guarantees contained in E.O. 12,333 is that the relevant agencies collect, retain, and disseminate information only in accordance with procedures set down under departmental guidelines and approved by the Attorney General.[143] That requirement, however, applies only to U.S. persons. Although the procedures set down in the departmental guidelines can authorize a wide range of activities, there are certain limits specified in E.O. 12,333. For instance, they can only authorize "information acquired by overhead reconnaissance not directed at specific United States Persons."[144] With respect to collection techniques, E.O. 12,333 says that intelligence agencies "shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."[145] Under certain circumstances, the Attorney General must approve the use of collection techniques within the United States or directed against US persons abroad.[146] Unlike FISA surveillance, compliance with various requirements of E.O. 12,333 is not entrusted to a court but to internal executive branch mechanisms.[147]

Under E.O. 12,333, intelligence agencies are authorized to assist law enforcement agencies in a number of circumstances.[148] They are directed to collect information on "international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities

[138] Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Recommendation, Recommendation 12, at 145-46, Dec. 12, 2013.
[139] Laperruqu J. (2015), Updates to Section 702 Minimization Rules Still Leave Loopholes, available at https://cdt.org/blog/updates-to-section-702-minimization-rules-still-leave-loopholes.
[140] Exec. Order No. 12,333, 3 C.F.R. 200 (1981), as amended by Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004); and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008); [hereinafter E.O. 12,333].
[141] Donohue, Section 702 and the Collection of International Telephone and Internet Content 144-45.
[142] Kris & Wilson, National Security Investigations and Prosecutions 2d §2:7.
[143] E. O. 12,333, § 2.3.
[144] Id. § 2.3(h).
[145] Id. § 2.4.
[146] Id. § 2.5.
[147] E.O. 12,333, §§ 1.6(b), 1.6(c), 1.6(h).
[148] Kris & Wilson, National Security Investigations and Prosecutions 2d §2:8.

directed against the United States."[149] In turn, under the agency guidelines promulgated for US persons (and certainly with respect to non-US persons), they are allowed to share such information with law enforcement agencies, including incidentally acquired information that may indicate any other type of violation of law.[150] Intelligence agencies may also participate directly in law enforcement investigations of "clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities . . . ."[151] And they may, upon request of a law enforcement agency, "collect information outside the United States about individuals who are not U.S. persons," even if this information is intended to be used for a specific law enforcement investigation.[152]

3.2.4. Presidential Policy Directive 28

On January 17, 2014, the President issued Presidential Policy Directive (PPD)-28. PPD-28 has been said to reflect a major "conceptual shift" because it specifically recognizes and mandates certain privacy protections for non-US persons in the domain of foreign intelligence surveillance.[153] In doing so, it addresses the absence of data protection guarantees for non-US persons in foreign intelligence surveillance, especially evident in E.O. 12,333.

PPD-28 states that:

> Our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.[154]

The guarantees for non-US persons contained in PPD-28 hew closely to a classic data protection framework. It contains a general commitment to proportionality:

> Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.[155]

With respect to bulk collection such as PRISM and upstream collection (under Section 702), PPD-28 sets down a specific set of lawful purposes: signals intelligence collected in bulk shall be used

> only for the purposes of detecting and countering: (1) espionage . . . ; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to the US or allied Armed Forces or other U.S. or allied

[149] E.O. 12,333, § 1.4(b).
[150] E.O. 12,333, §§ 2.3(c), 2.3(i). See, e.g., United States Signals Intelligence Directive, USSID SP0018: Legal Compliance and U.S. Persons Minimization Procedures, §§ 5.4, 7.2, Jan. 25, 2011.
[151] E.O. 12,333, § 2.6(b).
[152] Kris & Wilson, National Security Investigations and Prosecutions 2d §2.9 (citing to 50 U.S.C. §3039).
[153] Kris D.S. (2014), On the Bulk Collection of Tangible Things, 7 J. Nat'l Security L. & Pol'y 209, 289.
[154] Presidential Policy Directive - Signals Intelligence Activities, Jan. 17, 2014 [hereinafter PPD-28], available at http:// www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, at 1.
[155] PPD-28, §1(d).

personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.[156]

PPD-28 anticipates that this list will be periodically updated.[157]

PPD-28 also addresses the dissemination and retention elements of proportionality. Dissemination of information acquired on non-US persons is only permissible in the same circumstances as comparable information on U.S. persons under E.O. 12,333. As the national security legal scholar, David Kris, observes, this is not a significant guarantee because of the broad dissemination permitted for US persons.[158] In line with PPD-28, the NSA procedures implementing this principle, allow dissemination not only for foreign intelligence purposes but also if the personal data "(iii) is related to a crime that has been, is being, or is about to be committed; or (iv) indicates a possible threat to the safety of any person or organization."[159] Likewise, retention is only permissible under the same circumstances and for the same period as applicable to US persons under E.O. 12,333.[160] Absent a comparability determination (on what the period would be for US persons), the retention period is to be five years (unless the Director of National Intelligence expressly determines that a longer period is appropriate).[161] The NSA's implementing procedures adopt the 5-year default period.[162]

Another data protection principle addressed in PPD-28 is security: personal data is to be stored in such a way as to protect against unauthorized access and only personnel "with a need to know the information to perform their mission" are to be given access to the information.[163] Personal data is to meet standards of accuracy and quality, a principle already guaranteed in E.O. 12,333.[164] Lastly, PPD-28 provides for internal executive branch oversight to ensure respect for these data protection safeguards, although again, such oversight is already an integral component of E.O. 12,333.[165] Overall, it is unclear what changes will be made to agency practice in the wake of PPD-28. As David Kris puts it, PPD-28 could either be a "new paradigm of transparency, privacy, and internationalism in US intelligence" or a "collection of fairly modest changes, largely cosmetic in nature, that were designed to placate critics in the United States and abroad."[166]

3.2.5. Key Findings

Foreign intelligence gathering, both inside and outside the United States, follows a two-track scheme, one for US persons and another for non-US persons. With the exception of FISA electronic surveillance orders, the data protection guarantees afforded to non-US persons are minimal. The stated intent of PPD-28 is to provide for stronger personal data

[156] PPD-28, § 1.
[157] Id. §2.
[158] See Kris, On the Bulk Collection of Tangible Things 293
[159] United States Signals Intelligence Directive, USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons, § 7.2, Jan. 12, 2015.
[160] PPD-28, §4(a)(i).
[161] Id.
[162] United States Signals Intelligence Directive, USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons, § 6.1, Jan. 12, 2015.
[163] Id. § 4(a)(ii).
[164] Id. § 4(a)(iii).
[165] Id. § 4(a)(iv).
[166] Kris, On the Bulk Collection of Tangible Things 294. For another assessment of PPD-28, see Edgar T.H., The Good News About Spying, Foreign Affairs, April 13, 2015.

protection for non-US persons, but it is difficult to come to any conclusions at this point in time on what effect it will have.

This two-track scheme, as originally articulated by the Supreme Court in the Keith Case, seeks to achieve robust internal democratic debate and privacy while at the same time enabling the government to protect national security. The evolution of technology and human rights law, however, has exposed certain flaws in this model. On the one hand, the revolution in digital technologies has allowed US Internet companies to hold far greater quantities of personal data on foreigners than was ever conceivable in the 1970s. This implicates the privacy interests of foreigners, as well as those of US citizens, whose personal data is very often mixed with that of foreigners. On the other hand, the limited geographical and personal scope of privacy rights under the US Constitution runs counter to the jurisprudence of the European Court of Human Rights, which has found that States must respect Convention rights in circumstances under which they either have de facto control over an area or over an individual. Those to have considered the issue, have argued that these principles require a state engaging in surveillance on its own territory, of the kind being conducted by the NSA under Section 702, to respect privacy rights, regardless of the location or nationality of the individuals on whom data is collected.[167]

Even with respect to US persons, the personal data protection guaranteed under foreign surveillance law raises a couple of questions. The first concerns the point in time when the right to privacy is burdened by government action. The US government has suggested that in the case of bulk collection of personal data, harm to the privacy interest only occurs after the personal data is used to search, or is derived from a search of, the information included in the data base. For instance, in the recent litigation on the Section 215 telephone records program, the government argued that there was no injury to the plaintiffs because "any alleged injuries here depend on the government's reviewing the information collected, and . . . appellants have not shown anything more than a 'speculative prospect that their telephone numbers would ever be used as a selector to query, or be included in the results of queries of, the telephony metadata.'"[168] Although this assertion was made in connection with the question of standing (and was rejected by the Second Circuit), it is consistent with statements elsewhere on the merits of the privacy analysis. While E.O. 12,333 speaks broadly of "collection," the NSA's procedures refer to two types of collection, the intentional interception of communications and the selection of communications through the use of a selection term, indicating that in the case of bulk collection, the guarantees applicable to "collection" arise only after the use of a selection term.[169] As the US has explained to the EU, under US law, "data is 'processed' only when it is analysed by means of human intervention."[170] This position stands in marked contrast with EU law, where it is well established the right to personal data protection is triggered at the moment that personal data is acquired by the government. Bulk collection, even though the personal data collected may never actually be accessed, is considered to be a serious

[167] Milanovic M, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, forthcoming in Harv. Int'l L.J.
[168] ACLU v. Clapper, No. 14-42, at 27 (2d Cir. May 7, 2015).
[169] United States Signals Intelligence Directive, USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons, § 4, Jan. 12, 2015.
[170] Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection § 3, Nov, 27. 2013.

interference with the right to personal data protection because of the number of people and the amount of personal data involved.[171]

Another question raised by this overview is the lack of legal limits in US law on the sharing of personal data between intelligence and law enforcement officials. Under EU law, the proportionality principle requires that personal data be collected for a carefully specified legal purpose and that it be used only as necessary to advance that purpose. In the realm of data processing by law enforcement and intelligence agencies, the cases that have been decided by European courts such as the European Court of Human Rights and the European Court of Justice have emphasized that intrusive surveillance can only be conducted to combat serious threats that are carefully defined in law and that the information that results from such surveillance can only be used for those purposes.[172] For instance, under Germany's G10 Act, which has been scrutinized by both the German Constitutional Court and the European Court of Human Rights, when the Federal Intelligence Service conducts strategic surveillance, it does so to collect intelligence on certain listed serious offenses and it may only transfer the information to the police authorities if a certain factual threshold is met for suspecting the individual of having committed or planning to commit one of the listed offenses. A very different approach is evident in the US law reviewed above: the law confers broad authority to transfer personal data collected through intelligence methods to law enforcement agencies, regardless of the type of criminal offense that is suspected.

[171] See Cases C-293/12, C-594/12, Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources, April 8, 2014; Weber and Saravia v. Germany, Eur.Ct.H.R., App. No. 54934/00, June 29,2006; Bundesverfassungsgericht, 1 BverfGE 518/02, Apr. 4, 2006.

[172] See Cases C-293/12, C-594/12, Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources, April 8, 2014; Bundesverfassungsgericht 1 BvR 256/08, 1 BvR 263/08, 1 BvR 589, March 2, 2010; Weber and Saravia v. Germany, Eur.Ct.H.R., App. No. 54934/00, June 29,2006; Bundesverfassungsgericht, 1 BVerfGE 2226/94, 2420/95,2437/95, July 14, 1999.

4. DISCLOSURE OF PERSONAL DATA TO THIRD COUNTRIES

In the context of law enforcement, personal data that may be useful for a foreign criminal investigation or prosecution can be shared with third countries through a number of avenues: traditional international judicial cooperation, i.e. letters rogatory, mutual legal assistance treaties, memoranda of understanding entered into between specific federal agencies and their foreign counterparts, e.g., the Securities and Exchange Commission, and a variety of other, less formal, cooperation agreements. Unlike EU law, US law does not contain a general prohibition on transfers of personal data to jurisdictions without adequate data protection guarantees. The different avenues for data transfers listed above, however, can contain specific privacy safeguards.

5. CONCLUSIONS AND POLICY RECOMMENDATIONS

This survey of US data protection guarantees in the field of law enforcement has revealed several discrepancies with respect to EU law. First, with regard to the data collection methods available in both ordinary criminal and national security investigations, there is a considerable divide between the privacy safeguards that apply to the content of communications and all other types of personal data. While the contemporaneous acquisition of the content of communications is subject to the stringent requirements of the Wiretap Act (for ordinary criminal investigations) and FISA electronic surveillance (for national security investigations), other types of personal data receive very little, if any, protection under US law: the relatively permissive regulation of the private sector allows law enforcement officials to access private sources of personal data such as commercial data brokers with virtually no legal oversight; metadata on communications and subscriber records can be obtained fairly easily under the Stored Communications Act and the Pen Register Act (for ordinary criminal investigations) and National Security Letters and the various provisions added to FISA after 9/11 (for national security investigations); and even with respect to content data, if it is held by a third party such as an ISP, the guarantees afforded under the Stored Communications Act (for ordinary criminal investigations) and possibly under FISA, depending on the Executive Branch's interpretation of the relevant provisions (for national security investigations) are significantly lower than in the case of real-time surveillance.

Second, in both ordinary criminal and national security investigations, the rules on the use and onward transfer of personal data are generous. All of the methods of collection regulated by statute implicitly or explicitly permit the sharing of personal data for any law enforcement purpose. The Privacy Act also creates a broad exception to the purpose limitation principle if the reason for onward transfer is related to law enforcement.

Third, with respect to the intelligence component of national security investigations, the FISA provisions enacted after 9/11 allow the government to engage in bulk collection based on a minimal showing of need. The law on bulk collection is currently in flux. One of the relevant provisions, Section 215 (the legal basis for the telephone records program), is set to expire on June 1, 2015 and legislation is currently being debated that would replace the existing provisions and end bulk collection. It would require the government to request call records from service providers based on a specific selector associated with an individual suspected of being involved in international terrorism. The version of the legislation that has been passed by the House of Representatives would require specificity also with respect to ECPA National Security Letters and FISA metadata surveillance.

On the guarantees available specifically to EU citizens (without permanent residence in the United States), US law generally excludes non-US persons from the scope of personal data protection. There are two important exceptions to this state of affairs. First, in the context of ordinary criminal investigations, the ECPA has been held to apply equally to US citizens and foreign citizens. Second, in the context of national security investigations, if the government seeks a traditional FISA order for purposes of either electronic or physical surveillance, it must demonstrate to the FISA court that there is probable cause that the individual is an agent of a foreign power or a lone-wolf terrorist. As discussed in the body of this study, the law on the treatment of EU citizens may change in the near future. Legislation has been proposed that would extend some of the judicial remedies available to US persons under the Privacy Act to EU citizens. As explained earlier, however, the proposed legislation has a couple of limitations: setting aside the unconventional structure of the bill, it does not guarantee absolute equality (for instance, EU citizens would not have a right to sue for damages caused by wrongful government determinations) and it is subject to the extensive carveouts that exist for law enforcement agencies and purposes. Furthermore, in the foreign intelligence domain, PPD-28 has acknowledged a right to

privacy for foreigners and has called on intelligence agencies to afford, at least in some respects, equal treatment for the personal data of foreigners.

How these very significant differences between EU and US law should affect the assessment of the adequacy of the US data protection system in the field of law enforcement is a complex issue. The question is of obvious importance for evaluating the EU-US data protection Umbrella Agreement. It is also relevant to the ongoing negotiations on Safe Harbor: with the Lisbon Treaty and the migration of police and justice affairs into the Treaty on the Functioning of the European Union, the EU institutions are responsible for assessing not only the adequacy of private sector guarantees for personal data but also the adequacy of the law under which public authorities can request access to private sector data for law enforcement purposes (and hence render the processing of such personal data legitimate in a proportionality analysis). Abstracting from the myriad details of US data protection law, there are at least three aspects that run deep and that are unlikely to undergo radical change in the immediate future: the difference between the treatment of content and non-content personal data (and in some cases stored content data); the permissive approach to data sharing, driven by the perception of the benefits of "big data," which has also shaped the law enforcement and national security domains in the post 9/11 era; and the bifurcation between the privacy rights of US citizens and the privacy rights of foreigners, which reflects the Supreme Court's jurisprudence on privacy as instrumental to a free, democratic (and national) political order.

That being said, there are at least two important mechanisms that can be used in the bilateral agreements under negotiation to improve the rights of EU citizens. The first is carefully drafted purpose, use, and sharing provisions that limit personal data processing to certain types of crimes and that ensure that EU personal data acquired from private actors or state authorities will not be placed in general-purpose data bases such as the FBI's Data Warehouse System. This device can compensate for the generous access afforded by US law to non-content data (in some cases, stored content data too), for the permissive arrangements that currently exist for information sharing for law enforcement purposes, and for the absence of data protection guarantees for EU citizens in the national security domain. The second type of guarantee is oversight and redress mechanisms for EU citizens that can operate in conjunction with those currently in place under US law. In the domain of personal data protection, the most important line of defense against individual data protection violations has generally been independent administrative authorities, not ordinary courts operating under theories of private law. Although internal oversight bodies like Inspectors General and agency privacy offices lack the independence of European DPAs, they are tasked with enforcing civil liberties and have the capacity to administer ombudsman-like complaints systems for those who allege that their privacy rights have been violated. Ensuring that such an ombudsman process exists in all significant law enforcement agencies, expressly acknowledging a right to participate for EU citizens, and allowing European DPAs to intervene on the behalf of EU citizens would improve significantly legal oversight of privacy rights.

LITERATURE REFERENCES

Bowden C & Bigo D (2013), The US surveillance programmes and their impact on EU citizens' fundamental rights, PE 474.405.

Cass R.A. et al. (2011), Administrative Law: Cases and Materials, 6th ed., New York: Wolters Kluwer.

Citron D.K. & Pasquale F (2011), Network Accountability for the Domestic Intelligence Apparatus, 62 Hastings L. J. 1441.

Donohue L.K. (2014), Bulk Metadata Collection: Statutory and Constitutional Considerations, 37 Harv. J. L. & Pub. Pol'y 757.

Donohue L.K. (2015), Section 702 and the Collection of International Telephone and Internet Content, 38 Harv. J. L. & Pub. Pol'y 117.

Edgar T.H., The Good News About Spying, Foreign Affairs, April 13, 2015

Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, May 2014.

Goitein E & Patel F (2015), What Went Wrong with the FISA Court, Brennan Center for Justice at New York University School of Law.

Hoofnagle C.J. (2004), Big Brother's Little Helpers: How Choicepoint and other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J. Int'l & Com. Reg.

Kerr O.S. (2004), A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208.

Kerr O.S. (2013), Computer Crime Law, 2nd ed., St. Paul, MN: West.

Kerr O.S. (2014), The Next Generation Privacy Act, 162 U. Penn. L. Rev. 373.

Kris D.S. & Wilson J.D. (2012), National Security Investigations and Prosecutions 2d.

Kris D.S. (2014), On the Bulk Collection of Tangible Things, 7 J. Nat'l Security L. & Pol'y 209.

Laperruque J. (2015), Updates to Section 702 Minimization Rules Still Leave Loopholes, available at https://cdt.org/blog/updates-to-section-702-minimization-rules-still-leave-loopholes.

Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, Dec. 12, 2013.

Milanovic M, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, forthcoming in Harvard Int. L.J.

Morrison T.W. (2008), The Story of United States v. United States District Court (Keith). The Surveillance Power in Schroeder C.H. & Bradley C.A. eds. Presidential Power Stories, New York: Foundation Press.

Murphy E (2013), The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions, 111 Mich. L. Rev. 485.

Office of the Inspector General, A Review of the Federal Bureau of Investigations Use of National Security Letters, at x-xiv (Mar. 2007).

Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014.

Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Jan. 23, 2014.

Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, Nov. 27, 2013.

Schlanger M (2014), Offices of Goodness: Influence Without Authority in Federal Agencies, 36 Cardozo L. Rev. 52.

Seifert J.W. (2006), Data-mining and Homeland Security: An Overview, Congressional Research Service Report for Congress.

Solove D.J. & Schwartz P.M. (2015), Privacy, Law Enforcement, and National Security, New York: Wolters Kluwer.

Stender-Vorwachs J (2004), The Decision of the Bundesverfassungsgericht of March 3, 2004 Concerning Acoustic Surveillance of Housing Space, 5 German L. J. 1337.

EUROPEAN PARLIAMENT

CATALOGUE QA-04-15-376-EN-N

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

ISBN 978-92-823-7156-5
doi: 10.2861/819030

Publications Office