THE TRANSATLANTIC FLOW OF DATA AND THE NATIONAL SECURITY EXCEPTION IN THE EUROPEAN DATA PRIVACY REGULATION: IN SEARCH FOR LEGAL PROTECTION AGAINST SURVEILLANCE

IOANNA TOURKOCHORITI*

Europe regulates data privacy against violations coming from the private sector more strictly than the U.S.[1] The EU Directive 95/46/EC has led to the implementation of a sophisticated system of data privacy regulation having strong enforcement mechanisms.[2] The European Commission has submitted a proposal for a new regulation, which updates data privacy law protection strengthening individual rights and foreseeing important penalties.[3] Both the existing Directive and the Proposed

* Lecturer, School of Law, National University of Ireland, Galway. The author would like to thank the participants in the Roundtable "Constitutionalism Across Borders in the Struggle Against Terrorism" of the Research Group on Constitutional Responses to Terrorism, of the International Association of Constitutional Law, held at Harvard Law School on March 6–7, 2014, for contributions of materials on the topic and interesting discussions. Special thanks go to David Cole, Vicki Jakson, Konrad Lanchmayer, Valerio Lubello, Valsamis Mitsilegas, Kim Lane Scheppele, Mark Tushnet and Arianna Vedaschi.

1 *See generally* Ioanna Tourkochoriti, *The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-E.U. in Data Privacy Protection*, 36 U. ARK. LITTLE ROCK L. REV. 161 (2014).

2 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive], *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (laying out regulations for protecting data privacy).

3 *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter Proposed Regulation], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (proposing "a new legal framework for the protection of personal data").

Regulation do not apply to activities concerning "national security."[4] The EU has succeeded through negotiations to level up the standards of data privacy protection in the private sector in the U.S. through the Safe Harbor Agreement.[5] This agreement also foresees an exemption of its application in case of national security, public interest, or law enforcement requirements.[6]

The European Regulation of privacy is indirectly affecting the access of public authorities to private data by limiting the possibility of private actors to collect and store this data, which they will be required to transmit to surveillance authorities.[7] A legal tool elaborated for a specific purpose to limit the access of private actors to personal information can operate protectively for another purpose: to limit access of the state to the same information. The Directive goes as far as prohibiting profiling altogether and establishing a "right to be forgotten."[8] It thus can limit the amount of information that private actors collect, which then results in the state authorities limiting their "data mining" potentiality.

Surveillance transcends the public/private divide,[9] as the PRISM program revealed recently gives public authorities access to information collected by the private sector. This paper analyzes the existing protection through the Safe Harbor Agreement and the Proposed Regulation, which strengthens the legal framework of

---

[4] *See* Tourkochoriti, *supra* note 1 (noting that the Directive is inapplicable in certain cases); Data Protection Directive, *supra* note 2, art. 3(2) (clarifying that the Directive does not "apply to the processing of personal data . . . in any case to processing operations concerning public security, defence, State security"); *see also* Proposed Regulation, *supra* note 3, art. 2(2)(a) (the Proposed Regulation foresees explicitly that it does not apply to the processing of personal data "in the course of an activity which falls outside the scope of Union Law, in particular concerning national security").

[5] *See* Dep't of Commerce, *Safe Harbor Privacy Principles*, EXPORT.GOV (July 21, 2000) [hereinafter Safe Harbor Privacy Principles], http://export.gov/safeharbor/eu/eg_main_018475.asp (explaining the Directive mandates that personal data transfers to non-EU countries must provide an "adequate" level of protection).

[6] *Id.* at 1 (stating the EU required "'adequacy standard'" on personal data transfers may be limited "to the extent necessary to meet national security, public interest, or law enforcement requirements").

[7] *See infra* Part 3.1.

[8] *Id.*

[9] *Cf.* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (arguing "public and private surveillance are simply related parts of the same problem, rather than wholly discrete.").

privacy against collection of data by the private sector. It analyzes how limiting the possibility of private actors to collect information may have an impact on what information the state collects from private actors. It then suggests ways of interpreting the national security exception existing both in the EU Regulation and the Transatlantic agreements in a way as to narrow its scope, in reference to the ECHR in Europe and to the ICCPR. It also points out the need for signing a new treaty to fill legal gaps in the protection of transfer of data through Cloud computing. The prima facie legal gap in the protection of privacy concerning Cloud computing can be filled in reference to other international instruments protecting privacy.

The transatlantic flow of data is of critical importance for both the economy of the EU and the U.S.[10] Following the revelations, the European Commission made clear that the standards of data protection will not be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership,[11] while the Committee on Foreign Affairs of the European Parliament insists that a separate agreement is necessary on strong data privacy protections.[12] The Commission refuses to negotiate data protection with the U.S. as, in its opinion, this is a "fundamental right" which is not negotiable.[13]

---

[10] *See, e.g.*, EUR. CTR. FOR INT'L POL. ECON., THE ECONOMIC IMPORTANCE OF GETTING DATA PROTECTION RIGHT: PROTECTING PRIVACY, TRANSMITTING DATA, MOVING COMMERCE 7 (2013) (noting that if services and cross-border data flows were to be disrupted as a consequence of the discontinuity of binding corporate rules, model contract clauses and the Safe Harbor, the negative impact on EU GDP could reach -0.8% to -1.3% and EU services exports to the U.S. would drop by -6.7% due to the loss of competitiveness).

[11] Press Release IP/13/1166, Eur. Comm'n, European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows (Nov. 27, 2013) [hereinafter Press Release IP/13/1166], *available at* http://europa.eu/rapid/press-release_IP-13-1166_en.htm (calling for actions to "restore trust in data flows between the EU and the U.S." and to "maintain the continuity of data flows").

[12] *See* Eur. Parliament Comm. on Foreign Affairs, *Draft Working Document on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens*, at 3 (Nov. 4, 2013) *available at* http://database.statewatch.org/article.asp?aid=32888 [*Working Document on Mass Surveillance*] (noting "it is crucial that agreement on strong data privacy protections is achieved separately from the [Transatlantic Trade and Investment Partnership].").

[13] *See* Memorandum MEMO/13/1059, Eur. Comm'n, Restoring Trust in EU-US Data Flows – Frequently Asked Questions, at 8 (Nov. 27, 2013) [hereinafter European Commission Memo] ("'Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable.'") (quoting Vice President Viviane Reding from a prior speech). Viviane Reding, Vice President, Eur.

The ECtHR has issued a number of decisions on surveillance issues, some of them more protective than others.[14] The same court has elaborated jurisprudence concerning the conditions under which European states can maintain databases on their citizens for surveillance and law enforcement purposes. [15] Furthermore, following the revelations, the Advocate General of the Court of Justice of the European Union issued a very promising opinion on the Data Retention Directive for the purpose of the investigation, detection, and prosecution of serious crime.[16]

Much of the foreign intelligence information collected by the NSA is shared with the governments of many other nations.[17] While the governments of the Member States are promoting cooperation with the U.S. on intelligence matters, the EU officials show a greater sensibility in favor of protecting data privacy.[18] Within the Member States, Europeans are split between the need of satisfying the negative reactions of their constituents to the revelations and using the result of their cooperation with the U.S. for their own security purposes.

One method of collecting Internet data is the PRISM program, which collects data from companies like Google, Apple and Facebook if the communications contain certain terms chosen by

---

Comm'n, SPEECH 13/867, Towards a More Dynamic Transatlantic Area of Growth and Investment (Oct. 29, 2013).

[14] *See* Klass v. Germany, Eur. Ct. H.R. 1, 14 (1978) analyzed *infra* Part 3.3 (pointing out the court does not recognize high standards of protection).

[15] *See infra* Part 3.3.

[16] Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine, and Natural Res. et al., [2013] (H. Ct.) (Ir.) [hereinafter Digital Rights Ireland Ltd.], *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=187576 (ruling on the "circumstances in which it is constitutionally possible for the European Union to impose a limitation on the exercise of fundamental rights"); *see also* Monika Ermert, *EU Data Retention Might Not Be Proportional to Risks* (July 9, 2013), http://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170 (during the oral hearing of the case in July, the judges seemed willing to confirm this approach).

[17] *See* Justin Cremer, *Denmark is One of the NSA's '9-Eyes'*, COPENHAGEN POST (Nov. 4, 2013, 10:10 AM), http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html (stating the NSA is reported to have a close relationship with the UK, Canada, New Zealand and Australia, called the '5-Eyes', but a more restricted intelligence-sharing relationship exists between Denmark, Norway, the Netherlands and France, which altogether compose the '9-Eyes.' The NSA has a less intimate relationship with Germany, Sweden, Belgium, Spain, and Italy, which adds up to the '14 eyes' with the other nine countries.).

[18] Press Release IP/13/1166, *supra* note 11.

the NSA.[19] The program gathers "massive data on life-styles in order to elaborate patterns and profiles concerning political attitudes and economic choices."[20] Another method collecting Internet content is "upstream" collection, which gives the NSA direct access to the data packets traveling through domestic and international fiber optic cables.[21] "Data is copied from both public and private networks . . . and from central exchanges which switch Internet traffic between the major carriers, through agreements negotiated with . . . the operating companies . . . ."[22] The NSA is reported to be copying all emails and text messages with one end outside of the United States in order to pull out communications

---

[19] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/usintelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (discussing a top-secret document discovered by The Washington Post that reveals a program, code-named PRISM, which allows the NSA to hack into the central servers of nine leading Internet companies, "extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets").

[20] *See* Note by Caspar Bowden, Directorate General for Internal Policies, Eur. Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs: The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights, at 8 (2013) (noting that by "gathering massive data on life-styles in order to elaborate patterns and profiles concerning political attitudes and economic choices, PRISM seems to have allowed an unprecedented scale and depth in intelligence gathering. . . .").

[21] *See* Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, THE WASH. POST (July 10, 2013), http://articles.washingtonpost.com/2013-07-10/business/40480665_1_nsa-slide-prism (discussing a classified NSA slide that describes "Upstream" data collection as accessing "'communications on fiber cables and infrastructure as data flows past.'"); *see also* Jennifer Valentino-DeVries & Siobhan Gorman, *What You Need to Know on New Details of NSA Spying*, WALL ST. J. (Aug. 20, 2013), http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html (stating that "Upstream" data collection involves splitting fiber optic lines at a junction, and then copying the traffic to an NSA processing system that filters through the data based on NSA parameters); Brett Max Kaufman, *A Guide to What We Know About the NSA's Dragnet Searches of Your Communications*, AM. CIVIL LIBERTIES UNION (Aug. 9, 2013), https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications (contrasting "Upstream" data collection with PRISM, noting that the former "involves the collection of communications—both their metadata and their content—as they pass through undersea fiber-optic cables.").

[22] *See* Bowden, *supra* note 20, at 13 (2013) (describing the "Upstream" surveillance program).

that match certain "selectors" relevant to foreign intelligence.[23] The agency has collaborated with domestic telecommunications companies to give it the ability to directly access up to approximately seventy-five percent of U.S. communications.[24] A program called XKEYSCORE allows the government to search essentially any Internet activity using approved search terms, and has vast capabilities, feeding much of it to other specialized databases.[25] It enables an analyst to discover "strong selectors" (search parameters which identify or can be used to extract data precisely about a target and to look for "anomalous events").[26] Because the amount of data that is scanned and stored is vast, it can only be stored for a limited time, three to five days for content and thirty days for metadata; other databases receiving information from XKEYSCORE keep the content of emails and email metadata for up to five years.[27] BULLRUN is the codename

---

[23] *See* Charlie Savage, *NSA Said to Search Content of Messages to and from U.S.*, N.Y. TIMES (Aug. 8, 2013), http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-bynsa.html?ref=todayspaper&pagewanted=all (describing how NSA officials must first collect all cross-border data, and a computer searches through the data using "selectors" or other keywords to selectively store data for human analysts to review later).

[24] *See* Valentino-DeVries & Gorman, *supra* note 21 (revealing that the NSA can access 75% of the telecommunications traffic in the U.S. through U.S. telecommunications companies, including not only metadata but the actual content of online communications).

[25] *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet*,' THE GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (describing how NSA analysts can use XKEYSCORE and other systems to mine enormous databases by completing a simple on-screen form giving only a broad justification for the search); *XKeyscore Presentation* (Feb. 25, 2008) THE GUARDIAN [hereinafter *XKeyscore Presentation*], *available at* http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (revealing slides from a presentation explaining the capabilities of XKeyscore).

[26] Greenwald, *supra* note 25; *XKeyscore Presentation*, *supra* note 25, at 15.

[27] *XKeyscore Presentation*, *supra* note 25, at 2, 17; *see* Marc Ambinder, *What's XKEYSCORE?*, THE WEEK (July 31, 2013, 3:58 PM), http://theweek.com/article/index/247684/whats-xkeyscore (describing XKEYSCORE as something that doesn't collect data, but rather "a series of user interfaces, backend databases, servers and software that selects certain types of metadata that the NSA has ALREADY collected using other methods."); *see also 21% of the Database Query Errors in NSA Report Involved the ~~Phone~~ Internet Dragnet Database*, EMPTYWHEEL (Aug. 16, 2013), https://www.emptywheel.net/2013/08/16/21-of-the-database-query-errors-in-1q-2012-involved-the-phone-dragnet-database/ (noting that 21% of the database query errors used by the NSA involve the MARINA database, which stores

for another program of the last decade, that can break into encryption technologies,[28] while information which recently came to light on the NSA's TAO hacking unit reveals they have been infiltrating computers around the world.[29]

The U.S. government has established several data centers to aggregate, compare, data-mine, and analyze information. The National Counterterrorism Center operates under the Director of National Intelligence and pulls employees from other federal agencies, like the FBI, the CIA, the Department of Agriculture and the U.S. Capitol Police.[30] The Center's mission is to "analyze and integrate" all terrorism and counterterrorism intelligence, collecting data from all other agencies.[31] It also assesses data from international travel-related datasets, immigration benefits-related datasets, and financial-related datasets.[32] The FBI's Investigative

---

Internet data).

[28] *See* James Ball, Julian Borger & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (revealing an NSA classification guide which states, "'Project Bullrun deals with NSA's abilities to defeat the encryption used in specific network communication technologies. Bullrun involves multiple sources, all of which are extremely sensitive.'").

[29] *See* SPIEGEL Staff, *Inside TAO: Documents Reveal Top NSA Hacking Unit*, SPIEGEL ONLINE (Dec. 29, 2013, 9:18 AM), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html (revealing that the NSA's TAO hacking unit is considered the agency's "top secret weapon" capable of maintaining its own covert network that hacks into computers around the world).

[30] National Security Act of 1947, Pub. L. No. 80-235, 61 Stat. 496 (codified as amended at 50 U.S.C. § 15 (2007) [hereinafter National Security Act of 1947] (establishing a system for national security); U.S. Dep't of Justice et al., Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (2003), *available at* http://www.fas.org/sgp/othergov/mou-infoshare.pdf; *see also* Exec. Order No. 13354, 69 Fed. Reg. 53589 (Aug. 27, 2004), *available at* www.gpo.gov/fdsys/pkg/FR-2004-09-01/pdf/04-20050.pdf (stating that the Center is also given the authority to "receive, retain, and disseminate information" from any domestic government agency or other source; each agency that holds terrorism information must provide the Center with access to the information).

[31] National Security Act of 1947, *supra* note 30; *see generally* Rachel Levinson-Waldman, *What the Government Does With Americans' Data,* Brennan Ctr. for Justice at N.Y.U. L. Sch., at 20 (2013).

[32] *See* Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information, at 12 (2012), *available at*

Data Warehouse conducts data mining, which it collects from the Departments of Treasury, State and Homeland Security, the Bureau of Prisons, and non-governmental sources.[33] The National Security Agency Data Center also collects material.[34] A series of statutes and executive orders facilitate the sharing of information among all levels of government and private sector (ISE-SAR).[35] For the information to be retained an assessment is required by an analyst that there is a "potential terrorism nexus," which is established by the federal government.[36] The criterion used is that which would make a "reasonable person" suspicious.[37]

---

http://www.fas.org/sgp/othergov/intel/nctc_guidelines.pdf (according to the 2012 Guidelines to the authority, the NCTC can disseminate information that "reasonably appears to be necessary to understand or assess terrorism information"); *see generally* Levinson-Waldman, *supra* note 31, at 20.

[33] *See Report on the Investigative Data Warehouse*, ELECTRONIC FRONTIER FOUND., § 4 (Apr. 2009) [hereinafter Report on IDW], https://www.eff.org/issues/foia/investigative-data-warehouse-report (describing the FBI's Investigative Data Warehouse as a massive centralized online repository for "intelligence and investigative data"); *see also* Fed. Bureau of Investigation, Dep't of Justice, Request for Records Disposition Authority, N1-65-10-31 (2010), *available at* http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-10-031_sf115.pdf (stating that the "Investigative Data Warehouse (lDW) is a centralized repository for copies of intelligence and investigative data with advanced search capabilities" providing users with "information needed to successfully accomplish the FBI's counterterrorism, counterintelligence, and law enforcement missions.").

[34] Levinson-Waldman, *supra* note 31, at 22 (2013); James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM) www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

[35] Levinson-Waldman, *supra* note 31, at 23 (2013).

[36] *See* Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5 (ISE-FS-200), at 2 (2009) [hereinafter Information Sharing Environment (ISE) Functional Standard], *available at* http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf (detailing that an Information Sharing Environment-Suspicious Activity Report is a Suspicious Activity Report "that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism.")); *see also* Levinson-Waldman, *supra* note 31, at 24 (stating that "[c]ertain criminal behaviors are considered automatic indicators of a terrorism nexus—[such as] attempting to enter a restricted site," while other non-criminal behavior can still "trigger a finding of a potential terrorism nexus" if the activity "would make a 'reasonable person' suspicious.").

[37] Information Sharing Environment (ISE) Functional Standard, *supra* note 36, at 29–30 (defining potential criminal or non-criminal activity that would require additional investigation).

1. BASIC DIFFERENCES BETWEEN EU AND U.S. DATA REGULATION REGIMES AND THE SAFE HARBOR AGREEMENT

There are many differences between the EU and U.S. data protection regimes that derive principally from the trust of Europeans towards the state to regulate the private sector containing the data and the distrust towards the state in the U.S.[38] The differences concern first, the fundamental presumptions concerning the processing of personal data. The presumption in the U.S. is that the processing of personal data is permitted unless it causes harm or is limited by law.[39] The opposite presumption is dominant in the EU where processing is prohibited unless there is a legal basis that allows it.[40] Second, the limits on contractual freedom differ. The EU Directive does not allow a data subject to enter into an agreement that permits a data controller from derogating fundamentally from their basic duties on the basis of Article 6 principles relating to data quality and Article 12 concerning access rights of the data subject to the data.[41] The U.S. data protection regime affords contract and market mechanisms greater latitude in setting data privacy standards and permits a significant degree of contractual "override" of the privacy-related interests of data subjects. Third, there are differences concerning the coverage of protection. The Directive is broad in scope and applies to the processing of personal data in the private and public sectors. U.S. law contains only limited sector-specific protections for sensitive information. It does not generally restrict automated processing.[42] Fourth, there are differences in the definition of the

---

38 Tourkochoriti, *supra* note 1, at 170 (interpreting the divergence in systems to be due to a difference in how citizens understand the role of the state).

39 Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1978–79 (2013) (discussing the U.S. approach that is largely unregulated, giving companies freedom to "try new kinds of data processing").

40 Data Protection Directive, *supra* note 2, arts. 1, 5, 6, 7 (regulating the processing of personal data).

41 *Id.*; *see also* Lee A. Bygrave, *Transatlantic Tensions on Data Privacy* 6 (Transworld: The Transatlantic Relationship and the Future Global Governance, Working Paper No. 19, Apr. 2013), *available at* http://www.iai.it/pdf/Transworld/TW_WP_19.pdf (discussing the "basic differences in the US and EU approach to data privacy regulation.").

42 Schwartz, *supra* note 39, at 1979 (discussing the U.S. sectoral approach to data privacy restrictions).

protected data. The EU protects information that is identifiable to a person, whereas the U.S. protects information that is actually linked to an identified person.[43] The EU approach is over inclusive, whereas the U.S. approach is under inclusive, given that whether information can be re-identified depends upon technology and corporate practices that permit the linking of de-identified data with already identified data.[44] Fifth, the scope of the protection differs, as generally under EU law, as well as under the law of the Council of Europe, data concerning activities even of a professional nature are protected.[45] Finally, the powers of the enforcing authorities differ. Member states have established independent authorities to implement the Directive in the EU that monitor and enforce the data privacy laws, thereby contributing to its consistent application throughout the Union.[46] In the U.S., the Federal Trade Commission shares some of the powers used by its counterpart authorities in Europe to combat unfair or deceptive acts or practices affecting commerce.[47] There are, nevertheless, limits on the scope of its activities. The Federal Trade Commission does not have jurisdiction over all companies,[48] and its

---

[43] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 880 (2014) (explaining the difference between the U.S. and EU systems in its treatment of data "in situations where the data is merely *identifiable* but the people to whom the data pertains are not currently *identified*"). Under EU law, an identifiable individual is an individual which, "while not identified, is described in this information in a way which makes it possible to find out who the data subject is by conducting further research." EUR. UNION AGENCY FOR FUNDAMENTAL RTS. & COUNCIL OF EUR., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 39 (2013).

[44] Schwartz & Solove, *supra* note 43, at 893–94 (discussing the concerns about computerized, automated decision making).

[45] *See* Joined Cases C-92/09 and C-93/09, Volker and Markus Schecke GbR & Hartmut Eifert v. Land Hessen, 2010 E.C.R. 662, ¶ 59 ("The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of the Convention, that the term 'private life' must not be interpreted restrictively . . . .").

[46] Data Protection Directive, *supra* note 2, art. 28 (requiring each Member State to create a supervisory authority and laying out the responsibilities of this supervisory authority).

[47] The Department of Transportation has similar authority over air carriers. 49 U.S.C. § 41712 (1994) (granting authority to the Secretary of Transportation to investigate "unfair or deceptive practice or an unfair method of competition").

[48] Exempt from the FTC's jurisdiction are many types of financial institutions, airlines, telecommunications carriers and other types of entities. 15 U.S.C. § 45(a)(2) (1952) (creating exemptions for "banks, savings and loan institutions . . . federal credit unions . . . common carriers . . . air carriers and foreign air carriers . . . .").

enforcement has not extended to the narrow range of Fair Information Practices used in the United States.

The standards of transferring data set by the 1995 EU Data Protection directive presuppose that the Commission determines that a non-EU country ensures an "adequate level of protection."[49] The EU privacy regime has succeeded through these "adequacy decisions" in leveling up the protection of privacy in the U.S.[50] The Department of Commerce of the U.S. issued the Safe Harbor Principles, recognized by the European Commission.[51] The

---

[49] Articles 25 and 26 of the Data Protection Directive of October 24, 1995 lay out the legal framework for transfers of personal data from the EU to third countries outside the EEA. Both the law of the Council of Europe and the European Union law foresee contractual clauses between the data exporting controller and the recipient in the third country as a possible means of safeguarding a sufficient level of data protection at the recipient. The European Commission has developed standard contractual clauses officially certified as proof of adequate data protection. Controllers can formulate ad hoc contractual clauses. Protection can also be guaranteed by binding corporate rules, usually multilateral, which may involve several European data protection authorities at the same time. *See* Article 29 Data Protection Working Party, *Working Document Setting Up a Framework for the Structure of Binding Corporate Rules,* WP 154 (June 24, 2008) (establishing a framework to provide guidance to organizations developing BCRs regarding international transfers of personal data); Article 29 Data Protection Working Party, *Working Document Setting Up a Table with the Elements and Principles to Be Found in Binding Corporate Rules*, WP 153 (June 24, 2008) (laying out the criteria for approval of BCRs).

[50] According to Article 26(1) of the Data Protection Directive, which contains provisions similar to those of the Additional Protocol to Convention 108, interests of the data subject may justify the free flow of data to a third country if the data subject has given unambiguous consent to the export of the data, the data subject enters or prepares to enter into a contractual relationship which clearly requires that the data be transferred to a recipient abroad, or transfer is necessary in order to protect the vital interest of the data subject, in case the data exists in public registers, the legitimate interests of others may justify free trans-border flow of data. This is also justified by an important public interest, apart from matters of national or public security, as they are not covered by the Data Protection Directive, or to establish, exercise or defend legal claims. Data Protection Directive, *supra* note 2, art. 26(1) (providing that a transfer of personal data to a third country may take place with other conditions).

[51] The Safe Harbor decision was determined following an opinion of Article 29 Working Party and an opinion of the Article 31 Committee delivered by a qualified majority of Member States. In accordance with Council Decision 1999/468, 1999, O.J. (L 184) 23 (EC), the Safe Harbor decision was subject to prior scrutiny by the European Parliament. Commission Decision 2000/520/EC, of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7 [hereinafter Safe Harbor Decision] (implementing the Safe Harbor Privacy Principles).

principles institute a system of self-certification of the companies, which have signed up for it by notifying the U.S. Department of Commerce while the U.S. Federal Trade Commission enforces the agreement.[52] Signing up for the arrangements is voluntary and resubmitted on an annual basis.[53] Financial services and telecommunication industries are outside the Federal Trade Commission enforcement powers and thus are excluded from the Safe Harbor,[54] whereas many industry and services sectors are present among certified companies including Internet companies and industries ranging from information and computer services to pharmaceuticals, travel and tourism services, healthcare and credit card services, which provide services in the EU internal market.[55]

The Safe Harbor Principles are intended for use by U.S. organizations receiving personal data from the EU for the purpose of meeting the presumption of "adequacy" foreseen in the EU regulations. Decisions by organizations to qualify for the safe harbor are voluntary, but once it complies with the principles, which rely in whole or in part on self-regulation, the failure to comply must be actionable.[56] According to the principles of the safe harbor agreement, an organization must *inform* individuals

---

[52] The Department of Commerce reviews Safe Harbor self-certifications and annual recertification submissions that it receives from companies to ensure that they include all the elements required and updates a list of companies that have filed self-certification letters. The FTC intervenes against unfair or deceptive practices, within its powers of consumer protection according to Section 5 of the Federal Trade Commission Act. The FTC is committed to review, on a priority basis, all referrals from EU Member State authorities. Federal Trade Commission Act, 15 U.S.C. § 5 (1914) [hereinafter Federal Trade Commission Act] (detailing prohibition of "unfair or deceptive acts or practices in or affecting commerce").

[53] Companies must also identify in their publicly available privacy policy that they adhere to the Principles and comply with them. By late September 2013, the Safe Harbor agreement had a membership of 3,246 companies. *See* European Commission Memo, *supra* note 13, at 2 (answering questions regarding "actions to be taken to restore trust in data flows between the EU and the U.S.").

[54] Federal Trade Commission Act, *supra* note 52, § 5 (detailing prohibition of "unfair or deceptive acts or practices in or affecting commerce").

[55] *See Communication from the Commission to the European Parliament and the Council, on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 5, COM (2013) 847 final (Nov. 27, 2013) [hereinafter *Communication on the Functioning of the Safe Harbour*], *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf ("51% are firms that process data of employees in Europe transferred to the US for human resource purposes.").

[56] Federal Trade Commission Act, *supra* note 52, § 5 (prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts).

about the purposes for which it collects and uses information about them.[57] An organization must offer individuals the opportunity to *choose* whether their personal information is to be disclosed to a third party or to be used for a purpose that is incompatible with the purposes for which it was originally collected or subsequently authorized.[58] Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding, or enters in agreement with third parties requiring that they provide at least the same level of privacy protection.[59] Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure alteration and destruction. Information must be *relevant* for the purposes for which it is used and individuals must have *access* at each moment and the *possibility to correct it.*[60] And effective privacy protection must include mechanisms for assuring compliance with the Principles, as well as recourse for individuals to whom the data relate affected by non-compliance with the principles.[61] The Safe Harbor agreement follows the EU definition of personal data saying that it concerns "data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form."[62]

Following the Commission's alert to the Department of

---

[57] Such organizations must also inform individuals about how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. *See Safe Harbor Privacy Principles*, *supra* note 5.

[58] In case of sensitive personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual, individuals must be given affirmative or explicit choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. *See id.*

[59] *Id.*

[60] *Id*.

[61] *Id*.

[62] *See* Safe Harbor Decision, *supra* note 51, at Annex I (delineating the Safe Harbor Privacy Principles and detailing the requirement that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection).

Commerce, the latter made it mandatory since March 2013 for a Safe Harbor company to make their privacy policy for customer/user data readily available on their public website.[63] For the Commission, the Department of Commerce must actively follow up on the effective incorporation of the Safe Harbor principles in companies' privacy policies rather than leave enforcement action to the initiative of individuals' complaints.[64] In this respect, apart from the FTC's enforcing authority within its powers against unfair or deceptive acts or practices in affecting commerce, the Commission proposes that organizations must commit to cooperating with the EU Data Protection Panel.[65] Further, Article 29 Working Party found insufficiencies in the

---

[63] *Communication on the Functioning of the Safe Harbour*, *supra* note 55, at 7 (discussing the requirement of transparency of companies' privacy policies under the Safe Harbor). They are also required to identify on their website an Alternative Dispute Resolution provider and to include a link to the Safe Harbor self-certification on the website of the Department of Commerce. *Id.* at 8. According to estimates, over thirty percent of the Safe Harbor members do not provide dispute resolution information in the privacy policies on their websites, citing Chris Connolly's (Galexia) appearance before the European Parliament LIBE Committee inquiry on 7 Oct. 2013. *Id.* at 7. According to the European Commission, up to ten percent of the certified companies have not fully complied with the requirement to post a privacy policy containing the Safe Harbor statement on their websites, while another ten percent post false claims of safe Harbor adherence. *Id.* About ten percent of companies claiming membership in the Safe Harbor are not listed by the Department of Commerce as current members of the scheme, which is due either to failure to resubmit their certification annually or to not having self-certified in the first place. *Id.* The Commission has also found that many privacy policies of self-certified companies are unclear as regards the purposes for which data are collected, and the right to choose whether or not it will be disclosed to third parties, raising issues of compliance with the principles of "Notice" and "Choice." *Id.* at 9. In parallel, the Department of Commerce does not maintain an updated list of the companies who are indeed adhering to the Safe Harbor Privacy Principles. *Id.*

[64] *Id.* at 9 (noting that the incorporation of the Safe Harbor Privacy Principles is not "sufficiently ensured").

[65] This is a body competent for investigating and resolving complaints lodged by individuals for alleged infringement of the Safe Harbor Privacy Principles by a U.S. company member. Companies that self-certify must choose to comply with independent recourse mechanism or to cooperate with the EU Data Protection Panel in order to remedy problems arising out of failure to comply with Safe Harbor Privacy Principles. Cooperation with the EU Data Protection Panel is mandatory when the U.S. company processes human resources personal data transferred from the EU in the context of an employment relationship. If the company commits itself to cooperate with the EU panel, it must also commit itself to comply with any advice given by the EU where it takes the view that the company needs to take specific action to comply with the Safe Harbor Privacy Principles including remedial or compensatory measures.

absence of a public body which would enforce the Safe Harbor principles, as the FTC has only limited powers which do not include sectors such as financial services (banks and insurance), telecommunications, transportation, employment relationships and non-profit activities.[66]

Under the Safe Harbor Agreement, the EU national Data Protection Authorities have the right to suspend data transfers to Safe Harbor certified companies in specific cases.[67] Independent from the powers they have under the Safe Harbor decision, EU national Data Protection Authorities also have powers distinct from those provided by the Safe Harbor Agreement that permit intervention in data transfers in order to assure compliance with the general principles of data protection set forth in the 1995 Data Protection Directive. These include the ability to intervene in the case of international transfers.[68] If a company has not joined the Safe Harbor Privacy Principles, then in case of data flow from a company situated in a member state of the European Union in a

---

[66] Article 29 Data Protection Working Party, *Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles"* 1, 3, WP 32 (May 16, 2000), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf (noting that safe harbor benefits only apply to organizations that are subject to FTC-type jurisdiction). Enforcement of the principles would rely either on Alternative Dispute Resolution or on the injunctive powers of the Federal Trade Commission which were not found to be satisfactory either as the bridge between the two layers is uncertain: the ADR bodies should notify to the FTC cases of failure to comply, but there is no obligation for them to do so. *Id.* at 7. The powers of the FTC are discretionary, which means that although the individuals concerned can file a complaint, there is no guarantee that the FTC will examine their case, and individuals do not have a right to be heard before the FTC, neither to enforce the ADR bodies' decisions nor to challenge them or the lack thereof. This means that individuals concerned by an alleged violation of the principles would not be assured of the right to stand before an independent instance. *Id.* at 7.

[67] "[S]uspension of transfers can be required in two situations, where: (a) the government body in the U.S. has determined that the company is violating the Safe Harbor Privacy Principles; or (b) there is a substantial likelihood that the Safe Harbor Privacy Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the company with notice and an opportunity to respond." *Communication on the Functioning of the Safe Harbour*, *supra* note 55, at 4 n.12.

[68] *Id*. at 4 (noting that EU national data protection authorities are competent to intervene, even in the case of international transfers, to ensure compliance).

parent company in the United States, the exporter based in the EU must go through the proceedings laid down in the EU Member state where the company is situated.[69] The European Commission can adapt the decision, suspend it, or limit its scope at any time in light of its implementation,[70] especially if there is a systemic failure on the U.S. side, if a body responsible for ensuring compliance with the Safe Harbor Privacy Principles in the United States is not fulfilling its role, or if the level of protection provided by the Safe Harbor is overtaken by the requirements of U.S. legislation.[71] Following the revelations on U.S. surveillance programs, German Data Protection Authority ("DPA") went further, expressing concerns that there may be violations of the principles in the

---

[69] *Id.* at 5.

[70] *See* Regulation 182/2011, 2011 O.J. (L 55) 13 (setting out the examination procedure).

[71] Gaps in transparency or in enforcement on the U.S. side due to the voluntary adherence of these companies, result in responsibility being shifted to European Data Protection authorities and to the companies, which use the scheme. *See, e.g.*, Düsseldorfer Kreis decision of 28/29 (Apr. 2010) *and* Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28/29 (Apr. 2010), *available at* http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile (expounding on decisions by German data protection authorities requesting companies transferring data from Europe to the U.S. to actively check that companies in the U.S. importing data comply with Safe Harbor Privacy Principles and recommending that at least the exporting company must determine whether the Safe Harbor Certification by the importer is still valid).

However, the European Data Protection Supervisor (EDPS), Peter Hustinx expressed an opinion at the European Parliament LIEBE Committee Inquiry on October 7, 2013 that "substantial improvements have been made and most issues now been settled" as far as Safe Harbor is concerned. Peter Hustinx, *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens* (Oct. 7, 2013), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf.
Past similar cases include the French CNIL finding in 2012 that Google provides insufficient information to its users on its personal data processing operations. Press Release, CNIL, Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data Across Services, *available at* http://ec.europa.eu/justice/data-protection/article29/documentation/otherdocument/files/2012/20121016_press_release_google_privacy_cnil_en.pdf (stating that "Google does not provide user control over the combination of data across its numerous services" and "Google does not provide retention periods").

Commission's decisions and requested that companies transferring personal data to U.S. providers inform the DPA on whether and how the concerned providers can prevent access by the NSA.[72]

All companies involved in the PRISM program that grant access to U.S. authorities to data stored and processed in the U.S. are Safe Harbor certified. The national security exception means that information obtained in violation of the Safe Harbor Agreement and transferred to the State authorities that conduct surveillance is not protected and the individual has no right whatsoever to it. Under the existing agreements, the Safe Harbor is not protective enough. The current Safe Harbor Agreement cannot survive under the new regulation proposed by the Commission, which is currently under deliberation.[73] If, under the new regulation (once it is enacted), the Safe Harbor provisions are amended to be compatible with the regulation, then there is a possibility that protection may be more efficient. The EU Regulation raises the standards of protection to a point, which must either force the renegotiation of the Safe Harbor and other agreements or is bound to be unenforceable.[74] Moreover, the Safe Harbor focuses essentially on notice and choice of the data and contains very few provisions prohibiting the acquisition and retention of data

---

[72] *See Conference of Data Protection Commissioners Says that Intelligence Services Constitute a Massive Threat to Data Traffic Between Germany and Countries Outside Europe*, DIE BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT (July 24, 2003), http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870 (discussing a resolution of a German Conference of data protection commissioners with regard to Internet traffic between companies in Germany and countries outside of Europe). The Irish and Luxembourg DPAs have not found an absence of compliance in complaints that reference the Safe Harbor agreement or violation of their national data protection laws. *See* David Meyer, *Privacy Campaigners Lose Luxembourg Bid to Censure Microsoft over NSA Links* (Nov. 18, 2013, 4:36 AM), *available at* https://gigaom.com/2013/11/18/privacy-campaigners-lose-luxembourg-bid-to-censure-microsoft-over-nsa-links/ (discussing a statement from the National Commission for Data Protection finding that Microsoft's data transfer from Europe to the U.S. did not break EU privacy law). The Irish High Court has granted an application for judicial review on the inaction of the Irish Data Protection Commissioner following a complaint by a student group. *See Communication on the Functioning of the Safe Harbour*, *supra* note 55 (discussing that the Irish DPA declined to investigate two complaints referencing the Safe Harbor program, one of which was filed by a student group, Europe v. Facebook (EvF), who had also filed other complaints).

[73] *See infra* Part 3.1.

[74] *See infra* Part 3.1.

altogether, which is imposed under the new regulation.[75]

The European Commission is trying, through interpretation, to limit the scope of the national security exception in the transatlantic flow of data,[76] pointing out that this exception as a limitation of a fundamental right must be narrowly construed, set forth in a publicly accessible law and necessary and proportionate in a democratic society.[77] Under current U.S. legislation, "there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes."[78] Further, companies do not systematically indicate in their privacy policies when they apply exceptions to the principles. Individuals and companies are not aware of what is being done with their data. The Commission also recommends that the privacy policies of self-certified companies should include information on the extent to which U.S. law allows public authorities to collect and process data transferred under the Safe Harbor.[79]

---

[75] *See infra* Part 3.1.

[76] *See* Safe Harbor Privacy Principles, *supra* note 5 (existing also in the Safe Harbor Privacy Principles as well as Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, mentioned throughout the paper, as well as the proposal for Regulation of the European Parliament and of the Council).

[77] *See Communication on the Functioning of the Safe Harbour*, *supra* note 55, at 19. The wording of the national security exceptions is that limitations are allowed only "to the extent necessary" to meet national security, public interest, or law enforcement requirements." Safe Harbor Decision, *supra* note 51, at annex I. The Commission also requires to be notified by the Department of any statute or government regulations that would affect adherence to the Safe Harbor Privacy Principles, while it stresses that the use of exceptions should be carefully monitored and the exceptions must not be used in a way that undermines the protection afforded by the Principles. *See* Article 29 Data Protection Working Party, Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles," EUR. COMM'N, WP 32 (May 16, 2000) [hereinafter Article 29 Working Party Opinion 4/2000]; *see also Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows*, at 11, COM (2013) 846 final (Nov. 27, 2013) [hereinafter *Rebuilding Trust*], *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[78] *Communication on the Functioning of the Safe Harbour*, *supra* note 55, § 7.2, at 17.

[79] This means that companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements and stresses that the exception must be used only to an extent that is strictly necessary or proportionate. The Commission's concern, however, is limited to imposing a

2. DATA COLLECTION AND THE U.S. AUTHORITIES UNDER THE U.S. PATRIOT ACT

2.1. Surveillance Within the U.S.

According to the Foreign Intelligence Surveillance Act, any government agency seeking to use electronic surveillance for foreign intelligence purposes inside the United States must obtain a warrant [80] from a special court, the Foreign Intelligence Surveillance Court. [81] The warrant may be issued upon government proof of "probable cause to believe that the target of the electronic surveillance" is an agent of a foreign power.[82] FISA imposes "minimization" procedures to protect the privacy rights of individuals who are not "targets" of FISA surveillance, but whose conversations or personal information are incidentally picked up in the course of electronic surveillance of legitimate targets under the

---

duty to the private actors who are collecting data that they may be obligated to disclose to certain authorities or other third parties. "For example, Nokia, which has operations in the U.S. and is a Safe Harbor member[,] provides [the] following notice in its privacy policy: 'We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate.'" European Commission Memo, *supra* note 13, at 5.

[80] 50 U.S.C. §§ 1801–1863 (1978).

[81] Established by the Foreign Intelligence Surveillance Act (FISA), the Foreign Intelligence Surveillance Court (FISC) consisted initially of seven, and now eleven, federal judges appointed by the Chief Justice of the United States to serve staggered terms on the FISC. *Id.* § 1822.

[82] *Id.* § 1805. FISA requires the Attorney General to approve all applications for FISA warrants, to report to the House and Senate Intelligence Committees every six months on the FISA process and the results of FISA-authorized surveillance, and to make an annual report to Congress and the public about the total number of applications made for FISA warrants and the total number of applications granted, modified, or denied. *Id.* § 1802. It expressly provides that no United States citizen or legal resident of the United States may be targeted for surveillance under FISA "solely upon the basis of activities protected by the first amendment to the Constitution of the United States." *Id.* § 1805. FISA requires the use of "minimization" procedures to protect the privacy rights of individuals who are not "targets" of FISA surveillance but whose conversations or personal information are incidentally picked up in the course of electronic surveillance of legitimate targets under the Act. *Id.*

Act.[83] Congress progressively extended the application of the FISA to pen register and trap-and-trace orders,[84] and to limited forms of business records, including documents kept by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[85]

The USA Patriot Act of 2001 empowered the Foreign Intelligence Surveillance Court to order the release of "any tangible thing," including historical and transactional information relating to telephone calls and emails, financial information and consumer credit information, to the FBI.[86] The first requirement is that this information is relevant to "an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."[87] The term "tangible things" may refer to any objects, or databases, library records and Internet browsing histories.[88] Phone records are to be collected containing subscriber information, toll billing records information or electronic communication transactional records,[89] as well as financial records. The second requirement is a statement of fact by the FBI proving that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation"[90] under the Act.[91]

---

[83] Minimization procedures govern the implementation of electronic surveillance to ensure that such implementation conforms to its authorized purpose. *Id.* § 1801. The procedures are adopted by the Attorney General and reviewed by the FISA Court. *Id.*

[84] This enables the government to obtain lists of the telephone numbers and e-mails contacted by an individual after the issuance of the order. 50 U.S.C. § 1842 (2008) (allowing access to pen registers and trap and trace devices for foreign intelligence and international terrorism investigations).

[85] 50 U.S.C. § 1862(a) (2001) (allowing access to certain business records).

[86] USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272 (codified as 50 U.S.C. § 1861(a)(1)(2012)).

[87] *Id.*

[88] Levinson-Waldman, *supra* note 31, at 8.

[89] 18 U.S.C. § 2709 (a).

[90] USA PATRIOT Act, *supra* note 86, at 50 U.S.C. § 1861(b)(2)(a).

[91] *See id.* § 1861 (c)(2)(D). To obtain a section 215 order, the U.S. Government must show that the item sought must be able to be "obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." *Id.*; *see also* ACLU v.

The Act authorizes the issuance of National Security Letters, a form of administrative subpoenas by which the FBI can obtain access to this material.[92] They are primarily used to obtain telephone toll records, e-mail subscriber information, and banking and credit card records.[93] Access to these records is allowed even if the subject is not a suspect in the investigation: under the Patriot Act, the FBI can issue an NSL when an authorized FBI official certifies that the records sought are "relevant to an authorized investigation."[94] The legality of these orders may be challenged by filing a petition within a year of their issuance.[95] Financial institutions are obliged to comply with a request for a customer's financial records when the authorities testify that the records are sought for foreign counterintelligence purposes.[96] Statutes authorizing National Security Letters include the Right to Financial Privacy Act,[97] the Fair Credit Reporting Act,[98] and the Electronic Communications Privacy Act.[99] For issuance of these letters, the requirement is "information or allegation" indicating that a threat to national security may occur, but not an "articulable factual basis" required by full FBI investigations.[100] This information can be kept for thirty years after the investigation's closure.[101] The

Clapper, 959 F. Supp. 2d 724, 743 (S.D.N.Y. 2013) ("Read in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas.").

92 18 U.S.C. § 2709 (a).

93 *Id.*; 12 USC § 3414 (allowing the FBI to gain access to records in financial institutions for purposes of foreign counterintelligence). Although initially used sparingly, in 2012 "the FBI issued 21,000 NSLs . . . primarily for subscriber information." LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 90 (Dec. 12, 2013) [hereinafter LIBERTY REPORT], *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

94 18 U.S.C. § 2709(b)(1).

95 USA PATRIOT Act, 50 U.S.C. § 1861 (f)(2)(A)(i).

96 12 U.S.C. § 3414(a)(5)(A).

97 12 U.S.C. § 3401.

98 15 U.S.C. § 1681.

99 18 U.S.C. § 2709.

100 John Ashcroft, U.S. Dep't of Justice, The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations 21–22, § VI.A., B. (2002) [hereinafter Ashcroft Guidelines].

101 OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006, 68 n.41 (Mar. 2008) [hereinafter 2008 OIG

statute allowing disclosure of a full credit report contains no limitations on dissemination. The financial and communications NSL statutes refer to the Attorney General Guidelines, which allow sharing with law enforcement agencies, the intelligence Community and foreign governments.[102] NSL derived information is uploaded into the Investigative Data Warehouse, and is likely to be available to the National Counterterrorism Center.

The Supreme Court has held that the "Fourth Amendment was not intended to interfere with the power of the courts to compel, through a subpoena the production" of evidence as long as the order compelling the production of records or other tangible objects meets the general test of "reasonableness."[103] Section 215 of the U.S. Patriot Act extends the principle of subpoena from the criminal investigation into the realm of foreign intelligence. Section 215 is based upon Supreme Court decisions, which held that individuals have no "reasonable expectation of privacy" in information they voluntarily share with third parties such as banks and telephone companies.[104] The philosophy behind this ruling is that what a person knowingly exposes to third parties is not a subject of Fourth Amendment protection.[105] The Court applied this reasoning to bank records[106] and to an individual's telephone calling records.[107] The Financial Privacy Act generally prohibited financial institutions from recording personal financial records and

---

REPORT], *available at* http://www.justice.gov/oig/special/s0803b/final.pdf ("The length of time that the FBI retains investigative information . . . depends on several factors . . . . In general, information related to intelligence investigations is retained in the FBI's files . . . for 30 years after a case is closed, and information related to criminal investigations is retained for 20 years after a case is closed.").

102 12 U.S.C. § 3414(a)(5)(B) (2013) ("The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counter-intelligence investigations . . . . "); 18 U.S.C. § 2709(d) (2013) ("The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General . . . . "); MICHAEL B. MUKASEY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL GUIDELINES FOR DOMESTIC FBI OPERATIONS 37, 41, § II (2008) [hereinafter MUKASEY GUIDELINES], *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf (providing guidelines for domestic FBI investigations).

103 Hale v. Henkel, 201 U.S. 43, 76 (1906).

104 Smith v. Maryland, 442 U.S. 735 (1979).

105 I am grateful to David Cole for this interpretation.

106 Miller v. United States, 425 U.S. 435, 440–41 (1976).

107 Smith v. Maryland, 442 U.S. 735, 742 (1979).

it expressly authorized them to disclose such records in response to lawful subpoenas and search warrants.[108]

The idea of separate spheres of privacy[109] that are not necessarily overlapping and are under the control of the individual is missing in U.S. law. According to this idea, if an individual consents to the use of some of her data by a private company, bank, credit card company, Internet service provider, telephone company, health-care provider, etc., this does not necessarily mean that she consents to further use of this data by other actors. The individual must retain the right to define and redefine at every moment who has access to what kind of information that concerns her.

In 2012, the Supreme Court held that long-term surveillance of an individual's location, effected by attaching a GPS device to his car, constituted a trespass and therefore, a "search" within the meaning of the Fourth Amendment.[110] Five Justices suggested that the surveillance might have infringed on the driver's "reasonable expectation of privacy," even if there had been no technical trespass and even though an individual's movements in public are voluntarily exposed to third parties.[111] A recent FISC opinion recognized that the "Supreme Court may someday revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, Smith remains controlling with respect to the acquisition by the government from service providers of non-content telephony metadata . . . ."[112] In another opinion of the

---

[108] Right to Financial Privacy Act, § 1114, Pub. L. 95-630, 92 Stat. 3707 (codified at 12 U.S.C. 3414) (1978).

[109] For a general analysis, see FERDINAND DAVID SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1992) (discussing the assumption in moral philosophy that social control is an intellectually and morally destructive source).

[110] United States v. Jones, 132 S. Ct. 945, 949–51 (2012).

[111] Justice Sonia Sotomayor observed in her concurring opinion that

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I would not assume that all information voluntarily disclosed to [others] for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Id. at 957 (Sotomayor, J. concurring) (citations omitted).

[112] *In re* Application of the Fed. Bureau of Investigation for an Order

same Court, the Court determined that the bulk telephony metadata program meets "the low statutory hurdle set out in Section 215."[113]

The phone metadata collected pursuant to Section 215 of the Patriot Act is retained for five years, unless it is responsive to authorized queries, and is thus retained pursuant to the procedures of the agency holding the information, e.g. the NSA or another agency such as the FBI with whom the NSA shared the data.[114] Similarly concerning onward transfers and sharing of data collected under Section 215, the orders for the production or telephony metadata among other requirements, prohibit the sharing of the raw data and permit the NSA to share with other agencies only data that are responsive to authorized queries for counterterrorism.[115]

The FISC has imposed limitations on the use of this metadata. The current program acquires a large amount of telephony metadata each day, which represents only a small percentage of the total telephony metadata held by service providers.[116] The FISC orders defining the use of this data prohibited the government from accessing the metadata for any purpose other than to obtain foreign intelligence information.[117] The FISA court

---

Requiring the Production of Tangible Things from [Redacted version], Docket No. BR 13-158 (FISC Oct. 11, 2013), pp. 5–6.

113 *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted version], Docket No. BR 13-109 (FISC Aug. 29, 2013), p. 22.

114 MUKASEY GUIDELINES, *supra* note 102. The guidelines provide that any information obtained will be kept in accordance with a records retention plan approved by the National Archives and Records Administration. The latter does not establish specific retention periods, providing instead that records should be deleted or destroyed when the agency determines they are no longer needed for administrative, legal, audit or other operational purposes. *Id.*

115 *Id.* at 8. The Attorney General's guidelines for Domestic FBI Operations also provide that the FBI may disseminate collected personal information to other U.S. intelligence agencies as well as to law enforcement authorities of the executive branch for a number of reasons or on the basis of other statutes and legal authorities.

116 A similar metadata program for Internet communications under the authority of FISA's pen register and trap-and-trace provisions (rather than the authority of section 215) was suspended, for operational and technical reasons, and because the program was insufficiently productive to justify the cost. *See* LIBERTY REPORT, *supra* note 93, at 97.

117 Access to this data is allowed only when there are facts giving rise to a "reasonable, articulable suspicion" that the selection term to be queried "is associated with a specific foreign terrorist organization," a finding which is made

does not review or approve individual queries either in advance or after the fact. It sets only the criteria for queries and receives reports every thirty days from the NSA concerning the number of identifiers used to query the metadata and the results of these queries.[118] While the FISC requires that the "reasonable, articulable suspicion" requirement be met, the NSA does not have to go back to the Court to justify particular queries, deciding itself whether this requirement is met. [119] While the administration has emphasized that only 300 identifiers were used to query the data during 2012, the NSA has acknowledged that it can obtain additional phone numbers that are up to three "hops" out from the original number.[120] These hops refer to the number of connections from the original number: the first "hop" is to phone numbers the original number is in contact with, the second is numbers in contact with the first "hop" numbers, and the third is the numbers in contact with those "second hop" numbers.[121] While the agency may not run a three-hop analysis on every contact, a decision to do so gives it access to the phone records of millions.

2.2. Surveillance Outside the U.S.

The United States Foreign Intelligence Surveillance Act of 2008 adopted different rules for international communications depending on whether the target of the surveillance was a "United States person" (a category including both American citizens and non-citizens who are legal permanent residents of the United States)[122] or a "non United States person."[123] According to Section

---

by one of twenty-two specially trained persons. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 3 (2013) [hereinafter WHITE PAPER], *available at* http://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html; *see also* LIBERTY REPORT, *supra* note 93, at 98 (discussing recommendations of the President's Review Group on Intelligence and Communications Technologies).

118 *Id*. at 100.

119 Levinson-Waldman, *supra* note 31, at 46.

120 WHITE PAPER, *supra* note 117, at 4.

121 *Id*. at 3–4.

122 *See* 50 U.S.C. § 1881a(i).

> 'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101

702 of the FISA Amendments Act ("FAA"), if the target of foreign intelligence surveillance is a non-United States person who is "reasonably believed to be located outside the United States," the Attorney General and the Director of National Intelligence may authorize surveillance upon the issuance of an order from the FISC without showing a probable cause to believe that the target is an agent of a foreign power, even if the interception takes place inside the U.S.[124] Section 702 authorized the FISC to approve annual

> (a)(20) of Title 8), an unincorporated association, a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

50 U.S.C. § 1801(i).

[123] LIBERTY REPORT, *supra* note 93, at 135.

> [I]f the target of the surveillance is a United States person, the same FISA procedures apply—without regard to whether the target is inside or outside the United States. . . . [This means that] surveillance is permissible only if it is intended to acquire foreign intelligence information and the FISC issues a warrant based on a finding that there is probable cause to believe that the United States person is an agent of a foreign power, within the meaning of FISA.

Id. See also 50 U.S.C. § 1881a(a).

[124] *Id.* An electronic communication service provider receiving a directive from the Attorney General and the Director of National Intelligence may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court. 50 U.S.C. § 1881a(h)(4)(A). Section 1881a mandates that the Government obtain the Foreign Intelligence Surveillance Court's approval of targeting and minimization procedures, and a governmental certification regarding proposed surveillance. 50 U.S.C. § 1881a(d); 50 U.S.C. § 1881a(e). Among other things, the Government's certification must attest that (1) procedures are in place "that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC] that are reasonably designed to ensure that an acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States;" (2) minimization procedures adequately restrict the "acquisition, retention, and dissemination of nonpublic information about non-consenting U.S. persons," as appropriate; (3) "guidelines have been adopted . . . to ensure compliance with" targeting limits and the Fourth Amendment; and (4) the procedures and guidelines referred to above comport with the Fourth Amendment. 50 U.S.C. § 1881a(g)(2); *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance*, FED. OF AM. SCI. (2000), http://fas.org/irp/nsa/standards.html; 50 U.S.C. § 1881a(d)(1)(A). The FISC assesses whether the targeting procedures are "reasonably designed" (1) to "ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States;" and (2) to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known . . . to be located in the United States." 50 U.S.C. § 1881a(d)(1)(A); 50 U.S.C. § 1881a(d)(1)(B).

certifications submitted by the Attorney General and the Director of National Intelligence ("DNI") that identify certain categories of foreign intelligence targets whose communications may then be collected, subject to FISC-approved targeting and minimization procedures.[125] The NSA determines which individuals to target pursuant to FISC-approved certifications, but the Government is not obliged to "describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized basis."[126] The NSA, on the basis of some identifiers (e-mail addresses or telephone numbers) that it reasonably believes are being used by non-U.S. persons located outside of the U.S. to communicate foreign intelligence information within the scope of the approved categories, then acquires the content of telephone calls, e-mails, text messages, photographs, and other Internet traffic using those identifiers from service providers in the U.S.[127]

> Section 702 requires that NSA's certifications attest that[:] [1] "a 'significant purpose' of any acquisition is to obtain foreign intelligence information . . . directed at international terrorism, nuclear proliferation, or hostile cyber activities[;] [2] that [the acquisition] does not intentionally target a United States person[;] [3] that it does not intentionally target any person known at the time of acquisition to be in the United States[;] [4] that it does not target any person outside the United States for the purpose of targeting a person inside the United States[;] and [5] that it meets the requirements of the Fourth Amendment.[128]

The FISC held in one instance [129] that the minimization procedures that applied to NSA's upstream collection of electronic communications did not meet the requirements of FISA or the Fourth Amendment, as the NSA's use of upstream collection often

---

125 LIBERTY REPORT, *supra* note 93, at 136.

126 50 U.S.C. § 1881a(g); *see* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1156 (2013) (Breyer, J., dissenting) (discussing Government's permitting of surveillance on a programmatic basis).

127 LIBERTY REPORT, *supra* note 93, at 136.

128 *Id*. at 136–37.

129 *In re* DNI/AG 702(g), Docket Number 702(i)-11-01, at 17, n.15 (FISC Oct. 3, 2011) [hereinafter FISC Oct. 3, 2011 Opinion].

involves the inadvertent acquisition of multi-communication transactions ("MCTs"),[130] many of which do not fall within the parameters of section 702. Thus the government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime to "engage in electronic surveillance under color of law except as authorized by statute . . . ."[131] For the Court, "[t]he fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications . . . does not render NSA's acquisition of those transactions 'unintentional.'"[132] Thus, due to the broad method of collection and technical reasons, personal data is collected that may not be relevant to foreign intelligence.

Section 702 affords United States persons the same protection against foreign intelligence surveillance when they are outside the United States as the FISA affords them when they are inside the country's borders. A United States person may not lawfully be targeted for foreign intelligence surveillance unless the FISC issues a warrant based on a finding that there is probable cause to believe that the targeted United States person is an agent of a foreign power.[133] Section 702 also has an impact on the privacy of communications of United States persons due to the risk of inadvertent interception. When incidental acquisition occurs in the

---

130 MCTs arise when many communications are bundled together within a single Internet transmission, resulting in a situation where the lawful interception of one communication in the bundle requires in the interception of them all.

131 FISC Oct. 3, 2011 Opinion, *supra* note 129.

> NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing only a single discrete communication to, from or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector. . . . The sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of the transactions is not feasible.

Id. at 31 (citations omitted). What is more,

> Internet service providers are constantly changing their protocols and the services they provide, and often give users the ability to customize how they use a particular service . . . . As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.

Id. at 32 (citations omitted).

132 *Id*. at 45.

133 LIBERTY REPORT, *supra* note 93, at 146.

course of Section 702 surveillance, existing minimization procedures require that any intercepted communication with a United States person, and any information obtained about a United States person, must be destroyed unless it has foreign intelligence value.[134]

As the Committee of Experts commissioned by the President found, Section 702 allows the government to target foreigners abroad under a lower standard than if the target was an American abroad or a foreigner in the U.S. communicating with an American in the U.S.[135] It is often difficult to determine whether the e-mail address, Internet communication, or telephone number of the non-targeted participant in a legally acquired communication belongs to a United States person, because that information often is not apparent on the face of the communication. Thus, there is a risk that communications involving United States persons will not be purged, and instead will be retained in a government database.[136] Furthermore, the very concept of information of "foreign intelligence value" is vague and can easily lead to the preservation of private information about known United States persons whose communications are incidentally intercepted in the course of a legal Section 702 interception.[137]

FISC proceedings are non-adversarial, and there is no representation before the FISA Court of the interests of the data subject during the consideration of an application for an order.[138] In addition, the U.S. Supreme Court has established that neither individuals nor organizations have standing to bring a lawsuit under Section 702 because they cannot know whether they have been subject to surveillance or not.[139] The orders of the FISC are

---

134 NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, § 5(1) (2011).

135 LIBERTY REPORT, *supra* note 93, at 148 (arguing that the current approach does not adequately protect the privacy of United States persons whose communications are incidentally acquired).

136 *Id.* at 149.

137 *Id.*

138 EUR. COMM'N, REPORT ON THE FINDINGS BY THE EU CO-CHAIRS OF THE AD HOC EU-US WORKING GROUP ON DATA PROTECTION 16, (Nov. 27, 2013) [hereinafter AD HOC EU-U.S. WORKING GROUP REPORT], *available at* http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

139 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (Breyer, J.,

classified, and companies are required to maintain secrecy regarding the assistance they are required to provide, which means that there are no avenues, judicial or administrative, for either U.S. or EU data subjects to be informed of whether their personal data is being collected or further processed.[140] There are thus no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.[141] Although "there is judicial oversight for activities that imply a capacity to compel information[,] . . . [t]here is no judicial approval of individual selectors to query the data collected under Section 215 or tasked for collection under section 702."[142] The FISC operates ex parte, and in camera, issuing classified opinions unless they are declassified.[143]

From the European point of view, the program under Section 702 violates the principle of reciprocity. As the Committee on Foreign Affairs of the European Parliament notes, although the Fourth Amendment of the U.S. Constitution does not apply to non-U.S. citizens, the European legal framework does not discriminate on the basis of citizenship for the rights that it protects, among which is the right to privacy.[144]

---

dissenting) (holding that Amnesty International did not have standing to challenge Section 702).

140 AD HOC EU-U.S. WORKING GROUP REPORT, *supra* note 138, at 17.

141 *Id.*

142 *Id.* at 18.

143 *Id.*

144 *See Working Document on Mass Surveillance*, *supra* note 12, at 2; *see also* LIBERTY REPORT, *supra* note 93, at 156–57 (outlining three proposals by the Committee commissioned by the President that are not fully satisfactory from the European point of view). The Committee suggests that there should be "three primary differences between the standards governing the acquisition of communications of United States persons and non-United States persons" which are warranted by the special obligation the U.S. government owes to its people:

> First, United States persons [should] be targeted only upon a showing of *probable cause*, whereas non-United States persons [should] be targeted upon a showing of *reasonable belief*. Second, United States persons [should] be targeted only if there is a *judicial warrant* from the FISC whereas non-United States persons [should] be targeted *without . . . warrant*, but with careful after-the-fact review and oversight. Third, the minimization requirements for communications of United States persons would not extend fully to non-United States persons located outside the United States, but importantly, information collected about such persons [should] not be disseminated unless it is relevant to the national security of the United States or [its] allies.

Id.

The Committee on Foreign Affairs also recommends that in the absence of a specific and compelling showing, the U.S. government should follow the model of the Department of Homeland Security and apply the Privacy Act of 1974 in the same way to both U.S. and non-U.S. persons.[145] The Privacy Act of 1974 provides what are known as "privacy fair information practices" for systems of records held by federal agencies.[146] These practices are designed to safeguard personal privacy, and include a set of legal requirements meant to ensure both the accuracy and security of personally identifiable information in a system of records.[147]

Presently, there are fewer safeguards for EU citizens in the U.S., as well as a lower threshold for the collection of their personal

---

[145] The Privacy Act regulates the federal government's collection, use, and disclosure of all types of personal information. 5 U.S.C. § 552(a). The law applies to the government's collection of all kinds of personal data concerning "education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." *Id.* § 552a(a)(4). The Act is generally less protective than European legislation on the same issues and contains many exceptions in particular for law enforcement agencies and the CIA. *Id.* § 552a(j). Although the NSA does not qualify for a general exemption, it can refer to the specific exemption for national security records under NSA/Central Security Service Privacy Act Program, 32 C.F.R. § 322 (2006). *Id.* § 552a(k)(2).

[146] This law provides protection analogous to the ones European nations follow under Directive 95/46. *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 632 (2007) (noting that the Privacy Act regulates government use of data from "start to finish.").

[147] LIBERTY REPORT, *supra* note 93, at 158. According to the Privacy Policy Guidance Memorandum of the Department of Homeland Security, the Privacy Act must apply in the same way to both U.S. persons and non-U.S. persons. As stated in the Memorandum, personally identifiable information ("PII") that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, legal permanent resident, visitor, or alien. This means that non-U.S. persons have the right to access their PII and the right to amend their records, absent an exemption under the Privacy Act. Because of statutory limitations, the policy does not extend or create a right of judicial review for non-U.S. persons. Intelligence agencies today are covered by the Privacy Act, and are granted exemptions to accommodate their need to protect matters that are properly classified, law-enforcement sensitive, or investigatory in nature. The NSA has filed twenty-six systems of records notices advising the public about data collections, including from applicants seeking employment, contractors doing business with the agency, and in order to conduct background investigations. Memorandum No. 2011–01 from the Dep't of Homeland Sec., Privacy Policy Guidance Memorandum of the Department of Homeland Security 2 (Feb. 11, 2011).

data.[148] The procedures regarding targeting and minimization of data collection apply only to U.S. citizens. Similarly, the constitutional protections of the First and Fourth Amendments do not apply to EU citizens that do not reside in the U.S. For the Commission, there is a lack of clarity concerning some available U.S. legal bases for authorizing data collection, such as Executive Order 12333, concerning the existence of other surveillance programs, as well as limitations applicable to these programs.[149] The Commission also finds that while there is a degree of oversight by the three branches of government that applies in specific cases including judicial oversight, for activities that imply a capacity to compel information there is no judicial approval for how the data collected is queried. Judges are not asked to approve the 'selectors' or analyze the criteria employed to examine the data and mine usable pieces of information.[150] Nor is there judicial oversight of the collection of foreign intelligence outside the U.S., which is conducted under the sole competency of the Executive Branch.[151]

As the European Commission notes, the legal framework of the U.S. intelligence collection programs needs more transparency. This includes interpretation by U.S. courts, as well as clarification on the quantitative dimension of U.S. intelligence collection programs.[152] The European Commission also requested an extension of the safeguards available to U.S. citizens and residents to EU citizens not residing in the U.S., an increase in the transparency of intelligence activities, and further strengthening of oversight.[153] The European Commission further suggested that the role of the FISC should be strengthened by "introducing remedies for individuals . . . [which] could reduce the processing of personal data of Europeans that are not relevant for national security purposes."[154]

---

148 European Commission Memo, *supra* note 13, at 9 (noting the different processing safeguards for EU citizens and U.S. citizens).

149 AD HOC EU-U.S. WORKING GROUP REPORT, *supra* note 138, at 17.

150 *Id*. at 10, 18.

151 *Id*. at 18.

152 *Id*. at 7.

153 *Rebuilding Trust*, *supra* note 77, at 7.

154 *See* European Commission Memo, *supra* note 13, at 7.

3. FILLING IN THE GAPS IN THE PROTECTION

The Charter of Fundamental rights of the European Union has an explicit clause protecting personal data[155] in addition to the clause guaranteeing respect for private and family life.[156] The system of data protection in the EU is composed of Directives 95/46 and 2002/58 in the telecommunications sector, Regulation 45/20001 and Directive 2006/24 regarding the field of police and judicial cooperation in criminal matters, and Framework Decision 2008/977/JHA.[157] The proposed regulation, however, establishes a stricter regime of privacy protection within the EU, harmonizing the existing national legislation that has been used to implement Directive 95/46.[158] However, the remaining question is whether the large scale collection and processing of personal information under U.S. surveillance programs is necessary and proportionate to meet the national security interests.[159] If interpreted properly, this principle of proportionality – omnipresent in the European Convention and in article 52(1) of the Charter of Fundamental Rights of the EU – could result in the important protection of data.

Expressing a fundamental principle of the rule of law, which is as old as Aristotle, is universalizable.[160] For Aristotle, justice was a matter of the right proportion between two extremes, an "intermediate between a sort of gain and a sort of loss."[161]

---

155 Charter of Fundamental Rights of the European Union art. 52, 2000 O.J. (C 364) 1 [hereinafter Charter of Fundamental Rights] (stating "[a]ny limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.").

156 *Id.* art. 7 (stating "[e]veryone has the right to respect for his or her private and family life, home and communications.").

157 Council Framework Decision 2008/977/JHA, of November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 2008 O.J. (L 350) 60.

158 Proposed Regulation, *supra* note 3, at 4 (harmonizing the rules purportedly increased legal certainty and reduced impediments to global operations).

159 *Rebuilding Trust*, *supra* note 77, at 4.

160 For Aristotle, in a world of contingence and perpetual flux, justice is a matter of right proportion. The right proportion is defined as the intermediate between two extremes. *See* ARISTOTLE, NICOMACHEAN ETHICS, *in* THE COMPLETE WORKS OF ARISTOTLE 1785 (Jonathan Barnes ed., 1984).

161 *Id.* at 1787–89. Further,

According to the principle of proportionality, limitations to individual freedoms must be necessary and appropriate to achieve their function, and they must use the least intrusive instruments possible to achieve the desired result. Since finding the right proportion is also a matter of interpretation, the principle by itself is dependent on the ad hoc evaluations and concerns of justices in association with the margin of appreciation of the state – another principle used by the European Court of Human Rights ("ECtHR").

3.1. New EU Regulation Strengthening the Protection of Data Privacy in the Private Sector and the Changes It Brings

The proposed regulation has the potential to indirectly limit the amount of information that ends up in the government's hands by limiting the amount of information that private actors can collect, process, and store.[162] Its clauses are so radical that it has been criticized as carrying a potential for destabilizing the current status quo.[163] For example, it will force the Safe Harbor principles to be redefined as principles used only for the possibility of notice and choice, and will focus less on the amount of information retained and processed. Although the new regulation contains a national security exception by limiting the private information in the hands of the private sector, it may indirectly limit the possibilities of state surveillance.

> [t]he man who acts unjustly has too much, and the man who is unjustly treated too little, of what is good. In the case of evil the reverse is true; for the lesser evil is reckoned a good in comparison with the greater evil, since the lesser evil is rather to be chosen than the greater, and what is worthy of choice is good, and what is worthier of choice a greater good.

Id. at 1786.

[162] The Committee for Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament overwhelmingly backed the European Commission's data protection reform proposals. The LIBE vote gave a mandate to the rapporteurs to negotiate with the Council of the EU. President Barroso underlined the importance of the reform and called for a swift adoption before the end of this parliamentary term. *See* Memorandum from the Eur. Comm'n, LIBE Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013) [hereinafter LIBE Committee Vote], *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[163] Schwartz, *supra* note 39, at 1994.

The Regulation develops a "right to be forgotten"[164] should a number of conditions apply and elaborates stricter requirements before "consent" can be used as a justification for data processing.[165] The right to be forgotten is described as the right of data subjects to have their personal data erased and no longer processed, and to obtain from third parties the erasure of any links to, or copies or replication of, that data:

> [W]here . . . the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; . . . the data subject withdraws consent on which the processing is based[;] . . . the data subject objects to the processing of personal data; [or] the processing of the data does not comply with this Regulation . . . .[166]

As it stands, this means that if an EU national complains to a supervising authority, the supervising authority can order and enforce any processor to, for example, erase material that concerns that national.[167] The Court of Justice of the EU recently held that even the operator of a search engine like Google engages in activities that "must be classified as 'processing' within the meaning of [Article 2(b) of Directive 95/46]" since the engine

---

164 Proposed Regulation, *supra* note 3, art. 17(1), at 51 ("The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data . . . .").

165 *Id*. art. 7 (requiring, among other things, that any written consent form must be presented to the subject independently).

166 *See* LIBE Committee Vote, *supra* note 162, at Commission Proposal, art. 17. This right is particularly relevant when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the Internet. The further retention of the data, however, should be allowed where it is necessary for historical, statistical and scientific research purposes; for reasons of public interest in the area of public health; and for exercising the right of freedom of expression when required by law, or where there is a reason to restrict the processing of the data instead of erasing them. Proposed Regulation, *supra* note 3, at Proposed Regulation Recital, 53.

167 Sam Schechner, *Google Sued in Europe-Privacy Test Case*, WALL ST. J. (Sept. 4, 2013), http://online.wsj.com/article/SB10001424127887323623304579055271398748940.html (describing the privacy case brought against Google by former Formula One racing president Max Mosley).

collects data which it eventually makes publicly available.[168] In exploring the Internet automatically, constantly, and systematically in search of published information, "the operator of a search engine 'collects' such data which it subsequently 'retrieves,' 'records,' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results."[169] The fact that the search engine operator applies this process to both non-personal and personal data and does not distinguish between the two is not significant for the court.[170] Also insignificant is the fact that the search engine is merely reorganizing and displaying data that is already published somewhere else on the Internet.[171] Search engines are "controllers" in the sense that they direct and determine the purpose and means of that activity, and process personal data within the framework of that activity.[172] They also play "a decisive role in the overall dissemination of those data" as they "render[] the latter accessible to any Internet user making a search on the basis of the data subject's name, including to Internet users who otherwise would not have found the web page on which those data are published."[173] Although publishers of websites have the option of indicating to search engine operators that they wish specific information published on their site to be wholly or partially excluded, this does not mean that the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.[174]

Another measure that the new regulation imposes is the prior approval of supervising authority for any processing of personal data.[175] This means that the data protection authorities whose

---

168 Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014), § 28, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=103833.

169 *Id. § 28.*

170 *Id.*

171 *Id.* §§ 28–30.

172 *Id.* § 33.

173 *Id.* § 36.

174 *Id.* § 39.

175 Proposed Regulation, *supra* note 3, art. 34, § 3.4.6.2. The European Parliament gave its support to the Commission's proposal to have a "one-stop

powers also cover the public sector must be consulted for any data collection program even in order to establish that the national security exception applies.[176] The regulation further establishes a right to object to processing for marketing purposes[177] and the right not to be subject to profiling.[178] This is defined as automated processing intended to evaluate certain personal aspects relating to a person or his or her performance at work, economic situation, location, health, personal preferences, reliability, or behavior for use in targeted ads.[179] The directive predicts some exceptions, including those related to public security, prevention, investigation, detection and prosecution of criminal offences of economic or financial interest, in particular.[180] However, the right not to be subject to profiling by the private sector implies an inability of the government to conduct data mining and obtain data concerning an individual from the private sector.

The new regulation requires controllers and processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected." [181] The regulation empowers the state supervisory authorities to impose administrative sanctions, which may reach up to five percent of the annual worldwide turnover to enterprises violating its clauses.[182]

The regulation defines its territorial scope as covering the "processing of personal data in the context of the activities of a . . . controller or a processor in the Union," whether the processing

---

shop" for companies that operate in several EU countries, and for consumers who want to complain against a company established in a country other than their own. Companies will have to deal with a single national data protection authority in the country where they are based. Proposed Regulation, *supra* note 3, Proposed Regulation Recital, at 98.

176 *See infra* Part 3.3 (describing the case law of the European Court of Human Rights, which concerns the requirements that the legislation establishing a data collection program must meet).

177 Proposed Regulation, *supra* note 3, art. 19, § 2.

178 *Id.* art. 20, § 2.

179 *Id.*

180 *Id.* art. 21(1)(a-c).

181 *Id.* art. 30, § 1.

182 *Id.* art. 79, § 2(c) (following European Parliament's Vote). The European Commission's initial proposal, before the Snowden revelations, was for fines up to two percent of annual turnover. *Id.* art. 6.

takes place in the EU or not.[183] It also applies to the processing of personal data of subjects in the EU by a controller or a processor, not established in the EU, where the processing activities are related to the offering of goods or services irrespective of payment to subjects in the EU or to the monitoring of data subjects.[184] On the basis of this clause, and given the radical nature of the new regulation, the Safe Harbor Agreement must be reformed.[185] These clauses can significantly affect the amount of information retained by U.S. authorities, as they obtain it from the private sector through the data mining processes.

Thus, since the EU regulations do not apply in cases of national security, data collected in violation of the existing directive and the proposed regulation in the EU pertaining to national security will be appropriated by surveillance authorities. If the private sector possesses information in violation of the EU's existing regulation that is handed over to the state, the individuals are not protected by the existing regulation. The regulation should be interpreted as allowing for sanctions on the private actors who are violating these clauses because this is material they were not allowed to collect in the first place. Although citizens cannot be protected against the state, in order for the protection to make sense in the future, the private actors should pay the penalties set forth in the regulation.[186]

While there are sparse U.S. state laws offering varying degrees of security and certainty, there is no U.S. federal regulation on data privacy protection for consumers.[187] Thus, the EU Commission has announced that once the new regulation obtains legal force, it expects the U.S. to implement a single and coherent set of data protection rules in order "to create a stable basis for personal data flows between the EU and the U.S.," considering that "[i]nter-

---

183 *Id*. art. 3, § 1 (following European Parliament's Vote); *see also* LIBE Committee Vote, *supra* note 162.

184 Proposed Regulation, *supra* note 3, art. 3, § 2 (following European Parliament's Vote); *see also* LIBE Committee Vote, *supra* note 162.

185 *See also Rebuilding Trust*, *supra* note 77, at 7. The proposed regulation contains exceptions to the prohibition of the processing of personal data. However, proposed regulation article 9(1), among others, notes that the "processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests." Proposed Regulation, *supra* note 3, art. 9, § 2(g).

186 *Id*. art. 9(2)(j).

187 Similarly, there is no common definition of personal information. *See supra* Part 1.

operability and a system of self-regulation is not enough. The existence of a set of strong and enforceable data protection rules in both the EU and U.S. would constitute a solid basis for cross-border data flows."[188]

3.2. Data Retention Directive

The data retention directive aims to harmonize Member States' data retention provisions in order to enhance protection of privacy. [189] These provisions dictate provider obligations concerning publicly available electronic communication services and public communication networks, with respect to the retention of certain data generated or processed by these providers for the purpose of investigation, detection, and prosecution of serious crimes.[190] In this respect, the Directive operates as an exception to the protective regime in the telecommunications sector guaranteed by Directive 2002/58,[191] complementing the principles established by Directive 95/46. The Court of Justice of the European Union recently ruled that the data retention directive is invalid because it does not contain enough guarantees for the protection of data privacy.[192] In this respect, it followed the findings of the Advocate

---

[188] European Commission Memo, *supra* note 13, at 8.

[189] Council Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, pmbl., ¶¶ 5–10 [hereinafter Council Directive 2006/24/EC].

[190] *See id.* at 54, 56.

[191] Council Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, *amended by* Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, and by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, 2009 O.J. (L 337) 37.

[192] Joined Cases C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Natural Res. and Kärntner Landesregierung et al., 2013 EUR-Lex CELEX LEXIS 1 at 157 (Dec. 12, 2013) [hereinafter Digital Rights Ireland Ltd.], *available at* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=145562.

General of the Court of Justice, almost verbatim.[193]

The Directive applies to traffic and location data on legal entities and natural persons.[194] It does not, however, apply to electronic communications, including information derived from using an electronic communications network.[195] It leaves the Member States the option to define the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data. In doing so, the Member States are required to act in accordance with necessity and proportionality, subject to the relevant provisions of EU Law or public international law, and in particular the European Convention of Human Rights ("ECHR") as interpreted by the European Court of Human Rights.[196] The data to be retained is necessary to trace and identify the source of a communication: actual telephone numbers, and the names and addresses of subscribers or registered users that have fixed network or mobile telephones.[197] This retention practice allows for

---

[193] *Cf.* Bundesverfassungsgericht [BvR] [German Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, 2 (Ger.) (decision of the German Federal Constitutional Court, holding that the implementing legislation did not set out appropriate safeguards concerning data security and limitation of legitimate use of the retained data); FRANZISKA BOEHM & MARK D. COLE, DATA RETENTION AFTER THE JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION (2014) (describing the decision of the Romanian Federal Constitutional Court, which found that the continuous limitation of the right to privacy, foreseen in the Data Retention Directive, makes the essence of the right); PI. ÚS 24/10, 22.03.2011 [Czech Republic Constitutional Court Judgment of Mar. 22, 2011], Data Retention in Telecommunication Services (Czech.) (decision of the Czech Republic's Constitutional Court, annulling part of the Act on Electronic Communication, and legally nullifying the obligation to retain traffic and location data and to make this data available to competent authorities). *See generally* Arianna Vedaschi & Valerio Lubello, Presentation at the Harvard Law School Roundtable: Constitutionalism Across Borders and the Struggle Against Terrorism: Data Retention and its Implications for the Fundamental Right to Privacy (Mar. 6–7, 2014).

[194] Council Directive 2006/24/EC, *supra* note 189, art. 1, § 2.

[195] *Id*.

[196] *Id*. art. 4.

[197] *Id*. art. 5, § 1(a)(1). Article 5, § 1(a)(2) further specifies that the user ID(s) allocated to a person's email address or Internet connection may be retained, as well as the name and address of the subscriber or registered user and "the user ID and telephone number allocated to any communication entering the public telephone network." *Id*. art. 5, §1(a)(2)(ii). The directive also covers the data necessary to identify the destination of a communication, the numbers dialed and re-routed, names of subscribers and users, user IDs or telephone numbers, names and addresses of subscribers or registered users, and the user IDs of recipients for Internet email and telephone. *Id*. art. 5, § 1(b). It also covers the data necessary to identify the date, time, and duration of a communication. *Id*. art. 5, § 1(c). Data necessary to identify the type of communication such as the telephone and

information to be retained for six months to two years from the date of the communication.[198] The directive establishes conditions of storage and access to the data,[199] and makes the national Data Protection Authorities responsible for monitoring its application regarding the security of the stored data.[200]

For the Court, although the retention of data satisfies an objective of general interest in the prevention of offenses and the fight against terrorism, it is an interference that is not proportionate to this legitimate objective.[201] According to the Court, the Directive does not define the limits of the competent national authorities' access to the data and their subsequent use for the purposes of prevention, detection, or criminal prosecutions.[202] The Directive does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use, limiting it to what is strictly necessary in light of the objective pursued.[203] By not laying down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, it does not provide for sufficient safeguards as required by Article 8 of the Charter against abuse and "any unlawful access and use of that data."[204] Finally, the Court notes that the Directive does not require the data in question to be retained within the European Union, with the result that the control of compliance by the requirements of protection and security by the data protection authorities is not fully ensured.[205]

The Advocate General noted that the Directive constitutes a "particularly serious interference with the right to privacy,"[206] as

---

Internet service used may also be retained under Article 5, § 1(d) and data necessary to identify users' communication equipment is covered under Article 5, § 1(e). *Id.* Information necessary to identify the location of mobile communication equipment is covered by Article 5, § 1(f). *Id.*

198 *Id*. art. 6.

199 *Id*. art. 7.

200 *Id*. art. 9.

201 Digital Rights Ireland Ltd., *supra* note 192.

202 *Id*. at 8.

203 *Id*. at 20 ("[The legislature] should have required a case-by-case examination of requests for access in order to limit the data provided to what is strictly necessary.").

204 *Id*. at 18–19.

205 *Id*. at 26.

206 *Id*. ¶ 67, at 12.

the retention of data in the hands of the private sector may lead to its "outsourcing" with further dangers for the right to privacy[207] in violation of even the rules of Directive 2006/24.[208] This risk is increased by the fact that the Directive does not require that data be physically stored in the EU, which creates jurisdictional difficulties that contribute to its potential to interfere with privacy.[209] This constitutes a "serious interference" with the right to privacy, which is not proportionate sensu stricto to the objective relating to the need to ensure the functioning of the internal market.[210]

The European Union legislature should have made several changes to the Directive. First, the legislature should have defined the principles that must govern the collection of data, as this is an exception from the guarantees laid down in the system of protection of privacy of the existing directives.[211] Second, "the EU should have provided a more precise description than 'serious crime' as an indication of the criminal activities which are capable of justifying access of the competent national authorities to the data collected and retained."[212] Third, the EU should have limited access to the data. This could have been accomplished by granting access "if not solely to judicial authorities, at least to independent authorities, or, failing that, by making any request for access subject to review by the judicial authorities or independent authorities . . . ." Fourth, the EU "should have required a case-by-case examination of requests for access in order to limit the data provided to what is strictly necessary."[213] Fifth, the EU should have laid down "the principle that Member States may provide for exceptions preventing access to retained data in certain exceptional

---

207 *Id.* at 13–14. In this instance, the Advocate General is alluding to the NSA collection of materials through the Internet.

208 *Id.*

209 *Id.* at 13.

210 *Id.* at 16 ("[T]he intensity of the intervention in the area of regulation of fundamental rights . . . is manifestly disproportionate to the objective relating to the need to ensure the functioning of the internal market . . . ."). The principle of proportionality in limiting freedoms is consecrated in article 52(1) of the Charter of the European Union. Charter of the Fundamental Rights of the European Union art. 52, Mar. 30, 2010, 2010 O.J. (C 83) 389, 391.

211 Digital Rights Ireland Ltd., *supra* note 192, at 19–20 (noting that the EU could and should have incorporated principles concomitant with the directive, which would have helped define the extent of the interference to privacy).

212 *Id.* at 20 (footnote omitted).

213 *Id.* (footnote omitted).

circumstances." Sixth, and last, the EU "should have established the principle that authorities authorised to access the data are required, first, to erase them once their usefulness has been exhausted" and "notify the persons concerned of that access, at least retrospectively . . . ."[214] Thus, the investigation, detection, and prosecution of serious crime, while pursuing a legitimate objective, allows for a disproportionate amount of time of retention. The Advocate General found no reason to extend the data retention period to over one year.[215]

3.3. Council of Europe and Barriers of Protection

The European Commission is requesting the U.S. to accede to the Council of Europe's Convention for the Protection of Individuals, "with regard to Automatic Processing of Personal Data . . . , as it acceded to the 2001 Convention on Cybercrime."[216] The convention states a number of principles that exist in the EU directives and the proposed regulation. According to these principles, data must be

> (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; [and] (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[217]

---

214 *Id.* The Advocate General also cites Framework Decision 2008/977 of the European Parliament, which guarantees the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and provides for guarantees of that kind in the context of data transmitted between Member States.

215 *Id.* at 23 (distinguishing 'present time' with 'historical time' and stating that data retention beyond one year would not be justified by any countervailing benefits).

216 European Commission Memo, *supra* note 13, at 8.

217 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, art. 5, Jan. 28, 1981 [hereinafter EC Treaty], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. The convention prohibits processing of special categories of data, unless domestic law provides

The convention foresees the possibility for a remedy in cases where a processor refuses to inform a person as to whether personal data has been stored, in cases of failure to communicate the data, and in cases of failure to obtain rectification or erasure of data if they have been processed contrary to the abovementioned prohibitions.[218] The treaty allows a party to prohibit, subject to authorization, the trans-border flow of certain categories of personal data under specific regulation if the other party does not provide equivalent protection.[219] A party may also prohibit the transfer of the same data through the intermediary of the territory of another party when the transfer aims to circumvent the legislation of the party prohibiting the circulation of data.[220] Presently, the NSA massive metadata collection program meets none of these requirements.

The ECtHR has issued a number of decisions concerning surveillance, some of which are more promising than others. The conditions of ordering telecommunication surveillance to intercept the content of communications in Europe are less strict than in the U.S., where a judicial order or a warrant is required.[221] In *Klass v.*

---

appropriate safeguards. Article 6 outlaws the prohibition of personal data revealing racial origin, political opinions or religious or other beliefs, data concerning health or sexual life, and data relating to criminal convictions.

218 EC Treaty, *supra* note 217, art. 8.

219 *Id.* art. 12, § 3 (a).

220 *Id.* art. 12, § 3 (b).

221 *See* 50 U.S.C. § 1805 (2006) (noting that FISA authorizes the interception of real time wire, oral, and electronic communications when the government demonstrates to the FISA Court that there is probable cause to believe that the target of the electronic surveillance is a foreign power, or agent of a foreign power, and that each of the facilities where electronic surveillance is directed or used, or is about to be used, is by a foreign power or an agent of a foreign power). A classified executive order of the former President circumvented FISA by authorizing a series of warrantless access to international telephone calls and electronic communications even when one party was a U.S. person located in the U.S. This government access developed through a public-private partnership in which the NSA was informally arranged with top officials from telecommunications companies to gain access to communications without warrants or court orders. *See* Stephanie K. Pell, *Systematic Government Access to Private-Sector Data in the United States*, 2 INT'L DATA PRIVACY L. 245, 249–50 (2012) ("Consistent with Fourth Amendment doctrine, law enforcement normally must get a warrant in order to search and seize a laptop, desktop, or thumb drive. In 1986, Congress extended the warrant protection via statute to communications content stored in an ECS (such as unopened email), but did not extend full warrant protections to communications content in RCS storage.") (footnotes omitted). In a white paper submitted to Congress, the administration founded

Germany, the Court held that the exclusion of judicial control in ordering surveillance measures "does not exceed the limits of what may be deemed necessary in a democratic society."[222] There, the initial control was affected by an official "qualified for judicial office" with oversight from a Parliamentary Board and the G-10 Commission as set up by the legislation.[223] The G-10 Commission is composed of a Chairman qualified to hold a judicial office and two independent assessors.[224] For the Court, the Parliamentary Board has a balanced membership, as government opposition is represented and thus "able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag."[225] Because the Parliament is an extension of the executive in Europe, this decision is not satisfactory. Unlike the U.S. government, where frequent elections of the two chambers of Congress allow for the coexistence of an executive with an opposite majority in either of the chambers of congress, the nature of many Parliaments of European states lends itself more easily to partisan control. The balanced membership of the Board composed by representatives of all political parties represented in the Parliament is not a sufficient guarantee, as politicians are not guaranteed to operate with objectivity and independence. Although there can be no recourse to the courts in respect to ordering and implementing restrictive measures – meaning that a warrant is not required to intercept a person's communications – the Court finds satisfactory that there are other remedies available, such as complaining to the Commission that orders and executes surveillance measures and to the Constitutional Court. [226]

---

this presidential authority through his constitutional powers under Article II of the U.S. Constitution, and through the authorization for the use of military force, which was enacted by Congress in the immediate aftermath of September 11. *See also* U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006).

222 Klass v. Germany, App. No. 5029/71 Eur. Ct. H.R. 20–21, ¶ 56 (1978) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510.

223 *Id*.

224 *Id* ¶¶ 20–21, at 7–8. The above-mentioned Board of five Members of Parliament appoints the Commission members for the current term of the Bundestag after consultation with the Government. They are "completely independent in the exercise of their functions and cannot be subject to instructions." *Id*.

225 *Id*. ¶ 56, at 20–21.

226 *Id*. ¶ 70, at 26 (reasoning that an individual does have some recourse if she believes that she is under surveillance, albeit not to the courts).

However, the Court also noted that information obtained through secret surveillance must be destroyed "as soon as they are no longer needed to achieve the required purpose."[227]

Nevertheless, there are important legal tools in the European Convention of Human Rights, and the methodology of its interpretation, which if used properly can be protective. The Court has held in a number of cases that the storage of personal data can constitute an interference with the right to respect private life under ECHR article 8(1) even if there is no evidence that the data was used to the detriment of the data subject or even at all.[228]

With regard to data withheld by surveillance authorities, the Court has held that surveillance of citizens is tolerable only if it is "strictly necessary for safeguarding the democratic institutions."[229] Domestic law concerning how public authorities file information about a citizen's private life must be defined with sufficient precision and must contain safeguards against abuses.[230] The law must be accessible and foreseeable to the person concerned. In addition, it must define the kind of information that may be recorded, the categories of people against whom surveillance measures (such as gathering and keeping information) may be taken, the circumstances in which such measures may be taken or the procedure to be followed, as well as the length of time for which the information should be kept.[231]

The Court has similarly held that the law must clearly indicate the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in the Surveillance Data base information on persons' private lives.[232] This discretion

---

[227] *Id.* ¶ 52, at 19.

[228] *See* Amann v. Switzerland, App. No. 27798/95, 2000-II Eur. Ct. H.R. 201, 238 (2000) (noting that "it is sufficient for [the Court] to find that data relating to the private life of an individual were stored by a public authority to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8, with the applicant's right to respect for his private life."). *Id.* ¶ 70.

[229] Rotaru v. Romania, App. No. 28341/95, 2000-V Eur. Ct. H.R. 61, 82 (2000), ¶ 47.

[230] *Id.*

[231] *Id.* ¶¶ 42–63 (holding that records containing information about an individual's life, studies, political activities, criminal record, constitutes an invasion of private life and thus violate article 8 of the European Convention of Human Rights).

[232] Shimovolos v. Russia, App. No. 30194/09, Eur. Ct. H.R. 16, ¶¶ 69–70 (2011), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105217.

includes information coming from wire-tapping such as the grounds for registration of a person's name in the database, the authorities competent to order such registration; the duration of the measure, the precise nature of the data collected, the procedures for storing and using the collected data, and the existing controls and guarantees against abuse.[233] The Court insists that individuals be aware of the circumstances under which surveillance may be ordered. Further, the Court maintains that there be sufficient guarantees against arbitrary interference in order for individuals to be able to obtain a remedy either at the national level or before the Convention institutions.[234] "The Court has also accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him."[235]

In *Amann v. Switzerland*, the court made clear that the national security limitations to the right to privacy, apart from being foreseen in a law, must be necessary in a democratic society to achieve the aim of national security.[236] The legal basis must be accessible and foreseeable.[237] In *Amann*, the Swiss government had ordered surveillance measures against a citizen for law enforcement purposes. The ECtHR found that Article 1 of the Federal Council's Decree, that foresaw the possibility of conducting surveillance on behalf of the federal police in the interests of the Confederation's internal and external security, contained no indication "as to the persons concerned by such measures, the circumstances in which they may be ordered, the means to be employed or the procedures to be observed."[238] Even

---

233 *Id*.

234 *Id*. ¶ 68, at 15–16.

235 Association "21 Decembre 1989" v. Romania, App. No. 33810/07, Eur. Ct. H.R. 27–28, ¶ 114 (2011), http://hudoc.echr.coe.int.

236 Amann v. Switzerland, 2000-II Eur. Ct. H.R. 201, ¶ 71, at 20 ("Such interference breaches Article 8 unless it is 'in accordance with the law', pursues one or more of the legitimate aims referred to in paragraph 2 and, in addition, is 'necessary in a democratic society' to achieve those aims.").

237 *Id*. ¶ 55, at 16 ("[T]he phrase 'in accordance with the law' implies conditions which go beyond the existence of a legal basis in domestic law and requires that the legal basis be 'accessible' and 'foreseeable.'").

238 *Id*. ¶ 58, at 17 (holding that the legal basis did not meet the foreseeability requirement because it did not contain any appropriate indication as to the scope and conditions of exercise of the power conferred on the Public Prosecutor's

if public authorities have a discretionary power in this area, a law must "indicate with sufficient clarity the scope and conditions" of the exercise of this power, in order to not violate the right to privacy.[239] It is doubtful whether U.S. legislation allowing the confiscation of any "tangible thing" leading to the mass collection of data meets the foreseeability requirement of the law according to the criteria of the ECtHR.

The ECtHR has also held that the collection and storage of personal information relating to telephony metadata – that is, the numbers dialed as well as the date and length of telephone conversations – and e-mail and Internet usage without a person's knowledge, amounts to an interference with the right to respect for that person's private life.[240] After thus collecting the different elements from different rulings on the topic, there can be some

---

Office to gather, record and store information. Furthermore, they did not specify the conditions in which cards may be created, the procedures that have to be followed, the information which may be stored, or the comments which might be forbidden).

[239] *See, e.g.*, *id.* ¶ 62, at 18 (holding that the interference with the applicant's private life through intercepting his communications was not in accordance with the law, "since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration"); *see also id.* ¶ 80 ("[T]he creation of the impugned card by the Public Prosecutor's Office and the storing of it in the Confederation's card index amounted to interference with the applicant's private life . . . ."). *Cf.* E.B. v. Austria, App. Nos. 31913/07, 38357/07, 48098/07, 48777/07, 48779/07, Eur. Ct. H.R., ¶ 75 (2014), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"appno":["31913/07"],"itemid":["001-127814"]} ("[T]he storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8, and that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention") (citing Gardel v. France, App. No. 16428/05, 2009-V Eur. Ct. H.R. 383, 402-07 (2009) (holding that, even though based on a judgment by a court that was delivered to the public, the sensitive nature of the information contained in a criminal record and the impact it may have on the individual concerned relates to that person's private life and amounts to interference).

[240] *See* Copland v. United Kingdom, App. No. 62617/00, 2007-I Eur. Ct. H.R. 317, 329, ¶ 43 (2007) (noting that even nominal data, such as the date and length of a phone call and the phone numbers dialed, may be protected by the right to privacy because they constitute an "'integral element of the communications made by telephone' . . . [and that t]he mere fact that these data may have been legitimately obtained" by a third party "in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8.") (citations omitted); *see also id.* ¶ 48, at 330 (holding that that there was no legal basis regulating monitoring of an employee's telephone, email, or Internet usage at the place of work).

optimism that the Court would apply the principle of proportionality in a way as to limit data collection from surveillance authorities. The Court has already fast-tracked a case brought by privacy and human rights advocates against Britain ordering Ministers to justify Government Communication Headquarters' mass surveillance programs.[241] An applicant before the ECtHR does not need to be a national of one of the member states, a policy that is in line with the Court's role as promulgating human rights in general.

3.4. Cloud Computing and the Safe Harbor

When the FISA Amendments Act was introduced in July 2008, it introduced "remote computing services," widening the scope to include cloud computing.[242] Cloud computing can be defined as the distributed processing of data on remotely located computers accessed through the Internet.[243] Since information stored in the cloud is stored in a physical machine owned by a company or person in a specific country, it may be subject to the laws of the country where the physical machine is located.[244] As it may be difficult though for an individual data subject to determine the location of data storage in the online context,[245] cloud providers are

---

241 Nick Hopkins, *Justify GCHQ Mass Surveillance, European Court Tells Ministers*, THE GUARDIAN (Jan. 23, 2014), http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights?CMP=ema_follow ("[T]he court in Strasbourg has told the government to provide submissions by the beginning of May about whether GCHQ's spying activities could be a violation of the right to privacy under article 8 of the European convention.").

242 The government can compel third party providers to disclose communications content in RCS storage with an 18 U.S.C. § 27803(c) order. For further discussion of Remote Computing Services under the Electronic Communications Privacy Act, see Pell, *supra* note 221, at 249.

243 *See generally* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 121 (2013).

244 Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM (Feb. 23, 2009), at 7 (noting that the physical location of information in the cloud may determine the legal rules that apply); *see also* KUNER, supra note 243.

245 The difficulties may arise due to the reluctance of the data controller to disclose such information based on concerns about data security, the fact that the controller has poor informational policies, and the number of parties involved in the processing, which complicates a determination about who is processing

considered transnational companies subject to conflicts of public international law. As a Note by Policy Department C of the European Parliament explains, "[w]hich law they choose to obey will be governed by the penalties applicable and exigencies of the situation, and in practice the predominant allegiances of the company management."[246] As a cloud is made up of shared systems and infrastructures, cloud providers process personal data emanating from a wide range of sources in terms of data subjects and organizations, allowing for the possibility that conflicting interests might arise. Moreover, the outsourcing of concrete services and chain processing involving multiple processors and subcontractors may complicate matters even further.[247] The cloud client is rarely able to know where the data are located or stored or transferred as they can move around all over the world.[248]

Cloud providers cannot fulfill any of the privacy principles on which Safe Harbor is founded as this was not resolved satisfactorily by the Commission: although U.S. cloud providers advertise Safe Harbor certifications, the Article 29 Data Protection Working Party has clarified that existing protection is not enough.[249] Cloud clients are also exposed to the dangers of sub-processing by third parties since cloud providers usually do not offer them such information.[250] Further:

---

particular data at a particular time. It can also be unclear which location should control the applicable law and jurisdiction – the location of the business establishment of the data controller, or the location of the data. *See id*. at 122.

246 Bowden, *supra* note 20, at 22 (citation omitted).

247 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, EUR. COMM'N (July 1, 2012), at 5 [hereinafter Article 29 Working Party Opinion 5/2012], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (indicating the potential absence of client control when data is handled by a cloud provider and outlining the risks associated with that absence of control). *See* Article 29 Working Party Opinion 4/2000, *supra* note 77.

248 Article 29 Working Party Opinion 5/2012, *supra* note 247, at 17 ("The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred.").

249 *Id.* ("[S]elf-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles"); *see also* Bowden *supra* note 20, at 22 ("[T]he EU is not addressing properly an irrevocable loss of data sovereignty, and allowing errors made during the Safe Harbor negotiations of 2000 to be consolidated, not corrected.") (citation omitted).

250 Article 29 Working Party Opinion 5/2012, *supra* note 247, at 17–18 (suggesting that national legislation should require that the terms regarding sub-processors, including their location and other data, be identified in the contract between the cloud client and the cloud provider).

> Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC . . . . In terms of data security, cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security.[251]

The existing EU directive and the proposed Regulation outline their territorial scope as covering "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether the processing takes place in the Union or not."[252] The proposed regulation defines its territorial scope as applying to non-EU companies that provide services through the cloud, as it applies to "the processing of personal data of [EU] data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behavior."[253] Moreover, the proposed privacy law is overbroad. The proposed regulation associates monitoring the behavior of data subjects with the processing techniques of profiling. However, there are many innocuous activities that require the monitoring of data. For instance, many cloud services track an individual's data merely to

---

[251] *Id.* at 18. Standard contractual clauses or binding corporate rules can also be mediums of assuring protection on cross border data transfers. The Article 29 Working Party has underlined the need to make sure that processors who sub-contract services out to sub-processors make this information available to the client. This can be accomplished by detailing the type of service subcontracted, by describing the characteristics of the current or potential sub-contractor, and by setting out the obligations and responsibilities required by data protection legislation in order to ensure effective control over and allocate clear responsibility for processing activities. *Id.* at 9.

[252] LIBE Committee Vote, *supra* note 162, at 6 (backing reform after an overwhelming EU vote in favor of the proposals).

[253] *Id.*; Proposed Regulation, *supra* note 3, at 41 (adopting the proposal including Article 3, § 2).

provide the individual with additional storage capacity. Because the regulation fails to distinguish between these activities from real profiling, it will prevent consumers from realizing many benefits of networked intelligence.[254] This is another reason the existing Safe Harbor agreement is insufficient.[255]

A Working Party Opinion underlines the importance of adding an additional restriction to the proposed regulation. Controllers operating in the EU "must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority."[256] A comprehensive international treaty is necessary to guarantee full reciprocity of rights and to grant EU citizens equal protection to U.S. citizens in U.S. courts.[257] The European Parliament should consider amending the Data Protection Regulation to require prominent warnings to individual data subjects of vulnerability to political surveillance before EU Cloud data is exported to U.S. jurisdiction.[258] European companies are using cloud-computing services in the U.S. for the purposes of data storage. The company offering the storage must subscribe to the Safe Harbor Principles that are alternatives to a specific contractual arrangement between the two companies regarding the treatment of personal data

---

254 *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1644 (2013) (noting that equating monitoring with profiling creates impediments to the legitimate use of networked intelligence). Likewise, the EU's broad interpretation of 'automated processing' creates concern that the regulation would threaten "socially productive uses of analytics." *Id.* at 1647. At the same time, it can operate protectively against state surveillance by limiting the amount of information that private actors can withhold.

255 *Id.*

256 Article 29 Working Party Opinion 05/2012, *supra* note 247, at 23 ("[I]t is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority."). The opinion went on to state that Regulation (EC) NO 2271/96 demonstrates an example of legal ground for this proposition. The working party further stresses the need for the Regulation to include the obligatory use of Mutual Legal Assistance Treaties in case of disclosures not authorized by Union or Member States law.

257 Bowden, *supra* note 20, at 22 ("The primary desideratum would be a comprehensive international treaty guaranteeing full reciprocity of rights . . . .").

258 *Id.*

transferred to the U.S.[259] Since the protection offered by the Safe Harbor is not sufficient in reference to the national security exception and unless the U.S. adheres to the Council of Europe Convention 108, a special treaty is required which will extend the protection that U.S. nationals enjoy to non-nationals.

Furthermore, the existing Directive and the Proposed Regulation impose limitations on contractual freedom that conflict with the U.S. Terms of Service or take-it-or-leave-it contracts for cloud computing. EU law limits contracting out of the protection afforded by it, whereas the standardized offers of many cloud-computing services may impose contracting out of privacy protection.[260] In the U.S., some state laws regulate cloud computing by imposing obligations concerning data security, data breach security notification, and data disposal.[261] These differences and the insufficiency of the Safe Harbor principles necessitate an ad-hoc convention with the aim of elaborating model contractual clauses concerning the guarantees of the use of information stored in the cloud, which can also indirectly limit the amount of data that ends in the hands of public authorities for intelligence purposes.[262]

A Working Party Opinion has elaborated requirements for the minimum content of contractual safeguards of the "controller—processor" relationships. Among those are the specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the

---

[259] *E.g.*, Orange France is using the cloud computing services of Amazon U.S. for data storage, which means that Amazon must subscribe to the Safe Harbor Principles. A global company such as Mastercard – based in the U.S. and having a large number of clients in the EU – obtains the flexibility it needs for operations by subscribing to the Safe Harbor Principles while, at the same time, permitting the free flow of data outside of the EU, subject to the respect of the Safe Harbor Principles. *See* European Commission Memo, *supra* note 13, at 5.

[260] *See* Article 29 Working Party Opinion 05/2012, *supra* note 247, at 8 (discussing the imbalance of negotiating power with respect to contract terms between the large service providers and the relatively small controller).

[261] Schwartz, *supra* note 254, at 1659–60 (contrasting the broad 'regulatory thicket' approach to data privacy in the EU with the U.S. approach, which has relied more on contractual agreements and state-by-state regulation). California, for example, has created a requirement of reasonable security when personal data are processed. Applicable federal statutes in the healthcare and financial service sectors provide more specific rules regarding the safeguards that must be in place when personal information is processed, including when it is processed in the cloud. *Id*. at 1660.

[262] *Cf.* Schwartz, *supra* note 254, at 1659 (proposing that developing model contractual clauses for cloud-client relationships would help the EU streamline the regulatory process).

nature of the data, the subject and time frame of the cloud service, the extent, manner, and purpose of the processing, and the specification of the conditions for returning the data or destroying them once the service is concluded.[263] Additional elements should include confidentiality clauses or an express statement that the cloud provider may not communicate the data to third parties, unless they are subcontractors.[264] The cloud provider is obligated to provide a list of locations where the data may be processed and to notify the cloud client about any legally binding request for disclosure of the personal data by law enforcement unless otherwise prohibited. There is also a general obligation to give assurance that its internal organization and data processing arrangements are compliant with the applicable national and international legal requirements and standards.[265]

3.5. Does the Collection Meet the Requirements of the ICCPR?

The International Covenant on Civil and Political Rights protects privacy in Article 17. [266] According to the recommendations of the special rapporteur, limitations to the right

---

[263] *See generally* Article 29 Working Party Opinion 5/2012, *supra* note 247.

[264] *Id*. at 13.

[265] *Id*. at 13–14. They must also inform clients about all subcontractors contributing to the provision of the respective cloud service and all locations in which data may be processed by the cloud provider and/or its subcontractors. *Id*. at 20. The Committee of Experts Commissioned by the U.S. President to issue proposals for a better protection recommends regarding encryption as a measure to increase security and user confidence. The Committee also advises that the U.S. government should fully support and not undermine efforts to create encryption standards, and not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software. The Committee urges the U.S. government and U.S. companies to increase the use of encryption, in order to better protect data in transit, at rest, in the cloud, and in other storage. LIBERTY REPORT, *supra* note 93, at 216. The U.S. government thus should make it clear that the NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce, that it will not demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA's clandestine collection of information by users of the product, and that it will not hold encrypted communication as a way to avoid retention limits. The United States should not provide competitive advantage to U.S. firms by the provision to those corporations of industrial espionage, and similarly it should commit to international norms on the issue.

[266] *See generally* International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, 6 I.L.M. 368 (1967), S. Treaty Doc. No. 95-20, art. 17.

to privacy should pass the "permissible limitations test" foreseen in Articles 21 and 22 of the same Covenant for the limitation of freedom of assembly and freedom of association.[267] According to this test, "(a) restrictions must be prescribed by national law; (b) they must be necessary in a democratic society; and (c) they must serve one of the legitimate aims enumerated in each of the provisions that contain a limitations clause."[268] The Human Rights Committee has also set a permissible limitations test for the right to privacy.[269] These requirements mean that the essence of a human right is not subject to restrictions, any restrictions must be necessary for reaching the legitimate aim, and they must conform to the principle of proportionality.[270] States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds.[271] Put differently, "[t]here must be some factual basis, related to the behavior of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack."[272] The principle of proportionality does not seem to be met by the massive collection of data by the U.S. authorities for a number of reasons.

First, there is no explicit obligation to minimize impact on non-U.S. persons outside the U.S.[273] According to a FISC opinion, measures previously proposed by the government to comply with this requirement have been found to be unsatisfactory in relation to "upstream" collection and processing.[274] New measures were only found to be satisfactory for the protection of U.S. persons.[275]

---

267 Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, at 8, Human Rights Council, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (by Martin Scheinin) [hereinafter Special Rapporteur on Human Rights].

268 *Id.*

269 Human Rights Committee, *General Comment No.* 27: Freedom of Movement (Article 12), U.N. GAOR, 67th Sess., 1783rd mtg. at 4, U.N. Doc CCPR/C/21/Rev.1/Add.9 (Nov. 1, 1999).

270 *Id.*

271 Special Rapporteur on Human Rights, *supra* note 267, at 9.

272 *Id.*

273 50 U.S.C. § 1801(h) (1978) (foreseeing minimization procedures for U.S. persons only).

274 FISC Oct. 3, 2011 Opinion, *supra* note 129, at 49.

275 *Id.* at 65.

Furthermore, the FISC review does not include review of potential measures to protect the personal information of non-U.S. persons outside the U.S.[276] "'[U]nreviewed data[,]' collected under Section 702, is generally retained for five years, although data collected via upstream collection is retained for two years."[277] The U.S. stated that in fifty-four instances, collection under Sections 702 and 215 contributed to the prevention and combating of terrorism; twenty-five of those instances involved EU Member States.[278]

Furthermore, the technical impossibility to distinguish the relevant communications from the non-relevant in many of the NSA programs justifies the massive collection of data that does not serve national security purposes. As the FISA Court noted in multi-communication transactions ("MCTs"), "NSA acquires not only the discrete communication that references the tasked selector, but also in many cases the contents of other discrete communications that do not reference the tasked selector and to which no target is a party."[279] The sole reason these non-target communications are collected is because they contain "'a tasked selector used by a person who has been subjected to NSA's targeting procedures.'"[280] Moreover, upon acquisition, "NSA's upstream collection devices often lack the capability to determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction."[281]

The Court found that the upstream collection acquires tens of thousands of discrete communications of non-target United States persons and persons in the United States, protected by the Fourth Amendment, "by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream

---

276 AD HOC EU-U.S. WORKING GROUP REPORT, *supra* note 138, at 11.

277 *Id*. These retention periods apply to all unreviewed data, including both U.S. and non-U.S. person information.

278 The U.S. was unable to provide figures regarding Executive Order 12333. The U.S. confirmed that out of the total of fifty-four cases, forty-two cases concerned plots that were foiled or disrupted, and twelve cases concerned material support for terrorism cases. *Id*. at 12.

279 FISC Oct. 3, 2011 Opinion, *supra* note 129, at 42–43. "By acquiring such MCTs, NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector." *Id.* at 43.

280 *Id*.

281 *Id*.

collection devices."[282] This means that communications were collected concerning persons who are non-targets, located inside the U.S. and for whom there is no reason to believe that all of their discrete communication will be to, from, or about the targeted selector. Additionally, if the person is in the U.S., the Court presumes that the majority of that person's communication will be with other persons in the U.S., many of whom will be U.S. persons.[283] NSA acquires at least 1.3 million MCTs each year of non-targets located outside the United States whose communications will presumably be mostly with persons outside the U.S., most of whom are non-U.S. persons.[284] It also acquires 97,000–140,000 MCTs each year concerning persons whose identity or location cannot be identified.[285] This unknown category adds substantially to the number of non-target communications of or concerning United States persons or that are to or from persons in the United States being acquired by NSA each year.[286] For the same Court, "NSA's collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that . . . do not serve the national security needs underlying the Section 702 collection . . . ."[287] The U.S. President committed to applying restrictions on the use of information incidentally collected from communications between foreign citizens and U.S. citizens under Section 702.[288]

In addition, there are doubts as to whether the telephony metadata program provides information that cannot be provided through more conventional investigative techniques. A Federal

---

282 *Id.* at 37.

283 *Id.* at 38.

284 FISC Oct. 3, 2011 Opinion, *supra* note 129, at 39–40 (discussing that "even if only 1% of these MCTs contain a single non-target communication of or concerning a United States person, or that is to or from a person in the United States, NSA would be acquiring in excess of 10,000 additional discrete communications each year that are of or concerning United States persons, or that are to or from a person in the United States.").

285 *Id.* at 40.

286 *Id.* at 41.

287 *Id.* at 78.

288 Barack Obama, President of the United States, Speech on NSA Reform (Jan. 17, 2014) (transcript available at *Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, WASH. POST (Jan. 17, 2014) [hereinafter Obama Speech], http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

district court examining a preliminary injunction found that there is significant likelihood that the program constitutes an "unreasonable search" under the Fourth Amendment of the U.S. Constitution, as the Government did not "cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature."[289]

---

[289] Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C. 2013). For the court, none of the three episodes cited by the government that supposedly illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack involved any apparent urgency. In the first case, the metadata did not reveal any new information that had not already come to light in the investigation up to that point; in the second, the metadata analysis was used only after the terrorist was arrested "to establish [his] foreign ties and put them in context with his U.S. based planning efforts[;]" in the third, the metadata analysis "revealed a previously unknown number for [a] co-conspirator. . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists." *Id.* (internal quotations omitted). The court cites Assistant Director Holley of the FBI who concedes that bulk metadata analysis only "*sometimes* provides information earlier than the FBI's other investigative methods and techniques." *Id.* (internal quotations omitted); *contra* ACLU v. Clapper, 959 F. Supp. 2d 724, 727 (S.D.N.Y. 2013) (holding that relevance to an authorized investigation under section 215 is to be defined broadly as concerning tangible items which "bear on or could reasonably lead to other matter that could bear on the investigation."). For the court, since "there is no way for the Government to know which particle of telephony metadata will lead to useful counterterrorism information[,] . . . courts routinely authorize large-scale collections of information, even if most of it will not directly bear on the investigation." *Id.* at 747. For the court, "aggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. And NSA's warehousing of that data allows a query to be instantaneous." *Id.* at 748 (citing Smith v. Maryland, 442 U.S. 735 (1979), as controlling precedent which held that an individual has no legitimate expectation of privacy in information provided to third parties; the judge held that the program is legal). First, according to the judge, NSA needs to collect bulk telephony metadata to be able to query the telephony metadata database. "Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three 'hops' of the 'seed.' Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to. . . . [It only sees] that telephone number A called telephone number B." *Id.* at 750–51. For the judge, "the Government's subsequent querying of the telephony metadata does not implicate the Fourth Amendment – any more than a law enforcement officer's query of the FBI's fingerprint or DNA databases to identify someone." *Id.* at 751 (citing Maryland v. King, 133 S. Ct. 1958, 1963–64 (2013)). For the court, "there is no evidence that the Government has used any of the bulk telephony metadata it collected for any purpose other than investigating and disrupting terrorist attacks. While there have been unintentional violations of guidelines, those appear to stem from human error and the incredibly complex computer programs that support this vital tool. And once detected, those violations were self-reported and stopped." *Id.* at 757. In a recent report of the New America Foundation on the effectiveness of the NSA Bulk Surveillance

Similarly, the Committee of Experts commissioned by the President found that the information contributed to terrorist investigations by the use of Section 215 telephony metadata was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional Section 215 orders.[290] The Committee expressed caution as to whether the program is "efficacious in alleviating concern about possible terrorist connections, given the fact that the meta-data captured by the program covers only a portion of the records of only a few telephone service providers."[291] The Committee noted also that the bulk telephony metadata collection program has experienced several significant compliance issues, as the FISC found that for two and a half years the NSA had searched all incoming phone metadata using an "alert list" of phone numbers of possible terrorists that had been created for other purposes, as almost 90 percent of the numbers on the alert list did not meet the "reasonable, articulable, suspicion" standard.[292] The FISC concluded that the minimization procedures had been "'so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively'" due to misunderstandings on the part of analysts about the precise rules governing their use of the metadata.[293]

Programs, this opinion was criticized as exhibiting substantial deference to the government's broad claims regarding its use of bulk collection under Section 215 and little examination of the particular cases beyond the government's statements. *See* Peter Bergen et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AM. FOUND. (Jan. 2014), *available at* http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists (noting that the role of the NSA in the cases of individuals charged with some kind of terrorism crime was "limited and insufficient to generate evidence of criminal wrongdoing without the use of traditional investigative tools."). The Report concludes that "the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques." *Id.* at 3.

290 LIBERTY REPORT, *supra* note 93, at 104.

291 *Id.* The section 215 telephony metadata program has made only a modest contribution to the nation's security having generated relevant information in only a small number of cases, while there has been no instance in which NSA could say with confidence that the outcome would have been different without the section 215 telephony metadata program.

292 *In re* Production of Tangible Things from [redacted], No. BR 08-13 (FISC Mar. 2, 2009).

293 *Id.* at 105.

According to the findings of the District Court for the District of Columbia[294] and the Committee, the program does not seem to meet the standards of the ICCPR.[295]

The Committee stresses that the government must end the storage of bulk telephony under Section 215 and that it must transition to a system in which the metadata are held either by private providers or by a private third party. These private data holders should only allow access to their archives only when the FISC authorizes a Section 215 order that meets the requirements described above. The court should require reasonable grounds to believe that the information sought is relevant to an authorized investigation protecting "'against international terrorism or clandestine intelligence activities'" and ensure "the order is reasonable in focus, scope and breadth."[296] This approach is similar to the one followed by the EU in its data retention directive.[297] Legislation might require relevant telephone providers to retain the data for a specified period of time, though no longer than two years, to ensure that it will be available if and when the government needs to query it.[298]

---

294 *See generally* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); LIBERTY REPORT, *supra* note 93, at 105 (quoting FISC Judge Reggie Walton in his opinion from Klayman v. Obama).

295 The same committee recommended that the statutes that authorize the issuance of National Security Letters be amended to permit their issuance only upon a showing that: "(1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect 'against international terrorism or clandestine intelligence activities' and (2) like a subpoena, the order is reasonable in focus, scope and breadth." LIBERTY REPORT, *supra* note 93, at 24. The committee also recommends "that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders." *Id.* at 25. NSLs should not be issued by the FBI itself, but by a court, which would mean "a significant expansion in the number of FISC judges, the creation within the FISC of several federal magistrate judges to handle NSL requests, and use of the Classified Information Procedures Act to enable other federal courts to issue NSLs." LIBERTY REPORT, *supra* note 93, at 93 (internal citation omitted).

296 LIBERTY REPORT, *supra* note 93, at 24. In a line of thinking where private actors are more trusted by the government, the Committee notes that "the government can query the information directly from the relevant service providers after obtaining an order from the FISC," as originally envisioned when section 215 was enacted, a change that would greatly reduce the intake of telephony metadata by NSA and would reduce the risk of government abuse. *Id.* at 118.

297 *See supra* Part 3.2.

298 In that case, the government should reimburse the providers for the cost

The President did not accept this proposal, and determined that for reasons of accountability, it would be preferable for the federal government to collect this data.[299] The President committed to modifying the program in querying phone calls only two steps (or "hops") removed from a telephone number linked to a terrorist network, instead of the current three steps removed standard.[300] He also committed to querying the database only after "a judicial finding or in case of a true emergency."[301] The reason put forward for the mass collection of telephone metadata is to protect the information that might be useful at some point. The difficulties in querying the material collected raise concerns as to whether this insurance-style purpose meets the standard of proportionality. If according to the recent reports, the material provides only small parts of information, which also can be obtained by the use of conventional investigative techniques, and thanks to a better cooperation between the CIA and the FBI,[302] then the principle of proportionality does not appear to be met.

In general, there are doubts as to whether governments, unlike

---

of retaining the data. An FCC regulation already requires providers to hold such information for 18 months, so it seems feasible to change the retention period for telephone records. *See* LIBERTY REPORT, *supra* note 93, at 119; *see also* 47 C.F.R. § 42.6 (1986) (laying out rules for the retention of telephone toll records: "Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.").

299 *See* Obama Speech, *supra* note 288 (noting "any third party maintaining a single, consolidated database would be carrying out what is essentially a government function but with more expense, more legal ambiguity, potentially less accountability – all of which would have a doubtful impact on increasing public confidence that their privacy is being protected."); *see also* Senator Dianne Feinstein, Remarks at a Hearing on President's Review Group on Intelligence and Communications Technologies Before the Judiciary Committee (Jan. 14, 2014), (transcript available at http://www.judiciary.senate.gov/imo/media/doc/01-14-14FeinsteinStatement.pdf) (highlighting Senator Feinstein's belief that, in the interest of timeliness, the state must be able to query the data at any time).

300 *See* Obama Speech, *supra* note 288.

301 *Id.*

302 *See* Bergen, *supra* note 289, at 7 (calling attention to "'serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.'") (quoting U.S. District Judge Richard Leon in his opinion from Klayman v. Obama); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

marketers, are able to conduct data mining in a way that might be useful in actually serving the purpose of identifying terrorists.[303] Data mining "occurs without legal guarantees for the accuracy or appropriateness of the data or the searches, redress for people injured by being falsely identified as posing a threat, or judicial or legislative oversight."[304] The President addressed neither the issue of massive data collection nor the NSA's attempts to weaken encryption technologies.

In May 2014, the House Permanent Select Committee on Intelligence approved a compromise bill on NSA reforms that was unanimously approved by the House Judiciary Committee.[305] The bill was passed in the House of Representatives on May 22, 2014.[306] It was, however, defeated in the Senate on November 18, 2014.[307] The bill would ban the bulk collection of all types of records, not just the Section 215 phone metadata program. It would prohibit other types of bulk collection by requiring that any records obtained be linked to a specific person, account, or entity.[308] The bulk records would stay in the hands of phone companies, which would not be required to retain them for any longer than they normally would.[309] The government would be able to obtain

---

303 Levinson-Waldman, *supra* note 31, at 3 (noting that although marketers can use data mining to predict purchasing practices of customers, researchers have demonstrated persuasively that it is impossible and unlikely ever to become possible, to predict whether a person will take part in a terrorist act*); see also* Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, POL'Y ANALYSIS (Dec. 11, 2006), at 3 (arguing "the possible benefits of predictive data mining for finding planning or preparation for terrorism are minimal. The financial costs, wasted effort, and threats to privacy and civil liberties are potentially vast. Those costs outstrip any conceivable benefits of using predictive data mining for this purpose.").

304 Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 436 (2008).

305 *House Intelligence Committee Approves NSA Reforms*, BRENNAN CTR. FOR JUSTICE (May 8, 2014) [hereinafter Brennan Center for Justice Report], *available at* http://www.brennancenter.org/press-release/house-intelligence-committee-approves-nsa-reforms.

306 Jonathan Weisman & Charlie Savage, *House Passes Restraints on Bulk Data Collection*, N.Y. TIMES (May 22, 2014), http://www.nytimes.com/2014/05/23/us/politics/house-votes-to-limit-nsas-collection-of-phone-data.html?_r=0.

307 Charlie Savage & Jeremy W. Peters, *Bill to Restrict N.S.A. Collection Blocked in Vote by Senate Republicans*, N.Y. TIMES (Nov. 18, 2014), *available at* http://www.nytimes.com/2014/11/19/us/nsa-phone-records.html.

308 *See* Brennan Center for Justice Report, *supra* note 305.

309 Charlie Savage, *Obama to Call for End to N.S.A.'s Bulk Data Collection*, N.Y.

access to the records through a FISA court order to individuals' phone records up to two "hops."[310] The bill would not end searches in which the government collects the content of phone and email communications of foreigners overseas without a warrant, and then searches them for communications to, from, or about Americans.[311] The compromise bill omitted key transparency provisions, including government reporting requirements and a provision for a special advocate to argue the other side in significant cases before the secret FISA Court.[312]

CONCLUSION

As the Committee of Experts commissioned by the President notes, there are special historical reasons for which FISA protects U.S. persons more strictly. The bill's authors were particularly concerned by the fact that at the time the law was enacted U.S. citizens were the object of government surveillance in the U.S.[313] The Committee cites a number of pragmatic reasons in support of the need to increase protection for non-U.S. persons, among which are the duty of reciprocity requiring that the U.S. treat other citizens well if it wants its own citizens to be treated well by other governments.[314] Second, aggressive surveillance policies under Section 702 might trigger economic repercussions for American businesses, potentially causing them to lose market shares due to growing distrust of their capacity to guarantee the privacy of their international users.[315] Unrestrained American surveillance of non-

---

TIMES (Mar. 24, 2014), *available at* http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?_r=0.

310 *See* Brennan Center for Justice Report, *supra* note 305.

311 *Id*.; s*ee also* The Editorial Board, *A Stronger Bill to Limit Surveillance*, N.Y. TIMES (July 27, 2014), *available at* http://www.nytimes.com/2014/07/28/opinion/a-stronger-bill-to-limit-surveillance.html.

312 Brennan Center for Justice Report, *supra* note 305.

313 LIBERTY REPORT, *supra* note 93, at 154.

314 *Id*. at 155.

315 *Id.* at 155 (U.S. researchers estimate that as consequence of mistrust caused by NSA program, $180 billion or 25% of U.S. overseas information technology services risk to be lost by 2016); *see also* Allan Holmes, *NSA Spying*

United States persons might alienate other nations, fracture the unity of the Internet, and undermine the free flow of information across national boundaries.

The EU, on the other hand, insists on the need to use the formal channels negotiated between itself and the U.S., such as the Mutual Legal Assistance agreement, in order to augment the exchange of data for the prevention and investigation of criminal activities.[316] A U.S.-EU Mutual Legal Assistance agreement has been in place since 2003, which facilitates and accelerates assistance in criminal matters between the EU and the U.S., including through the exchange of personal information.[317]

The EU and the U.S. are currently negotiating a new framework agreement on data protection in the field of police and judicial cooperation.[318] The EU authorities aim to ensure a high level of data protection, in line with the EU data protection acquis for citizens whose data is transferred across the Atlantic, thus strengthening EU-U.S. cooperation in the fight against crime and terrorism.[319] Under U.S. law, Europeans who are not U.S. residents do not benefit from the safeguards of the 1974 U.S. Privacy Act, which limits judicial redress to U.S. citizens and legal permanent residents. The Commission is requesting that EU citizens who are not U.S. residents must be given enforceable rights, notably the

---

Seen Risking Billions in U.S. Technology Sales, BLOOMBERG (Sept. 10, 2013, 11:33 AM), *available at*

http://www.bloomberg.com/news/2013-09-10/nsa-spying-seen-risking-billions-in-u-s-technology-sales.html (finding that after a report surfaced that the NSA built "backdoors" in technology security products sold overseas, U.S. technology companies could see overseas sales drop by as much as $180 billion).

316 *See* Letter of Viviane Reding, Vice President, Eur. Comm'n, to Eric H. Holder, Jr., Att'y Gen. of the U.S. Dep't of Justice (June 10, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf (pointing out to Attorney General Holder that the Mutual Legal Assistance Agreement "should be used to the greatest possible extent").

317 Agreement on Mutual Legal Assistance Between the European Union and the United States of America, 2003 O.J. (L 181) 34, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:en:PDF.

318 *Communication on the Functioning of the Safe Harbour*, *supra* note 55, at 8.

319 *See* Memorandum from the Eur. Comm'n, Joint Press Statement Following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington (Nov. 18, 2013) (during which the EU and the U.S. committed to complete the negotiations on the agreement ahead of summer 2014).

right to judicial redress, and there seems to be willingness to converge on this issue.[320] The Commission also aims to narrowly define the derogation based on national security. This "umbrella agreement" on the general framework needed to ensure a high level of protection of personal data when transferred to the U.S. for the purpose of preventing or combating crime and terrorism, will not provide the legal basis for any specific transfers of personal data between the EU and the U.S. A specific legal basis for such data transfers would always be required, such as a data transfer agreement or a national law of an EU member state.

In parallel, there exists a special international agreement dictating how data on passenger names collected by air carriers would be shared and managed between the EU countries and the U.S.[321] Another special agreement between the EU and the United States was concluded in order to secure adequate data protection in SWIFT transaction.[322] The U.S. Treasury Department may

---

[320] The negotiations aim also to limit how and for what purposes the data can be transferred and processed, as well as the conditions for and the duration of the retention of the data. *How Will the EU's Data Protection Reform Simplify the Existing Rules?*, EUR. COMM'N, *available at* http://ec.europa.eu /justice/data-protection/document/review2012/factsheets/6_en.pdf.

[321] *Compare* Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR agreement), July 26, 2007, *available at* https://www.dhs.gov/sites/default/files/publications/privacy/pnr-2007agreement-usversion.pdf (binding the EU to ensure that air carriers operating passenger flights to and from the USA will make available to the Department of Homeland Security passenger data), *with* Council Decision 2012/472/EU, of 26 April 2012 on the Conclusion of the Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 2012 O.J. (L 215) 4. The period during which PNR data may be stored and used is reduced from fifteen to ten years for transnational serious crimes. PNR data is stored for fifteen years for terrorism, and all data should be anonymized after six months. The agreement shall remain in force until 2019.

[322] Council Decision 2010/412/EU, on the Conclusion of the Agreement Between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 195) 3 (discussing the conclusion of the agreement between the EU and the U.S. on the processing and transfer of Financial Messaging Data from the EU to the U.S. for the purposes of the Terrorist Finance Tracking Program). The Society for Worldwide Interbank Financial Telecommunications is based in Belgium and is the processor for most of the global money transfers from European Banks. The SWIFT Agreement is valid for five years, until August 2015. *Id*. art. 3.

request financial data from SWIFT only under narrowly defined circumstances. [323] These concrete agreements present the advantage of defining narrowly the circumstances of retention and use of data allowing awareness of the persons concerned.

A necessary accommodation to the realities of modern life, which means that individuals have to reveal personal information to third parties, does not mean that they are willing to give up their privacy entirely. In a world of complex technology, it is unclear whether the distinction between "meta-data" and other information carries much weight. [324] As Justice Sotomayor observed about GPS monitoring of locational information in the *Jones* case, data on telephone calls can reveal "a wealth of detail" about an individual's "familial, political, professional, religious, and sexual associations."[325] Defining privacy as a right to control who has access to a person means recognizing that the person is entitled to consent to any use of the information that concerns her. This is in accordance with a vision of privacy as deriving from the general concept of human dignity, which means that human beings are entitled to respect by the very fact that they are human beings. The need to narrowly define the circumstances of violation of data privacy is quintessential to the very legitimacy of the program.

---

[323] *Id*. at 8. The request must identify as clearly as possible the financial data, substantiate the necessity of the data, tailor the data as narrowly as possible to minimize the amount of data requested, and not seek any data relating to the Single Euro Payments Area. The department must store the financial data in a secure physical environment where they are accessed only by analysts investigating terrorism or its financing, and the financial data must not be interconnected with any other database. *Id.* at 8.

[324] *See July 13 Version: International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY AND PROPORTIONATE (July 10, 2013), *available at* http://en.necessaryandproportionate.org/text (discussing the relationship between privacy rights and the current digital surveillance technologies). The Committee commissioned by the president recommends that the government should commission a study of the legal and policy options for assessing the distinction between metadata and other types of information. *See* LIBERTY REPORT, *supra* note 93, at 120.

[325] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting calling data reveals "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on") (internal quotations omitted) (citation omitted).