CHAPTER 6:

COMPARATIVE SURVEILLANCE SAFEGUARDS DEVELOPED BY OXFORD RESEARCH TEAM

[1] To assist in the comparison of EU and US national security surveillance practices, this Chapter applies criteria for national security surveillance laws developed by a team led by noted European privacy expert Professor Ian Brown of Oxford University.[1]

[2] The Oxford team developed a framework to analyze the categories of reform called for in democratic societies in the wake of revelations of large-scale electronic surveillance by the US and EU Member States. The Oxford team based its framework on what it called four "prominent" proposals for surveillance reforms:[2]

1. The International Principles on the Application of Human Rights to Communications Surveillance, which listed 13 "necessary and proportionate" principles to codify human rights obligations in the field of foreign surveillance.[3]

2. The report of the European Parliament Civil Liberties (LIBE) Committee concerning the Snowden revelations.[4]

3. Principles for surveillance reform that were endorsed by leading technology companies including AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo.[5]

4. The recommendations of President Obama's Review Group on Intelligence and Communications Technology, on which I served.[6]

[3] This Chapter applies the 11 categories of safeguards derived by the Oxford team from these four sources. For each category, I cite the applicable guidance from the four reform proposals,

---

[1] Professor of Information Security and Privacy at the Oxford Internet Institute. His research is focused on surveillance, privacy-enhancing technologies, and Internet regulation. He is an ACM Distinguished Scientist and BCS Chartered Fellow, and a member of the Information Commissioner's Technology Reference Panel. *See* IAN BROWN, MORTON H. HALPERIN, BEN HAYES, BEN SCOTT, AND MATHIAS VERMEULEN, TOWARDS MULTILATERAL STANDARDS FOR SURVEILLANCE REFORM, https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf. The discussion in this chapter is based on my review of the paper, and I have not been in contact with Professor Brown or his team in the preparation of my testimony.

[2] *Id.* at 18-24.

[3] NECESSARY AND PROPORTIONATE, *July 2013 version: International Principles on the Application of Human Rights to Communications Surveillance* (July 10, 2013), https://necessaryandproportionate.org/text/2013/07/10 [hereinafter *International Principles*].

[4] European Parliament Comm. on Civil Liberties, Justice and Home Affairs, *Rep. on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, A7-0139/2014 (Feb. 21, 2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN [hereinafter *LIBE Report*].

[5] REFORM GOV'T SURVEILLANCE, *Global Government Surveillance Reform: The Principles* (Dec. 9, 2013), https://www.reformgovernmentsurveillance.com/ [hereinafter *Company Principles*].

[6] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (2014), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter REVIEW GROUP REPORT].

listed above. I cite the Review Group recommendations and US reforms to date for that category. I then cite reviews of European practices by EU commentators since the Snowden disclosures.

[4] I believe this approach provides a systematic and relatively objective way to assess and reconcile current EU and US safeguards. As discussed further in the conclusion, my own view is similar to that of the Oxford team: that the US, after the reforms that occurred in the wake of the Snowden revelations, is the new "benchmark" for transparent principles, procedures, and oversight for national security surveillance.[7]

I. Categories for Comparison

[5] After grouping the reform recommendations into 11 categories, the Oxford team summarized each of the reform proposals relative to the respective category: (1) mandatory retention of metadata; (2) bulk collection; (3) data mining; (4) judicial control; (5) disclosure of legal authorities; (6) rights of subjects of foreign surveillance; (7) notification of data subjects; (8) data minimization; (9) onward transmission/purpose limitation; (10) transparency; and (11) oversight. For each of the categories developed by the Oxford team, I provide: (a) the approach recommended by the Review Group and subsequent US reforms; and (b) review of European practices by EU commentators since the Snowden disclosures.

1. Mandatory Retention of Metadata

[6] In the category of mandatory retention of metadata, the Oxford team identified the following reform approaches:

> *The International Principles*: The reforms focused on the idea that *a priori* data collection and retention should not be required of service providers.[8]
>
> *The LIBE Report*: The document stated that data retention was incompatible with Article 52(1) of the Charter of Fundamental Rights of the European Union.[9]
>
> *The principles of technology companies:* The companies advocated for limitations on the government's ability to compel service providers to disclose user data.[10]
>
> *The Review Group:* For foreign intelligence purposes, it recommended the US government introduce a system in which metadata is no longer held by the government, but is held by private providers or by a private third party, with access to such data permitted only with an order from the Foreign Intelligence Surveillance Court (FISC).[11]

[7] Brown et al., *supra* note 1, at 19.
[8] *See International Principles*, *supra* note 3, at "Integrity of communications systems"; Brown et al., *supra* note 1, at 20.
[9] *LIBE Report*, *supra* note 4, at Preamble; *see* Brown et al., *supra* note 1, at 20.
[10] *Company Principles*, *supra* note 5, para. 1; *see* Brown et al., *supra* note 1, at 20.
[11] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 5; *see* Brown et al., *supra* note 1, at 20.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[7] *Review Group Recommendation 5:* "We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intelligence Surveillance Court."[12] This recommendation was based, in large part, on the Review Group's finding "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."[13]

[8] *Reforms since 2013:* The USA FREEDOM Act ended the bulk collection practice under Section 215 for collection of "tangible things" (including phone records).[14] There is no mandatory data retention in the US for Internet records. Telephone records that are needed for billing purposes are retained for 18 months.[15]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[9] *Review by Professor Federico Fabrinni:* Data retention requirements have been a prominent feature of European debates about how to achieve privacy protection consistent with law enforcement and national security goals. In 2006, the EU promulgated a Data Retention Directive,[16] which required publicly available electronic communications services to retain records for an extended period of time, for purposes of fighting serious crime. For instance, for email and other electronic communications, the communications services were required to retain "the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication."[17] In the *Digital Rights Ireland* case, the European Court of Justice struck down that Directive due to privacy concerns related to excessive access to the retained data and lack of assurances that the records would be destroyed at the end of the retention

---

[12] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 5.
[13] *Id.*
[14] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), Pub. L. No. 114-23, § 103 (2015), https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf.
[15] 47 C.F.R. § 42.6. The telephone retention rule is discussed in REVIEW GROUP REPORT, *supra* note 6, at 119 n. 118.
[16] EU 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), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [hereafter "Data Retention Directive"].
[17] *Id.*, Art. 5(1)(b).

period.[18] In the wake of that judgment, a number of EU Member States have reinstated modified data retention requirements for telephone and Internet communications.[19]

[10] Data retention is an ongoing issue, with cases pending before the European Court of Justice.[20]

2. Bulk Collection

[11] In the category of bulk collection, the Oxford team analyzed the following reform approaches:

> *The International Principles:* The group advocated for a prohibition on bulk collection.[21]
>
> *The LIBE Report:* The report advocated for a prohibition on bulk collection.[22]
>
> *The principles of technology companies:* The companies advocated for a prohibition on bulk collection.[23]
>
> *The Review Group:* We recommended an end to collection and storage of all mass undigested, non-public personal information. We also suggested that any program involving collection or storage of such data should be narrowly tailored to serve an important government interest and called for agencies to examine the feasibility of creating software allowing targeted information acquisition.[24]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[12] *Review Group Recommendation 4:* "We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest."

---

[18] *See* Case C-293/12, *Digital Rights Ireland v. Minister of Commc'ns*, 2014 E.C.R. I-238, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

[19] *See* Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RIGHTS J., 73-74, 88 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.

[20] *Op. of the Advocate General* in Joined Cases C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and C-698/15, *Sec. of State for Home Dep't v. Watson* (2016), http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=EN&mode=req&occ=first.

[21] *International Principles*, *supra* note 3, at "Proportionality" and "Competent Judicial Authority"; *see* Brown et al., *supra* note 1, at 20.

[22] *LIBE Report*, *supra* note 4, at paras. 17, 21; *see* Brown et al., *supra* note 1, at 20.

[23] *Company Principles*, *supra* note 5, para. 1; *see* Brown, et al., at 20.

[24] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 4, 20; *see* Brown et al., *supra* note 1, at 20.

[13] *Review Group Recommendation 20:* "We recommend that the US Government should examine the feasibility of creating software that would allow the [NSA] and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection."[25]

[14] *Reforms since 2013:* The USA FREEDOM Act prohibited bulk collection under three authorities: (1) Section 215, for collection of "tangible things" (including phone records);[26] (2) Foreign Intelligence Surveillance Act (FISA) pen register and trap and trace authorities (to/from information about communications);[27] and (3) National Security Letters (phone, financial, and credit history records).[28]

[15] In addition, Section 2 of Presidential Policy Directive 28 (PPD-28) creates new limitations on the use of signals intelligence for the collection of communications that, in the initial stages, targets not an individual but a large flow of data. More specifically, PPD-28 limits the use of signals intelligence for "authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants," such as email or other selectors.[29] PPD-28 announces purpose limitations – when the US collects large quantities of nonpublicly available information, it shall use that data only for purposes of detecting and countering:

(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the US and its interests;
(2) Threats to the US and its interests from terrorism;
(3) Threats to the US and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
(4) Cybersecurity threats;
(5) Threats to US or allied armed forces or other US or allied personnel;
(6) Transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.[30]

If this list is updated, it will be "made publicly available to the maximum extent feasible."[31]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[16] *Review in the 2013 Report to the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs*: According to the Report, the "practice of so-called 'upstreaming' –

[25] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 20.
[26] USA FREEDOM Act § 103.
[27] *Id.* at § 201.
[28] *Id.* at § 501.
[29] THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, Presidential Policy Directive, Signals Intelligence Activities, PPD-28, § 2 (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28]. PPD-28 further provides that the "[t]he limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." *Id.*
[30] *Id.*
[31] *Id.*

tapping directly into the communications infrastructure as a means to intercept data – appears to be a relatively widespread feature of surveillance by several EU Member States, namely the UK, Sweden, France, and Germany."[32] The UK's Tempora program is engaged in routine interception of approximately 200 undersea cables that transmit Internet data into and out of the British Isles.[33] In Sweden, the government monitors cable-bound communications into and out of Sweden, including telephone calls, text messages, and emails.[34] The French program for large-scale surveillance is reported to collect, process, and store petabytes of data collected from at least 20 interception points comprised of both satellite stations and tapping fiber-optic submarine cables outside the country.[35] In Germany, the program for large-scale surveillance directly connects to digital traffic nodes through which foreign communications flows. German intelligence agencies are legally allowed to search up to 20% of the communications having a foreign element for national security reasons.[36] The Report concluded: "Surveillance programs in EU member states are incompatible with minimum democratic rule of law standards derived from the EU Charter of Fundamental Rights and the European Convention on Human Rights, and are in turn essential components of their national constitutional traditions."[37]

3. Data Mining

[17] In the category of data mining, the Oxford team identified the following reform approaches:

The International Principles: The issue was not addressed.[38]

The LIBE Report: The issue was not addressed.[39]

The principles of technology companies: The issue was not addressed.[40]

The Review Group: We recommended Civil Liberties Impact Assessments to ensure that any big data and data-mining programs are statistically reliable, cost-effective, and protective of privacy.[41]

---

[32] Didier Bigo et al., European Parliament Comm. on Civil Liberties, Justice and Home Affairs, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law* (2013), at 20, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.
[33] *Id.* at 50-51.
[34] *Id.* at 58-60.
[35] *Id.* at 63-64.
[36] *Id.* at 73-74.
[37] *Id.* at 27.
[38] The category is not addressed in the *International Principles*; *see* Brown et al., *supra* note 1, at 21.
[39] The category is not addressed in the *LIBE Report*; *see* Brown et al., *supra* note 1, at 21.
[40] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 21.
[41] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 35, 36; *see* Brown et al., *supra* note 1, at 21.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[18] *Review Group Recommendation 35:* "We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties."[42]

[19] *Review Group Recommendation 36:* "We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies."[43]

[20] *Reforms since 2013:* Since 2013, the Privacy and Civil Liberties Oversight Board (PCLOB) has released detailed reports on the Section 215[44] and Section 702[45] surveillance programs, making numerous recommendations. Its central recommendations on the Section 215 telephone metadata program were enacted in the USA FREEDOM Act. Overall, the PCLOB made 22 recommendations in its Sections 215 and 702 reports, and virtually all have been accepted and either implemented or are in the process of being implemented.[46]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[21] *Review by the Report prepared for the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs:* According to the Report, the scale of the big data collected from Upstream interception requires establishing techniques, methods, and infrastructure to filter the enormous data flows. Large-scale electronic surveillance suggests data extraction, data comparison, data retention, and the use of numerous databases. The Report found it unfortunate that concrete and detailed information on how data is collected in these Upstream programs by Member States is unavailable, although hints were uncovered in reports and expert statements.[47]

[22] The Report discussed the so-called "Massive Volume Reduction" employed by the UK's Government Communications Headquarters (GCHQ) to remove approximately 30% of the data that is deemed less intelligence relevant. It noted that the lack of details on this program or the others used by EU Member States "leaves an important gap in our understanding of the practices that intelligence services are engaging in to exploit the bulk data collected. These details would

---

[42] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 35.
[43] *Id.* at Recommendation 36.
[44] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (January 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.
[45] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.
[46] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATIONS ASSESSMENT REPORT (February 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.
[47] Bigo et. al, *supra* note 32, at 23.

be critical to determine operational legitimacy and interaction with national frameworks regulating surveillance."[48]

4. Judicial Control

[23] In the category of judicial control, the Oxford team identified the following reform approaches:

> *The International Principles:* The group looked to an independent, impartial, and competent authority capable of reviewing to determine whether less invasive techniques have been considered.[49]
>
> *The LIBE Report:* The report asserted that principles of legality, necessity, proportionality, due process, and transparency – consistent with the European Convention on Human Rights – should be adhered to, with strict limits on the duration and scope of the surveillance.[50]
>
> *The principles of technology companies:* The companies advocated for independent reviewing court with an adversarial process.[51]
>
> *The Review Group:* In addition to existing judicial control under the Foreign Intelligence Surveillance Court, we recommended the creation of the position of Public Interest Advocate to represent privacy and civil liberties interests before FISC.[52]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[24] *Review Group Recommendation 28:* "We recommend that:

> 1. Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court;
> 2. the Foreign Intelligence Surveillance Court should have greater technological expertise available to the judges;
> 3. the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards; and

---

[48] *Id.*
[49] *International Principles*, *supra* note 3, at "Proportionality" and "Competent judicial authority"; *see* Brown et al., *supra* note 1, at 21.
[50] *LIBE Report*, *supra* note 4, at paras. 22, 77; *see* Brown et al., *supra* note 1, at 21.
[51] *Company Principles*, *supra* note 5, para. 2; *see* Brown et al., *supra* note 1, at 21.
[52] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 12 and 28; *see* Brown et al., *supra* note 1, at 21.

4. Congress should change the process by which judges are appointed to the Foreign Intelligence Surveillance Court, with the appointment power divided among the Supreme Court Justices."[53]

[25] *Reforms since 2013:* Consistent with the Review Group recommendation, the USA FREEDOM Act authorized the creation of a group of independent experts, called "*amici curiae*" (friends of the Court), to brief the Foreign Intelligence Surveillance Court (FISC) on important cases.[54] The law instructs the FISC to appoint an *amicus curiae* for a matter that, in the opinion of the court, "presents a novel or significant interpretation of the law."[55] The court retains discretion on when to appoint an *amicus curiae*, but the clear intent of the statute is that independent lawyers with security clearances shall participate before the FISC in important cases.

[26] This reform provides the opportunity for independent views to be heard by the FISC in important cases, so that the assertions of government officials can be carefully tested before the judge. The first statutory criterion for selection is "expertise in privacy and civil liberties."[56] The FISC has named six expert lawyers, including a professor and lawyers who have been involved in these matters either in prior government service or in private practice.[57]

[27] The USA FREEDOM Act provides that an *amicus* may be appointed for proceedings in the Foreign Intelligence Surveillance Court of Review (FISCR), under the same provision as the *amicus* is appointed for the FISC.[58] The statute also makes a provision for the appointment of an *amicus* in the event that a case is appealed from the FISCR to the United States Supreme Court.[59]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[28] *Review by the Oxford team:* The Oxford team noted the Reform Group proposal for adversarial counsel in the FISC. The Oxford team lamented that many European states do not have a clear legal process in which such privacy advocates could participate.[60]

[29] *Review by the European Union Agency for Fundamental Rights:* According to the report, only France, Germany, the Netherlands, Sweden, and the UK among the Member States have detailed public laws related to the collection of signals intelligence.[61] The EU Agency for

---

[53] *Id.*, at Recommendation 28.
[54] USA FREEDOM Act § 401.
[55] *Id.*
[56] *Id.*
[57] *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae. For a recent report on how one such *amicus curiae* case has worked in practice, *see* Tim Cushing, *FISA Court's Appointed Advocated Not Allowing Government's 'National Security' Assertions To Go Unchallenged*, TECHDIRT.COM (Dec. 11, 2015), https://www.techdirt.com/articles/20151210/08175733048/fisa-courts-appointed-advocate-not-allowing-governments-national-security-assertions-to-go-unchallenged.shtml.
[58] USA FREEDOM Act § 401; 50 U.S.C. § 1803.
[59] *Id.*
[60] Brown et al., *supra* note 1, at 30-31.
[61] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf [hereinafter AGENCY FOR FUNDAMENTAL RIGHTS REPORT], at 54.

Fundamental Rights found that none of these Member States had judicial approval of signals intelligence. Their report noted that Germany and Sweden each have an expert body in charge of authorizing signals intelligence.[62]

5. Disclosure of Legal Authorities

[30] In the category of disclosure of legal authorities, the Oxford team identified the following reform approaches:

> *The International Principles:* The group focused on notification issues that are discussed below. [63]
>
> *The LIBE report:* The report put forth the idea that secret courts violate the rule of law.[64]
>
> *The principles of the technology companies*: The companies advocated for disclosure of important rulings, in a timely manner, to ensure the courts are accountable to the public.[65]
>
> *The Review Group*: The Review Group made multiple recommendations supporting greater transparency in various respects, but did not make a specific recommendation concerning publication of legal rulings.[66]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[31] *Reforms since 2013:* Prior to 2013, the statutory provisions in the Foreign Intelligence Surveillance Act and other statutes relating to foreign intelligence were publicly available. The USA FREEDOM Act added a new provision concerning transparency of the law applying to foreign intelligence cases. Going forward, orders of the Foreign Intelligence Surveillance Court (FISC) that involve substantial interpretations of law must either be declassified or summarized and then made publicly available on the Internet.[67] This new statutory provision directly addresses the risk of secret law.

[32] Since 2013, the US administration has reviewed FISC opinions in order to declassify to the extent consistent with national security, resulting in the numerous disclosures discussed in Chapter 5 on the activities of the FISC. The Office of the Director of National Intelligence maintains a website, accessible to the public, which contains declassified opinions of FISC and its reviewing

---

In this type of collection, selectors are later applied to the data to draw out information relevant to intelligence work.

[62] *Id.*, at 54-55.

[63] *International Principles*, *supra* note 3, at "User Notification"; *see* Brown et al., *supra* note 1, at 21.

[64] *LIBE Report*, *supra* note 4, at para.14; *see* Brown et al., *supra* note 1, at 21.

[65] *Company Principles*, *supra* note 5, para. 2; *see* Brown et al., *supra* note 1, at 21.

[66] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 7, 8; *see* Brown et al., *supra* note 1, at 21-22.

[67] 50 U.S.C. § 1872(b).

body, the Foreign Intelligence Court of Review.[68] This website is called "IC on the Record" and is located at https://icontherecord.tumblr.com/.

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[33] *Review by the Council of Europe's Commissioner of Human Rights*: The report found: "In many Council of Europe members states, bulk untargeted surveillance by security services is either not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures. This is problematic from a human rights perspective because it makes it difficult for individuals and organizations to understand the legal basis and reasons for which their communications may be intercepted, or to challenge such surveillance as being unlawful."[69]

[34] *Review by Dr. Christina Casagran*: To the extent that public laws exist, intelligence services in the EU are only regulated at the national level. There are no EU-level laws regulating the information processed by these bodies.[70] "As a result, EU data protection rules can be circumvented via intelligence services." [71]

[35] *Review by the Oxford team:* The team concluded that, in contrast to the clear and specific rules in the US, "many of the comparative legal frameworks in European states appear to give foreign and military agencies 'carte blanche'" to engage in foreign intelligence surveillance.[72]

6. Rights of Subjects of Foreign Surveillance

[36] In the category of rights of subjects of foreign surveillance, the Oxford team discussed the following reform approaches:

> *The International Principles:* The group advocated for individuals having access to a fair and public hearing within a reasonable time by an independent tribunal, except in cases of emergency where there would be imminent risk of danger to human life.[73]

---

[68] Any additional appeals would be taken to United States Supreme Court.

[69] Council of Europe Commissioner for Human Rights, *Issue Paper: Democratic and effective oversight of national security services* (2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770, at 23.

[70] CRISTINA BLASI CASAGRAN, GLOBAL DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT: AN EU PERSPECTIVE 188 (2017).

[71] *Id.*

[72] Brown et al., *supra* note 1, at 9; *see also* CASAGRAN, *supra* note 87, at 187 ("It can be concluded that intelligence services in Member States often have a *carte blanche* to collect and process information and turn it into intelligence. Data collected does not only belong to EU citizens under suspicion or linked to criminal groups, but it also includes data from innocent individuals.").

[73] *International Principles*, *supra* note 3, at "Due Process"; *see* Brown et al., *supra* note 1, at 22.

The LIBE report: The report called for the US to amend legislation to recognize the privacy of EU citizens, to provide judicial redress, and to put the rights of EU citizens on an equal footing with those of US citizens.[74]

The principles of the technology companies: The companies did not address this issue.[75]

The Review Group: We recommended applying the 1974 Privacy Act[76] to both US persons and non-US persons and exploring arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens with a small number of closely allied governments.[77]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[37] *Review Group Recommendations 14:* "We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons."[78]

[38] *Reforms since 2013:* In February 2016, the US enacted the Judicial Redress Act extending privacy protections and remedies available under the Privacy Act to qualifying non-US individuals of covered countries. These protections generally include rights to review, copy, and request amendments to covered records maintained by designated federal agencies in the US.[79]

[39] In 2014, President Obama announced Presidential Policy Directive 28 (PPD-28), granting significant further protections to non-US citizens. PPD-28 states that – regardless of nationality – "all persons have legitimate privacy interests in the handling of their personal information," and it mandates that US intelligence agencies make privacy integral to signals intelligence planning.[80] Specifically, PPD-28 requires agencies to prioritize alternative sources of information – such as diplomatic sources – over signals intelligence.[81] Where surveillance is used, it must be "as tailored as feasible," proceeding via selectors whenever practicable.[82] Bulk collection cannot be used except to detect and counter serious threats, such as terrorism, espionage, or nuclear proliferation.[83] The European Commission found that PPD-28's protections, which apply equally to US and non-

---

[74] *LIBE Report*, *supra* note 4, at para. 30; *see* Brown et al., *supra* note 1, at 22.
[75] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 22.
[76] The Privacy Act regulates the US government's use of computerized databases of information, imposing restrictions on each federal agency's collection, use, or disclosure of personal information. 5 U.S.C. § 552a.
[77] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 14, 21; *see* Brown et al., *supra* note 1, at 22.
[78] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 14.
[79] *See generally* The Judicial Redress Act of 2016, Pub. L. No. 114-126, https://www.congress.gov/bill/114th-congress/house-bill/1428/text. For a more detailed discussion of the Judicial Redress Act, *see* Chapter 7, Section I(A)(1).
[80] Chapter 3, Section IV(B) contains a detailed discussion of the significant safeguards instituted by PPD-28. *See also* PPD-28, *supra* note 29.
[81] *See id.* § 1(d).
[82] *See id.*
[83] *See id.* § 2.

US persons, embody "the essence of the principles of necessity and proportionality."[84]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[40] *Review by Oxford team:* In EU Member States, the collection of electronic communications from outside the borders of the country is authorized for a variety of purposes. EU Member States have given themselves greater flexibility to do surveillance outside of their borders than within. For example, the UK's surveillance targets communications of non-UK residents, and the Swedish program is focused on foreign communication. Broadly speaking, the purposes for foreign surveillance in EU Member States relate to national security, external military threats, the prevention and detection of serious crimes (including terrorism), and a Member State's policy or economic interests.[85]

[41] *Review by Venice Commission:* The Venice Commission expressed its concern for a distinction being made between citizens and residents, on the one hand, and non-citizens and non-residents, on the other hand, when applying standards for targeting individuals and retaining data collected by surveillance measures. The Commission specifically focused on the US and Germany, whose safeguards legislation it stated does not apply to non-citizens and non-residents.[86]

7. Notification of Data Subjects

[42] In the category of notification of data subjects, the Oxford team identified the following reform approaches:

> *The International Principles:* The group would provide individuals with notification of decisions authorizing surveillance with enough time and detail to allow them to appeal, unless notification would seriously jeopardize the purpose of the surveillance.[87]
>
> *The LIBE report:* The report advocated for respect for the principle of user notification.[88]
>
> *The principles of the technology companies*: The technology companies do not discuss this issue.[89]

---

[84] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, para. 76, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

[85] Brown et al., *supra* note 1, at 10.

[86] European Commission for Democracy through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, (Apr. 7, 2015), http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e [hereinafter "VENICE COMMISSION REPORT"], at 19, n.38.

[87] *International Principles*, *supra* note 3, at "User Notification"; *see* Brown et al., *supra* note 1, at 22.

[88] *LIBE Report*, *supra* note 4 at para. 22; *see* Brown et al., *supra* note 1, at 22.

[89] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 22.

The Review Group: The Review Group recommended limits on nondisclosure orders, with service providers being able to provide notice once the order expires.[90] More generally, a theme of this testimony is the importance of creating effective systemic safeguards against excessive surveillance,[91] while being cautious about providing individual notice or individual remedies if they can be used as a vector of attack by hostile actors to national security secrets.[92]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[43] *Review Group Recommendation 8:* "We recommend that:

1. legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;
2. nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and
3. nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality."[93]

[44] *Reforms since 2013.* In January 2014, President Obama announced that indefinite secrecy would change for National Security Letters (NSLs). He directed the US Attorney General to change NSL rules so that secrecy about NSLs "will not be indefinite," and "will terminate within a fixed time unless the government demonstrates a real need."[94] As of 2015, the FBI presumptively terminates NSL secrecy for an individual order when an investigation closes, or no more than three years after the opening of a full investigation.[95] Exceptions are permitted only if a senior official determines that national security requires NSL secrecy to be extended in the particular case, and explains the basis in writing.[96]

---

[90] *Id.* at Recommendation 8.
[91] *See generally* Chapter 3.
[92] *See generally* Chapter 8.
[93] *Id.*
[94] *Remarks by the President on Review of Signals Intelligence*, WHITE HOUSE, OFFICE OF PRESS SEC'Y (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter *Remarks by the President*].
[95] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform: 2015 Anniversary Report*, IC ON THE RECORD, https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[96] *Id.*

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[45] *Review by Agency for Fundamental Rights:* Eight Member States do not provide a notice obligation or the right to access data collected for foreign surveillance purposes.[97] In Member States that provide a right to access and an obligation for the agency to inform the individual, these rights "tend to be restricted on the ground that the information would threaten the objectives of the intelligence services or national security."[98] In Bulgaria, the rights of notification and access only apply to unlawful surveillance.[99] In Germany, the individual must establish a special interest to be able to exercise the right to access.[100] In Sweden, the data subject has a right to be informed, within a month of the collection, if the search terms directly relate to him/her. As of the date of the Agency for Fundamental Rights Report, no individuals had been informed – due to secrecy reasons.[101]

[46] The Agency for Fundamental Rights Report explained that three Member States have established timeframes that must be exhausted before notice applies and access rights can be exercised.[102] For example, in the Netherlands, individuals are notified five years after the surveillance, such as intercepting telecommunications, has taken place. This five-year deadline for notification can be further postponed if it will affect foreign intelligence information or relations with an ally.[103] The Hague District Court has held that there is not absolute duty of notification, and that, in cases involving surveillance, the secrecy of that surveillance prevails.[104]

[47] Ten Member States have a mechanism to involve the oversight body or court to determine whether the invoked grounds for restricting the rights are reasonable.[105] For example, in Austria, the right to access is restricted if that access could threaten the security of the state. The individual

---

[97] These countries are: the Czech Republic, Ireland, Latvia, Lithuania, Poland, Slovakia, Spain, and the UK. AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 62.
[98] *Id.* at 63.
[99] *Id.*; Закон за специалните разузнавателни средства [Bulgaria Special Intelligence Means Act], Oct. 21, 1997, Нов - ДВ, бр. 109 от 2008 г., изм. - ДВ, бр. 70 от 2013 г., в сила от 09.08.2013 г. [as amended by SG. 109 of 2008, SG. 70 of 2013, effective Aug. 9, 2013] (Bulg.).
[100] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 63; Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) [German Federal Act on the Protection of the Constitution] Dec. 20, 1990, das zuletzt durch Artikel des Gesetzes vom 26. Juli 2016 [last amended by Article 1 of the Law of July 26, 2016 (I, at 1818)]; Gesetz über den Bundesnachrichtendienst [BNDG] [German Act on the Federal Intelligence Service], Dec. 21, 1990, das zuletzt durch Artikel des Gesetzes vom 26. Juli 2016 (BGBI. I.S.1818) [last amended by Art.2 of the Law of July 26, 2016 (I, at 1818)] at § 7.
[101] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 63; *see also* Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] (Neth.), at 6.
[102] These countries are Belgium, Croatia, and the Netherlands. AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 63.
[103] *Id.*, at 63-64; *see also* Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] (Neth.) at Art. 34, 35(7), 47, 53 (Neth.).
[104] Rechtbank Den Haag [Court of the Hague] 23 juli 2014, ECLI:NL:RBDHA: 2014: 8966 (C/09/455237/HA ZA 13-1325, *Dutch Association Criminal Lawyers / Netherlands*) (Neth.), (in Dutch) http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:8966.
[105] The countries are: Austria, Belgium, Cyprus, Denmark, France, Germany, Greece, Italy, Luxembourg, and the Netherlands. AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 64-65.

may turn to the Data Protection Authority (DPA) to request a check of the agency's reply, but this process does not confirm or deny that surveillance is occurring.[106]

8. Data Minimization

[48] In the category of data minimization, the Oxford team identified the following reform approaches:

> *The International Principles:* The group called for confining the data accessed to only that which is reasonably relevant and for promptly destroying any excess information collected.[107]
>
> *The LIBE report:* The report does not address the issue.[108]
>
> *The principles of the technology companies:* The technology companies do not address the issue.[109]
>
> *The Review Group:* We recommended extending provisions on data minimization for US citizens under Section 215 of the USA PATRIOT Act to National Security Letters.[110]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[49] *Review Group Recommendation 3:* "We recommend 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."[111]

[50] *Reforms since 2013:* As one mechanism to minimize collection of data, the USA FREEDOM Act prohibited bulk collection via National Security Letters (phone, financial, and credit history records).[112] Furthermore, Presidential Policy Directive 28 (PPD-28) requires US intelligence agencies to apply the same minimization protections to non-US persons that they apply to US persons. Data about non-US persons may only be retained when "retention of comparable information concerning persons would be permitted."[113] Similarly, data about non-US persons cannot be disseminated unless the same could be done with comparable data about US persons.[114]

---

[106] *Id.* at 64; *see* Bundesgesetz über den Schutz personenbezogener Daten [Federal law on the Protection of Personal Data] (Datenschutzgesetz 2000 (DGS2000)) [(Data Protection Act 2000 (DGS2000), as amended)] Bundesgesetzblatt [BGBl] No. 165/1999, as amended, at §§ 26(2), 30(3) (Austria).
[107] *International Principles*, *supra* note 3, at "Proportionality" and "Competent judicial authority"; *see* Brown et al., *supra* note 1, at 22-23.
[108] *LIBE Report*, *supra* note 4, at para. 106; *see* Brown et al., *supra* note 1, at 22.
[109] The category was not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 22.
[110] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 3; *see* Brown et al., *supra* note 1, at 22-23.
[111] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 3.
[112] USA FREEDOM Act, Sec. 501.
[113] *See* PPD-28, *supra* note 29, § 4(a)(i).
[114] *See id.*

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[51] *Review by Oxford team:* No European country "explicitly provides for minimization procedures or remedies for non-citizens."[115] Some European countries have safeguards aimed at minimizing the amount of data held on their own citizens. The Oxford team cited the Netherlands for having a statutory provision that requires the deletion of any data that has been "wrongly collected."[116] Generally, however, the Oxford team found that the laws in European Member States lack detail regarding the purpose, scale, nature, and oversight mechanisms for foreign intelligence surveillance.[117]

[52] The laws of the EU Member States do not explicitly rule out the bulk collection of foreign intelligence. Contrary to a prohibition on bulk collection, it is common for EU Member States' laws to compel telecommunication providers to cooperate with the country's intelligence agencies to allow the agencies access to foreign communications. After the communications are collected, the agencies filter the data based on selectors, which are keywords or personal information. In certain instances, these selectors need to be approved in advance by the executive branch, normally at a ministerial level; they may be subject to periodic review by the government or, in limited instances, there may be oversight by an independent body.[118]

9. Onward Transmission/Purpose Limitation

[53] In the category of onward transmission/purpose limitation, the Oxford team analyzed the following reform approaches:

> *The International Principles:* The groups urged that surveillance should only be accessed by the specified authority and used only for the purpose for which the authorization was given.[119]
>
> *The LIBE report*: The report did not address this issue.[120]
>
> *The principles of the technology companies:* The technology companies did not address this issue.[121]
>
> *The Review Group:* We advocated for no dissemination of information about non-US persons unless the information is relevant to protecting the national security of the US or its allies.[122]

---

[115] Brown et al., *supra* note 1, at 10.
[116] *Id*.
[117] *Id.*
[118] *Id*.
[119] *International Principles*, *supra* note 3, at "Proportionality" and "Competent judicial authority"; *see* Brown et al., *supra* note 1, at 23.
[120] The category is not addressed in the *LIBE Report*; *see* Brown et al., *supra* note 1, at 23.
[121] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 23.
[122] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 13(4); *see* Brown et al., *supra* note 1, at 23.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[54] *Review Group Recommendation 13(4):* "We recommend that, in implementing section 702, and any other authority that authorizes the surveillance of non-United States persons who are outside the United States, in addition to the safeguards and oversight mechanisms already in place, the US Government should reaffirm that such surveillance . . . must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies."

[55] *Reforms since 2013:* The agency procedures put in place pursuant to Section 4 of PPD-28 have created new limits that address this concern.[123] The new retention requirements and dissemination limitations are consistent across agencies and similar to those for US persons.[124] For retention, different intelligence agencies had previously had different rules for how long information about non-US persons could be retained. Under the new procedures, agencies generally must delete non-US person information collected through signals intelligence five years after collection.[125] For dissemination, there is an important provision applying to non-US persons collected outside of the US: "personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted."[126]

[56] The agency procedures make other changes for protection of non-US persons, including new oversight, training, and compliance requirements: "The oversight program includes a new requirement to report any significant compliance incident involving personal information, regardless of the person's nationality, to the Director of National Intelligence."[127]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[57] *Review by Oxford team:* In EU Member States, the collection of electronic communications from outside the borders of the country is authorized for a variety of purposes. EU Member States have given themselves greater flexibility to do surveillance outside of their borders than within.[128]

10. Transparency

[58] In the category of transparency, the Oxford team identified the following reform approaches:

---

[123] The US government will not consider the activities of foreign persons to be foreign intelligence just because they are foreign persons; there must be some other valid foreign intelligence purpose. *See* PPD-28, *supra* note 29, at § 4.
[124] The agency procedures create new limits on dissemination of information about non-US persons, and require training in these requirements. *Id.*
[125] There are exceptions to the five-year limit, but they can only apply after the Director of National Intelligence considers the views of Office of the Director of National Intelligence Civil Liberties Protection officer and agency privacy and civil liberties officials. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Strengthening Privacy and Civil Liberties Protections 2015 Anniversary Report*, IC ON THE RECORD, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[126] PPD-28, *supra* note 29, § 4(a)(i).
[127] *Id.*
[128] Brown et al, *supra* note 1, at 10.

The International Principles: The group supported requiring governments to publish periodic reports about foreign intelligence surveillance.[129]

The LIBE report: The report only spoke of transparency in general terms.[130]

The principles of the technology companies: The technology companies sought the ability to publish the number and nature of government demands for user information, and a requirement for governments to publicly disclose this information.[131]

The Review Group: We recommended increased transparency, both through government reporting and by permitting private sector recipients of government requests to provide more detail.[132]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[59] *Review Group Recommendation 9:* "We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security."[133]

[60] *Review Group Recommendation 10:* "We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security."[134]

[61] *Reforms since 2013:* In January, 2014 the US Department of Justice changed its reporting policies in response to litigation by five technology companies – Google, Microsoft, Yahoo, LinkedIn, and Facebook – to permit companies to report broad ranges of the numbers of orders they receive for collection of user information.[135] The USA FREEDOM Act codified and expanded

[129] *International Principles*, *supra* note 3 at "Public oversight"; *see* Brown et al., *supra* note 1, at 23.
[130] *LIBE Report*, *supra* note 4 at para. 62; *see* Brown et al., *supra* note 1, at 23.
[131] *Company Principles*, *supra* note 5, para. 2; *see* Brown et al., *supra* note 1, at 23.
[132] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 9, 10; *see* Brown et al., *supra* note 1, at 23.
[133] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 9.
[134] *Id.* at Recommendation 10.
[135] *See* Letter of January 27, 2014 from James M. Cole, Deputy Attorney General, US Dep't of Justice, to General Counsels of Google, Microsoft, Yahoo, Facebook, and LinkedIn, https://www.justice.gov/iso/opa/resources/422201412716042240387.pdf (proposing settlement terms for each company's respective legal action then pending in the F.I.S.C.).

this agreement. Companies now have four statutorily-guaranteed approaches by which they can provide statistics on orders for user information, and can do so – at their option – annually or semiannually.[136] Companies can report ranges of the number of (1) National Security Letters, (2) FISA orders or directives, and (3) non-content requests – along with the "number of customer selectors" targeted under each such request.[137] They may report ranges of the "total number of all national security process received," as well as the number of customers affected by such requests.[138]

[62] The USA FREEDOM Act codified expansion in the annual reporting by the US government about its national security investigations.[139] Each year, the government is required to report statistics publicly for each category of investigation. Specifically, the government is required to report to Congress, and make publicly available: (1) a report on applications for tangible things under Section 215, to include requests for call detail records and the number of orders issued approving such requests; (2) a report on the total number of applications filed and orders issued under Section 702 as well as the estimated number of targets affected by such orders, to include the PRISM and Upstream collection programs; and (3) a list of individuals appointed as *amicus curiae* as well as any findings that an appointment was not appropriate.[140]

[63] Administratively, the Office of the Director of National Intelligence's January 2015 report on Signals Intelligence Reform detailed eight categories of greater transparency that it had undertaken to that point.[141] Compared to the secrecy that historically had applied to signals intelligence, the shift toward greater transparency is remarkable, such as:

- The declassification of numerous FISC decisions;[142]
- A new website devoted to public access to intelligence community information;[143]
- The first "Principles of Intelligence Transparency for the Intelligence Community;[144]
- The first three Intelligence Community Statistical Transparency Reports;[145]

[136] USA FREEDOM Act, Sec. 604 (codified at 50 U.S.C. § 1874(a)).
[137] *See* 50 U.S.C. § 1874(a)(1).
[138] *Id.* § 1874(a)(3). If companies elect to report annually instead of semi-annually, they may report the total number of all national security process in bands of 100. *See id.* § 1874(a)(4).
[139] USA FREEDOM Act § 603.
[140] *Id.* §§ 601-602.
[141] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform, 2015 Anniversary Report – Enhancing Transparency*, IC ON THE RECORD (2015), https://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency.
[142] For detailed discussion of the rulings in these opinions, see Chapter 5.
[143] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), http://icontherecord.tumblr.com.
[144] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Principles of Intelligence Transparency for the Intelligence Community*, http://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20v1.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PRINCIPLES OF INTELLIGENCE TRANSPARENCY IMPLEMENTATION PLAN (2015), https://www.dni.gov/index.php/newsroom/reports-and-publications/207-reports-publications-2015/1274-principles-of-intelligence-transparency-implementation-plan.
[145] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

- Unclassified reports on NSA's implementation of Section 702[146] and its "Civil Liberties and Privacy Protections for Targeted SIGINT Activities;[147]
- Numerous speeches and appearances by intelligence community leadership to explain government activities, in contrast to the historical practice of very little public discussion of these issues;[148] and
- The Office of Director of National Intelligence now has a Civil Liberties Protection Officer.[149]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[64] Transparency about EU practices comes notably from public reviews in recent years, including:

1. *Review commissioned by the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs:* The 2013 briefing paper of the Center for European Policy Studies (CEPS) is approximately 75 pages, focusing on large-scale surveillance programs in the US and the EU.[150]

2. *Review by the Council of Europe's Commissioner of Human Rights*: The 2015 report is approximately 75 pages and details oversight of intelligence services.[151]

3. *Review by the European Union Agency for Fundamental Rights*: The 2015 report, which is approximately 100 pages, analyzes intelligence services and surveillance laws, oversight of intelligence services, and remedies.[152]

4. *Review by Venice Commission:* The 2015 report is approximately 40 pages and discusses democratic control, jurisdiction, accountability, and controls.[153]

---

[146] NATIONAL SECURITY AGENCY, *Civil Liberties and Privacy Home* (May 3, 2016), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.
[147] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.
[147] NATIONAL SECURITY AGENCY, *Civil Liberties and Privacy Home* (May 3, 2016), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.
[148] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.
[149] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, OFFICE OF CIVIL LIBERTIES, PRIVACY AND INTELLIGENCE, *Who We Are*, https://www.dni.gov/index.php/about/organization/civil-liberties-privacy-office-who-we-are.
[150] Bigo, et al., *supra* note 32, at 1-76.
[151] COUNCIL OF EUROPE COMMISSIONER OF HUMAN RIGHTS, ISSUE PAPER: DEMOCRATIC AND EFFECTIVE OVERSIGHT OF NATIONAL SECURITY SERVICES 1-74 (2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770.
[152] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 1-95.
[153] VENICE COMMISSION REPORT, *supra* note 87, at 1-39.

5. *Review by Professor Federico Fabrinni:* Approximately 30 pages in length, the 2015 article examines the privacy implications of the *Digital Rights Ireland* case.[154]

6. *Review by Dr. Christina Casagran*: This recently published book is approximately 240 pages. It highlights data protection relating to surveillance for law enforcement and foreign intelligence purposes.[155]

7. *Review by Oxford team:* The 2016 paper is approximately 40 pages and concentrates on existing foreign intelligence gathering standards, state obligations under international law, and proposals for surveillance reform.[156]

11. Oversight

[65] In the category of oversight, the Oxford team identified the following reform approaches:

The International Principles: The group proposed independent mechanisms that ensure transparency and accountability and have the authority to access all potentially relevant information about state actions.[157]

The LIBE report: The report urged oversight based on a strong legal framework, ex ante authorization, and ex post verification as well as adequate technical capability and expertise.[158]

The principles of the technology companies: The technology companies advocated for strong checks and balances. [159]

The Review Group: We recommended that the Director of National Intelligence establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional Intelligence committees.[160]

---

[154] Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS J. 65 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.
[155] Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, (New York: Routledge 2017), at 1-244.
[156] Brown et al., *supra* note 1, at 1-41.
[157] *International Principles*, *supra* note 3 at "Public oversight"; *see* Brown et al., *supra* note 1, at 23-24.
[158] *LIBE Report*, *supra* note 4, at ¶¶ 74-79; *see* Brown et al., *supra* note 1, at 23-24.
[159] *Company Principles*, *supra* note 5, ¶ 2; *see* Brown et al., *supra* note 1, at 23.
[160] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 18; *see* Brown et al., *supra* note 1, at 22-23.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[66] *Review Group Recommendation 18:* "We recommend that the Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees."[161]

[67] *Reforms since 2013:* In a close match with Review Group Recommendation 18, President Obama in 2014 announced that he was creating a process for senior policymakers to monitor the collection and dissemination activities of the Intelligence Community.[162]

[68] Since the Snowden revelations, the US has performed independent oversight through the Review Group and the Privacy and Civil Liberties Oversight Board (PCLOB).[163] Among other findings of the Review Group, we found strong compliance with existing requirements and no improper use of surveillance against political opponents.[164] We saw no instances of abuse of government power for inappropriate purposes, such as suppression of minorities, influencing of elections, or punishment of political opponents.

[69] Since 2013, the PCLOB has released detailed reports on Section 215 and 702 programs, making numerous recommendations.[165] Its central recommendations on telephone metadata program were enacted in the USA FREEDOM Act.[166] It made ten recommendations concerning Section 702, and virtually all have been accepted and either implemented or are in the process of being implemented.[167] In addition to the independent review by the Review Group and the PCLOB, Chapter 3 discusses the entire system of oversight that exists for foreign intelligence investigations, including the Foreign Intelligence Surveillance Court discussed in more detail in Chapter 5.

---

[161] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 18.
[162] *See Remarks by the President*, *supra* note 94.
[163] The PCLOB, at the time of these reports, had distinguished members with relevant expertise: (1) David Medine, the Chair, was a senior FTC privacy official who helped negotiated the Safe Harbor; (2) Rachel Brand has been the Assistant Attorney General for Legal Policy, serving as chief policy advisor to the US Attorney General; (3) Beth Collins has also served as Assistant General for Legal Policy at the US Department of Justice; (4) Jim Dempsey is a leading surveillance expert in US civil society, working for many years at the Center for Democracy and Technology; and (5) Patricia Wald was a judge on the Court of Appeals for the D.C. Circuit for twenty years, and has also served as a Judge on the International Criminal Tribunal for the former Yugoslavia.
[164] REVIEW GROUP REPORT, *supra* note 6, at 78, 182.
[165] *See, e.g.*, Privacy & Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Jan. 23, 2014*, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.
[166] This focused on Section 215 of FISA.
[167] For a list of the PCLOB's ten recommendations and the government's implementation actions in response, *see* Chapter 3, Section IV(C).

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[70] *Review by Oxford team:* The Oxford team explained that the quality of oversight depends on the resources available, the technical competence of the reviewers, and the avoidance of regulatory capture.[168] In its review, the Oxford team cited to the LIBE report, calling for oversight bodies to conduct on-site visits of intelligence agencies, interview senior officials, and ensure independence of inspectors. Both the Review Group and the PCLOB have had these characteristics.

[71] *Review by the European Union Agency for Fundamental Rights:* The Agency for Fundamental Rights Report noted that the general consensus is that oversight of foreign surveillance should combine executive control; parliamentary control; judicial review; and expert bodies:[169]

> Effective oversight does not necessarily require all four types of oversight mechanisms. Such oversight can be accomplished as long as the bodies in place complement each other and as a whole constitute a strong system capable of assessing whether the intelligence services' mandate is carried out properly.[170]

[72] The Agency for Fundamental Rights determined 24 EU Member States have parliamentary oversight, and 15 Member States have set up at least one expert body dedicated to the oversight of intelligence agencies.[171] The report analyzed the authority of Data Protection Authorities in EU Member States and determined that 12 of 28 have Data Protection Authorities with no power over national intelligence agencies, and another nine have limited powers related to intelligence.[172] Seven Member States have oversight systems that combine the executive, parliament, judiciary, and expert bodies. These seven Member States, however, do not include any of the Member States that have legal frameworks allowing signals intelligence collection.[173]

[73] With regard to signals intelligence, the report identified five Member States – France, Germany, the Netherlands, Sweden, and the UK – that engage in signals intelligence and have detailed legislation in place regarding this activity.[174] France has executive oversight, with the Prime Minister authorizing selectors and opinions offered by an oversight board.[175] The Netherlands collects non-cable bound communications (satellite and radio transmissions) without authorization outside of the agency, but must seek executive oversight for access using

---

[168] Brown et al., *supra* note 1, at 31.
[169] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 29; VENICE COMMISSION REPORT, *supra* note 87.
[170] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 57.
[171] *Id.* at 57-58.
[172] *Id*. at 49.
[173] *Id*. at 57.
[174] *Id*. at 20.
[175] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 56; *see* CODE DE LA SÉCURITÉ INTÉRIEURE [INTERIOR SECURITY CODE] Art L. 851-3 (Fr.), *La localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques*, http://www.assemblee-nationale.fr/14/projets/pl2669.asp.

keywords.[176] The UK requires warrants authorized by the Secretary of State.[177] The UK has an Investigatory Powers Tribunal to deal with individual complaints concerning surveillance, but its authority is limited to "assessing whether legislation has been complied with and authorities have acted 'reasonably.'"[178] Germany has oversight from both the Parliamentary Control Panel (telecommunications) and the G-10 Commission (selectors to filter the data).[179] Sweden has oversight by an expert body.[180]

[74] One of the Agency for Fundamental Rights' key findings was: "Access to information and documents by oversight bodies is essential. While information gathered by intelligence bodies is sensitive, and safeguards must guarantee that it will be dealt with accordingly, oversight bodies cannot carry out their tasks without first having access to all relevant information. The opposite, however, seems to be the norm [in the EU]."[181]

[75] *Review commissioned by the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs:* The briefing paper of the Center for European Policy Studies (CEPS) found that several Member States have oversight bodies that are faced with constraints that hamper their ability to apply sufficient scrutiny to intelligence agencies' surveillance practices. In Sweden, the two main oversight institutions, the intelligence court (UNDOM) and the Inspection for Defense Intelligence Operations (SIUN), were "deemed to be insufficiently independent." In France, the main oversight body, the CNCIS, was "found to be substantially constrained in its reach due to its limited administrative capacity."[182]

II. Conclusion

[76] The Oxford team found that the US legal system of foreign intelligence law contains "much clearer rules on the authorization and limits on the collection, use, sharing, and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States."[183]

---

[176] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 55; *see* Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] at Art. 26 (Neth.).
[177] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 55; s*ee* INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2015, HC 1075, at 37-38 (UK), *visit* http://isc.independent.gov.uk/committee-reports/special-reports *and click on* "Privacy and Security: a modern and transparent legal framework."
[178] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 68.
[179] *Id.* at 55.
[180] *Id.* at 54.
[181] *Id.* at 57. For example, in Poland, the prime minister appoints and dismisses the heads of the Polish intelligence services. She/he is in charge of approving their intelligence objectives and has the most far-reaching competences in terms of oversight of the intelligence services within the country. However, the Supreme Audit Office found that his/her oversight lacks efficacy, since he/she does not have access to the internal procedures of the intelligence services. The information given by the services both as to the content and the means by which intelligence is collected cannot therefore be verified. *Id.* at 32.
[182] Bigo et al., *supra* note 32, at 26.
[183] Brown et al., *supra* note 1, at 3. *See* Chapter 3 for a detailed discussion of the US system of foreign intelligence law.

[77] To the extent that the specifics of the EU Member States' legal frameworks for foreign intelligence surveillance are publicly available,[184] the Oxford team determined that "they generally compare unfavorably with the situation in the US after the adoption of [Presidential Privacy Directive 28]."[185]

[78] As the analysis in the article by the Oxford team charts, the Review Group made recommendations in most or all of the 11 categories identified by the Oxford team, and the US government has undertaken reforms in most or all of the categories since the release of the Review Group's recommendations.

[79] In conclusion, this independent framework for analysis provides a systematic and relatively objective tool to support my view that the safeguards in the US system of foreign intelligence law compare favorably to the regimes in other nations.

[184] Despite the limitations on the publicly available laws and procedures regulating foreign intelligence surveillance, the Oxford team found that the acts of the EU Member States share similar structures and that many European countries have made similar policy choices in respect to regulating foreign intelligence surveillance.

[185] Brown et al., *supra* note 1, at 10. After analyzing the laws of EU Member States, the Oxford team pointed out that European governments that want to further limit the NSA's activities concerning EU citizens first "need to get their own houses in order by developing, publicizing, and adopting publicly available standards that govern foreign intelligence collection." *Id.* at 10-11.