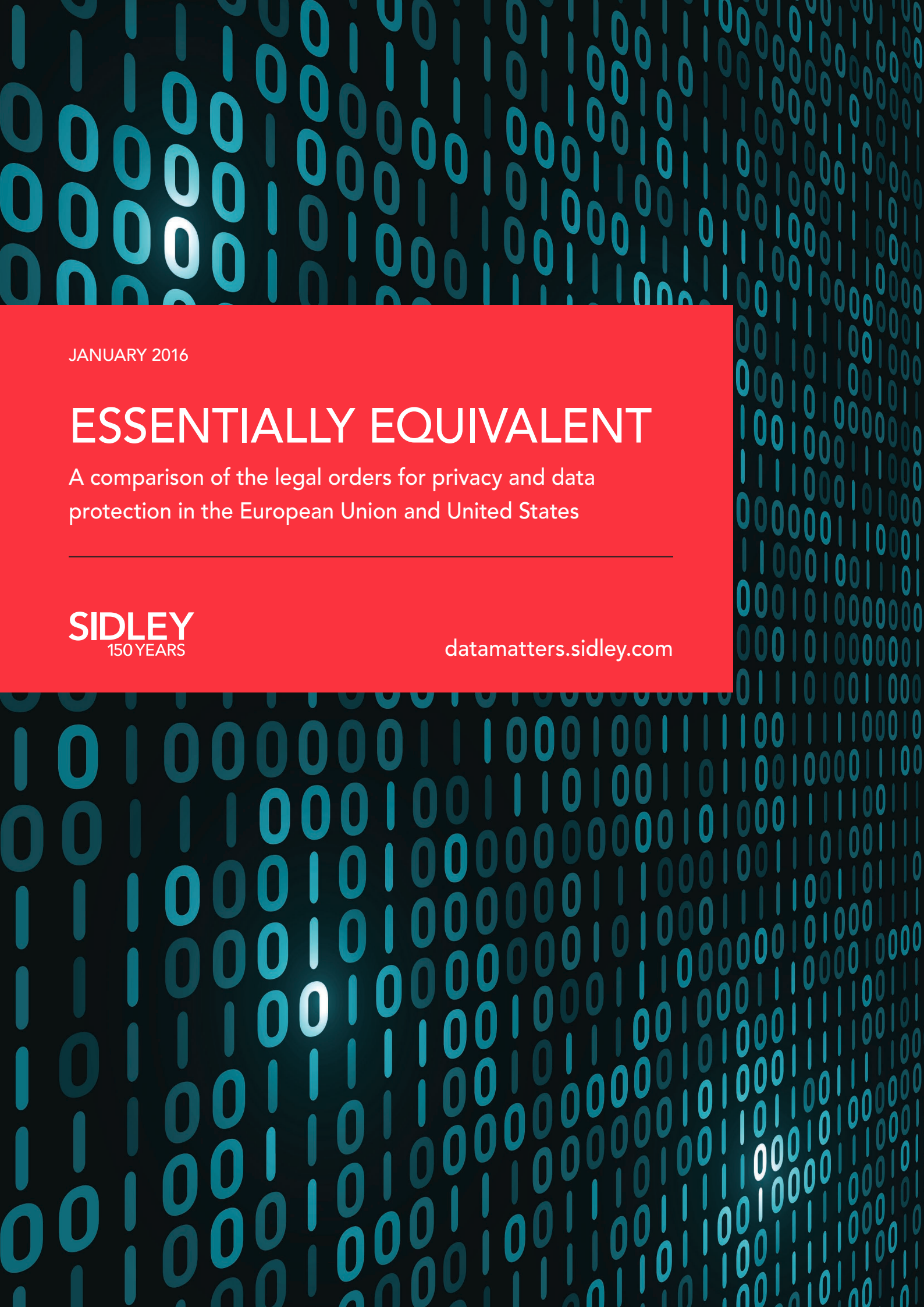


JANUARY 2016

ESSENTIALLY EQUIVALENT

A comparison of the legal orders for privacy and data protection in the European Union and United States

SIDLEY
150 YEARS

datamatters.sidley.com

SIDLEY
150 YEARS

25 January 2016

A report for:

H.E. Jean-Claude Juncker, *President of the European Commission*

H.E. Mark Rutte, *Prime Minister of the Netherlands*

H.E. Martin Schulz, *President of the European Parliament*

H.E. Donald Tusk, *President of the European Council*

The Hon. Isabelle Falque-Pierrotin, *Chairman of the Article 29 Working Party*

The Court of Justice of the European Union (CJEU) set out a test in *Maximillian Schrems v. Data Protection Commissioner* for deciding whether a third country's level of data protection is adequate under Article 25 of the European Union's Directive 95/46/EC (Directive 95/46). The CJEU declared that such a decision requires a finding that the level of protection of fundamental rights and freedoms in the laws and practices of the third country is "essentially equivalent" to that guaranteed within the European Union under that Directive read in light of the Charter of Fundamental Rights of the European Union (the Charter). Given the CJEU's invalidation of the European Commission decision underlying the EU-US Safe Harbour Framework, the Commission and supervisory authorities are now called upon to examine the legal order in the United States and compare its level of protection with that within the European Union. The legal order and corresponding substantive protection of each jurisdiction may not be assumed.

This report, "Essentially Equivalent: a comparison of the legal orders for data protection in the European Union and United States," provides a roadmap and resource for the requisite comparison. Following the analysis laid out by the CJEU in *Schrems*, the report shows how privacy values, deeply embedded in US law and practice, have resulted in a system that protects fundamental rights and freedoms and meets the test of essential equivalency.

The US system is not identical to that in the EU because, as a common-law country, the United States has evolved a multidimensional system of federal and state laws and jurisprudence rather than a single omnibus law comparable to Directive 95/46 (read in light of the Charter). This body of laws ensures that government access to data for law-enforcement and intelligence purposes is limited to what is necessary and proportionate. In addition, it governs the private sector and impels it to adopt strong privacy practices that, especially when reinforced by legally-binding commitments (pursuant to a Safe Harbour Framework or individualised data transfer mechanisms), correspond to the principles of Directive 95/46. Taken together, the practical effect of these laws and practices is to provide EU citizens, whose data is transferred to the United States, with a level of protection that is essentially equivalent to what these citizens receive under the legal order in the EU. (The report refers to the level of protection in the EU as the EU Benchmark).

Notable privacy protections under the US legal order begin with the Bill of Rights of the US Constitution, which protects the American people against unreasonable government searches and seizures and which has been interpreted as protecting interests in individual autonomy and dignity against government interference. The US Congress declared in the Privacy Act of 1974 that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States." Moreover, in legislation of 2004 and 2007, the Congress affirmed that any enlarged power of electronic surveillance

> "calls for *an enhanced system of checks and balances* to protect the precious liberties that are vital to our way of life and to ensure that the Government uses its powers for the purposes for which the powers were given. … [and that] if our liberties are curtailed, we lose the values that we are struggling to defend ….[and further, that] actions the executive branch takes to protect the Nation from terrorism [must be]… balanced with *the need to protect privacy and civil liberties*."[1]

And in a 2014 decision, the US Supreme Court denied the US government access to the electronic data stored in a smart phone because, in the words of the Chief Justice of the United States, "[p]rivacy comes at a cost."[2]

Foreign citizens also receive protection against US surveillance. The Foreign Intelligence Surveillance Act of 1978 and other statutes dictate the procedures with which law enforcement and the intelligence agencies must comply to collect, retain, and disseminate data transferred to the US. Executive orders further ensure that foreign citizens receive comparable privacy protections to those received by US citizens for communications collected outside the US and outside of FISA's reach. Specifically, a 2014 presidential order, binding on the government, directed the Nation's intelligence agencies that "[a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information."[3] This order is one of many checks and balances the US has added to surveillance safeguards, including terminating the bulk collection of telephone metadata under FISA. And US courts have held expressly that a key statute affecting the data of EU citizens stored in the US, the Electronic Communications Privacy Act, protects "any person, including foreign citizens." This statute provides one of several means of legal redress with respect to government surveillance.[4]

This report begins by analysing the *Schrems* judgment to specify what must be compared with respect to the US legal order, and to establish the EU Benchmark for the level of protection for privacy and personal data in the EU legal order. For the

---

[1] Pub. L. No. 110–53, § 801, 121 Stat. 353 (2007) (internal quotation marks and citations omitted; emphases added); Pub. L. No. 108-458, § 1061(a)(2), (2004).

[2] *Riley v. California*, 134 S. Ct. 2473, 2493 (2014).

[3] Presidential Policy Directive/PPD-28 (Jan. 17, 2014), http://fas.org/irp/offdocs/ppd/ppd-28.pdf.

[4] *Suzlon Energy Ltd. v. Microsoft Corp*., 671 F.3d 726, 729 (9th Cir. 2011).

EU legal order, the analysis begins, as the *Schrems* judgment did, with Articles 7 and 8 of the Charter. These articles establish respect for private life and protection of individuals with regard to the processing of data as fundamental rights. The analysis cannot end there, however, because the Charter applies only to EU law, and the Treaty on European Union makes national security the sole responsibility of the Member States, as allowed for in Article 13 of the present Directive 95/46 and Article 21 of the proposed General Data Protection Regulation.

Moreover, the privacy and data protection rights in Articles 7 and 8 must be balanced and applied in line with Article 52(1) of the Charter of Fundamental Rights. Limitations may be imposed on the exercise of these rights where the limitations are provided for by law, when they respect the essence of these rights and freedoms, and when, subject to the principle of proportionality, they are necessary to and genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

Subject to general principles of necessity and proportionality, therefore, EU law permits Member States a margin of discretion in the performance of essential state functions, including taking measures that balance data privacy rights with other fundamental rights protected by the Charter and measures to protect national security. Accordingly, the comparison of this legal order with the US legal order must be complete, accurate, and fair, with due consideration to international trade law obligations of the EU and Member States not to discriminate, and to practices as well as laws.

The report then looks at the contours of surveillance laws in both the US and EU in light of the basic requirements of the Charter as enunciated in *Schrems* and prior judgments and the margin of discretion under EU law. For the EU legal order, it looks at the scope of analogous laws in several Member States (which are partly outside the scope of EU law and its Charter of Fundamental Rights) and the range of protections and constraints applicable to the Member States in the area of national security. For the US legal order, the report focuses on the scope of the surveillance laws that may most affect personal data of European citizens that is transferred to the US and the protections that embody the principles of necessity and proportionality. Finally, although the CJEU did not consider the Safe Harbour principles themselves, the report also looks at the enforceability of the principles as well as the US legal order in the commercial arena in light of the criteria that have been applied in EU adequacy decisions involving third countries.

The comparison is a complex undertaking. As the European Union does not have competence with regard to national security, establishing the level of protection under the legal order for surveillance within the EU requires examination of the laws and practices of each of the Member States. Correspondingly, an assessment of the sectoral and federal system of privacy protection in the US requires examination of a range of federal laws as well as those of 50 states and the enforcement practices of numerous federal and state agencies.

This report is necessarily an overview of the relevant requirements, considerations, and practices. Given the breadth and complexity involved, it does not provide a comprehensive analysis of all relevant laws. It has been prepared in the wake of the

Schrems judgment to inform in a timely way the imminent debates on any new EU-US agreement with respect to transatlantic data transfers and other adequacy determinations. To these ends, the report intends to provide a thorough and thoughtful comparison that, while not complete in every detail, presents a fair picture of the level of protection of fundamental rights and freedoms for data and privacy in the United States as compared to the EU legal order.

This report provides substantial support for the proposition that the US legal order for privacy and data protection embodies fundamental rights consistent with the Charter, principles of proportionality, and checks and balances in both form and substance, and that these protections of privacy and data protection rights are essentially equivalent to those in the EU.

Respectfully submitted,

Jacques Bourgeois
Cameron F. Kerry
William R. M. Long
Maarten Meulenbelt
Alan Charles Raul

cc: The Honourable Anthony L. Gardner
U.S. Ambassador to the European Union

SIDLEY
150 YEARS

Essentially Equivalent

A comparison of the legal orders for privacy and data protection in the European Union and United States

Jacques Bourgeois

Cameron F. Kerry

William R. M. Long

Maarten Meulenbelt

Alan Charles Raul

January 2016

datamatters.sidley.com

Preface

This report was prepared by Sidley Austin LLP on behalf of the United States Chamber of Commerce, BSA | The Software Alliance, the Computer & Communications Industry Association, and the Information Technology Industry Council. The work was led by Cameron F. Kerry (Boston), Jacques Bourgeois and Maarten Meulenbelt (Brussels), William R. M. Long (London), and Alan Charles Raul (Washington). Additional Sidley Austin lawyers contributing to the report are Michele Boggiani, Ken Daly, Justine Fassion, Christian Grobecker, Pola Karolczyk, Cornelia Schiemann, and Michele Tagliaferri in Brussels; Francesca Blythe, and Geraldine Scali in London; Catherine Valerio-Barrad in Los Angeles; Kelly Rosencrans in San Francisco; and Colleen Theresa Brown, Christopher A. Eiswerth, Edward R. McNicholas, Vivek K. Mohan, Clayton G. Northouse, and Lacey Withington in Washington. We are grateful for assistance from Matthias Bäcker (Karlsruher Institut für Technologie), Laura Liguori (Portolano Cavallo), and Emmanuelle Mignon (August & Debouzy).

For further information regarding Sidley Austin and the authors, you may see pages at the end of this report or access our website at www.sidley.com, which contains address, telephone, and email for all offices and lawyers, as well as other information about the firm. Sidley Austin refers to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

Follow us at: Data Matters: Cybersecurity, Privacy, Data Protection, Internet Law and Policy, datamatters.sidley.com

SIDLEY AUSTIN LLP

CONTENTS

EXECUTIVE SUMMARY

In its 6 October 2015 decision in *Schrems v Data Protection Commissioner*,[5] the Court of Justice of the European Union (CJEU) did not rule that US data privacy protections are inferior to those in the EU. Rather, it ruled that, in its initial decision approving the Safe Harbour Framework (Decision 2000/520/EC),[6]and in the intervening years, the European Commission had not considered various safeguards for privacy and data protection in the US legal system, and thus had not ensured that EU citizens were adequately protected when their data is transferred to the US. The CJEU's judgment specified that the proper test for adequate protection would entail a finding that the level of privacy and data protection under the US legal system is "essentially equivalent" to that in the EU.

This report provides an in-depth survey designed to compare the legal orders for data protection in the European Union and the United States, and to explore how the US data protection regime is essentially equivalent to that of the EU under Directive 95/46/EC (Directive 95/46)[7] – especially when supplementary principles, commitments, and enforcement such as those under the Safe Harbour framework are taken into account.

On this basis, the European Commission should formally recognise that EU citizens are adequately protected when their personal data is transferred to the US. Such recognition would establish the most straightforward legal basis to sustain transatlantic data flows and mitigate the disruption of global commerce and cooperation that continues in the wake of the Schrems decision. Taking such a decision, however, requires a conscientious analysis of the law and practices in both the US and EU.

The detailed analysis below proceeds in three parts. First, the report reviews the "essentially equivalent" test under EU law to establish the analytical framework. Second, it compares the EU and US legal orders on government surveillance, which were central to the allegations influencing Mr. Schrems's complaint in Ireland. This comparison examines eight illustrative EU Member States as diverse and concrete examples of the operation of safeguards against abuse of surveillance powers under the EU legal order. These are Belgium, France, Germany, Ireland, Italy, the Netherlands, Poland, and the UK. The comparison shows that US surveillance of European personal data transferred to the US is not "mass and undifferentiated," and that the US safeguards are at least as strong as those in effect in the EU. Finally, the report explores the broad protection of data privacy in the commercial sector

[5] CJEU 6 October 2015, Case C-362/14, *Schrems*, ECLI:EU:C:2015:650.

[6] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000/520/EC), *OJ* 2000 L215/7.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 1995 L281/31, as amended.

under the US legal system, and assesses its alignment with principles of EU law applied in the Commission on the "adequacy" of third countries.

This review demonstrates that the legal orders for data protection in the EU and US are essentially equivalent. In brief, the report substantiates that:

> (a) notwithstanding differences in legal systems and aspects of data and privacy protection, there is a comprehensive system in the US to regulate and protect data privacy, particularly with regard to the most sensitive categories of personal data such as financial, medical, electronic communications, and children's data;
>
> (b) there is broad and effective public and private enforcement in the US with regard to data privacy in the commercial sector; and
>
> (c) there are substantial and effective safeguards, checks, balances, independent oversight and legal redress (including for EU citizens) applicable to electronic surveillance conducted by the US for national security and law enforcement purposes, and the applicable legal authorities and surveillance practices are at least as protective and focused as those under the EU legal order.

In all, there is a compelling – and at least sufficient – basis to find that the US legal order for privacy and data protection is essentially equivalent to that of the EU.

PART ONE:

The "essentially equivalent" test outlined by the CJEU calls for a thorough and balanced comparison of the legal order in both the EU and the US

It is important to be precise about what the CJEU's *Schrems* judgment held. The CJEU did not pass judgment on the Safe Harbour Framework itself, or even on the US data protection regime, but rather determined that the 2000 European Commission decision underlying the approval of the EU-US Safe Harbour decision failed to engage in a thorough enough analysis under EU law. This in turn resulted in the CJEU's invalidation of the decision approving the Safe Harbour Framework, which was designed to protect the data privacy rights of EU citizens whose data is transferred to the United States.

According to the CJEU, the Commission had failed in particular to establish that the level of protection of EU fundamental rights of privacy and data protection in the legal order of the United States is "essentially equivalent" to that guaranteed within the European Union. The CJEU decision and other CJEU rulings, together with case law of the European Court of Human Rights (ECtHR) that addresses surveillance by Member States, provide a legal framework for the analysis necessary to evaluate essential equivalence: a thorough and balanced comparison of both the law and practices in the respective compared jurisdictions. Part One of the report elaborates this framework under EU law.

The report examines the concrete ways in which the EU legal order protects the rights and freedoms of data subjects when measures are taken to pursue recognized public policy goals such as national security, for which EU Member States (rather than the EU itself) retain sovereignty. To establish an "EU Benchmark" by which to compare the equivalency of US law, the report uses four criteria, derived from both the CJEU and the ECtHR case law, that govern the discretion of EU Member States with respect to national and public security.

Finally, the report notes that application of the "essentially equivalent" test must take into account the commitments of the EU and its Member States under international trade laws. These commitments require that the EU and its Member States accord no less favorable treatment to US goods, US services, and US service providers than they accord other WTO members or Member States unless the discrimination can be justified as strictly necessary and proportionate for legitimate regulatory purposes.

The CJEU does *not* require that, to meet the "essentially equivalent" test, a level of protection be identical to that guaranteed in the EU legal order but, rather, that it be essentially equivalent in practice and effect, in substance rather than form. This focus on substance and effect provides the framework for analysis in the remainder of the report, which demonstrates that the US legal regime for privacy and data protection satisfies the necessary criteria.

PART TWO:

Comparison of the legal orders on government surveillance shows that US surveillance of European personal data transferred to the US is not "mass and undifferentiated" and is consistent with the legal order within the EU

Based on the principles enunciated in *Schrems* together with the decisions of the ECtHR relating to surveillance, the four main criteria to establish the EU Benchmark are the following:

1. *Specific legal authority.* Surveillance measures must be based on clearly stated legal authority. The legal bases or purposes for surveillance must be clearly spelled out. These purposes must be for legitimate aims of a serious nature with an objective reasonable basis in facts. There must be objective criteria by which to limit the discretion of authorities.

2. *Limited scope*. The amount of data collected or subject to retention requirements must not go beyond what is necessary to accomplish the purpose of the surveillance and cannot be generalised or indiscriminate. Discriminants (or particular search terms, "keywords", or "selectors" for surveillance purposes) must be established with due care and be consistent with the specified purposes for surveillance. The period of retention must be reasonable and finite.

3. *Oversight*. There should be some combination of executive, legislative, judicial, and expert oversight for approval and review of surveillance measures.

4. *Legal remedies and redress*. The public should be informed about surveillance laws and have some opportunity for access and rectification, and for judicial redress. If necessary for legitimate aims of surveillance, surveillance can be secret, in which event greater oversight or more general legal redress is necessary.

These criteria give substance to the principle of proportionality as implemented within the EU legal order. The application of this principle takes into consideration the "margin of discretion" granted to EU Member States by the ECtHR and the division of powers in the European Union. This discretion explicitly recognizes law enforcement needs and national security interests of the State pursuant to enduring Member State sovereignty.

Part Two of the report considers how the laws relating to government surveillance in each of the Illustrative Member States address the four criteria above. It is clear from this survey that the EU legal order on surveillance reflects variety and wide discretion as to the necessity of surveillance and the safeguards to limit interference with rights and freedoms.

Each of the Illustrative Member States authorizes various forms of surveillance by intelligence services in the interests of the State (*i.e.*, for the purposes of "national security" or "State security") and by the judicial system for criminal justice purposes (whether by intelligence services or law enforcement). For State interests, surveillance is authorized for electronic communications occurring both within and outside the jurisdiction of the Member State. The Illustrative Member States differ in the extent to which they specify and limit the purposes for implementing surveillance measures (with France having the most comprehensive list of State security interests that permit electronic surveillance). Several Illustrative Member States expressly authorise surveillance for the "economic interest" of the State.

Generally, the types of data covered by the surveillance laws of the Illustrative Member States are similar. In some of the Illustrative Member States, there are statutory distinctions among types of data. For example, four Illustrative Member States distinguish "metadata" from other types of data, allowing easier access to metadata.

All Illustrative Member States permit targeted surveillance, including targeted surveillance in order to prevent a crime that has not already been committed. The level of suspicion required to justify the surveillance varies among the Illustrative Member States, and in some cases is not explicitly provided for. In four of the Illustrative Member States, interception of communications that are not targeted at a specific individual or organization is permitted via use of keywords or other methods of filtering.

Provisions relating to the retention of data obtained by surveillance measures vary among the laws of the Illustrative Member States. Only three have prescriptive retention periods. Indeed, the majority of the Illustrative Member States still

prescribe the retention of data by telecommunications providers despite the CJEU finding Directive 2006/24/EC to be invalid. None of the surveillance laws of the Illustrative Member States contains detailed provisions on maintaining security of the data obtained via surveillance measures.

The oversight for approval and review of surveillance measures varies considerably among the Illustrative Member States. Whilst the majority have some combination of different degrees of executive, legislative, judicial or expert oversight, there are often specific exemptions to permit surveillance without prior authorization, only two require judicial authorization for intelligence surveillance, and most place such authorization in the hands of government ministers. As with oversight, the remedies and forms of redress available vary significantly among the Illustrative Member States. One commonality is that, for national security purposes, all Illustrative Member States allow restrictions on notifying data subjects that they are or have been the targets of surveillance, as well as on access to data by the targets of surveillance.

Part Two of this report also examines the corresponding provisions of the US legal order that authorise law enforcement and the intelligence agencies to conduct electronic surveillance, as well as the checks and balances in place to ensure that such surveillance is conducted only when necessary and in a proportionate manner. These laws and safeguards fall well within the range of discretion established by the EU Benchmark.

The US legal order embodies a robust system of checks and balances rooted in the US Constitution, which protects the right of the people to be free from unreasonable searches and seizures, which has been interpreted to protect “expectations of privacy” from government interference. These principles are thoroughly embedded in the checks and balances imposed on the powers of the US to conduct electronic surveillance. Indeed, in a 2014 decision involving digital information on a smart phone, the US Supreme Court denied the government access to the electronic data despite acknowledging its value to law enforcement because, in the words of the Chief Justice of the United States, “[p]rivacy comes at a cost.”

The report specifically describes the Wiretap Act, the Electronic Communications Privacy Act (ECPA), the Foreign Intelligence Surveillance Act of 1978 (FISA), and the USA PATRIOT Act (as amended recently by the USA FREEDOM Act), which authorise US intelligence agencies to intercept and collect the contents of communications and metadata.

These statutes, as described below in detail, actually prohibit the type of mass and indiscriminate surveillance feared by the CJEU in *Schrems*. To the contrary, these rules require both law enforcement and intelligence agencies to demonstrate a specific need for the information to be collected. The Wiretap Act and Title I of FISA, for example, require the government to demonstrate to an independent, neutral magistrate that it has “probable cause” to believe that the communications sought relate to criminal activity or foreign intelligence. Significantly, the relevant, neutral magistrate whose approval is required in each case is always a judge independent of the executive branch and, in the case of surveillance requests submitted by federal law enforcement or the intelligence agencies, a federal judge whose independence is further secured by holding life tenure. Section 702 of FISA, which authorises the

PRISM programme, and Section 215 of the USA PATRIOT Act likewise require the use of individualised selectors developed pursuant to court-approved processes.

The discussion further describes the safeguards and constraints in these legal authorities, including minimisation procedures that limit the retention and dissemination of collected communications, and it also highlights the additional protections and oversight mechanisms imposed by the President on the use of such power, including Executive Order 12,333 and Presidential Policy Directive/PPD-28. The latter order extends the privacy protections for Americans to citizens of all countries outside the US directing the Nation's intelligence agencies that "[a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information."

This legal order operates under comprehensive and elaborate constraints on the scope of the government's collection, retention, access, and use of individuals' private communications and data. These limitations include an outright ban on collecting communications to suppress speech or solely to benefit the economic interests of American corporations. They also impose temporal limits on surveillance authorisations, requiring the government to demonstrate any continuing need for previously approved information requests, and require data minimization and data security precautions to ensure that the information collected remains protected and respectful of privacy interests.

Moreover, various oversight bodies exist to monitor and police the limits placed upon the government. The most important of these groups is the federal judiciary, which has the power to hold surveillance activities to be unlawful – as it has done even in times of war. The executive branch too has significant internal compliance and auditing mechanisms in place, as well as embedded privacy and civil liberties officials and powerful and autonomous inspectors general. And Congress has also established powerful independent oversight bodies within the executive branch itself, including, most significantly, the Privacy and Civil Liberties Oversight Board, an independent agency with full access and subpoena authority, in addition to its own oversight role.

PART THREE:

A strong body of statutory law, common law, regulatory enforcement, litigation, and privacy and data protection practices, especially when coupled with binding adherence to EU data protection principles, ensure that EU citizens whose data is transferred to the US receive protection essentially equivalent to what they receive in the EU

Part Three of the report maps the US privacy protection regime to the EU's privacy principles. The Article 29 Working Party articulated the essential elements of Directive 95/46 as purpose limitation, data quality and proportionality, transparency, security, access and rectification, and restrictions on onward transfer. In addition to these principles, the report also assesses how the US legal order fulfils objectives of a data protection system to (i) deliver robust data protection compliance; (ii) provide support to individual data subjects in the exercise of their rights; and (iii) provide appropriate redress to the injured parties.

The common principles underlying the EU and the US data protection regimes are no accident. The development of both EU and US privacy and data protection law reflect historical cross-pollination of foundational concepts of liberty and human dignity, and principles of fair information practices in the modern era of computer processing. These are reflected in the legal orders of both jurisdictions.

US federal and state privacy laws, regulations, common law, and privacy practices on the ground establish a comprehensive privacy regime that aligns with EU law and meets the substance of Directive 95/46. The most sensitive data – such as financial, medical, health, electronic communications, and children's information – are protected by nearly two dozen federal sector-specific laws and numerous state laws. Almost all US states enforce broad data security and data breach notification laws that apply to sensitive personal data. These specific laws are backstopped by the broad reach of the Federal Trade Commission (FTC), which is the lead privacy enforcement agency in the US and exercises authority to protect consumers from unfair and deceptive practices or acts to regulate a broad range of activity involving data processing.

Companies that disregard the US privacy and data protection regime will face sanction on multiple, simultaneous fronts. US privacy and data protection laws are enforced by federal regulatory agencies, federal prosecutors, state Attorneys General and other state regulators. In addition to the FTC, federal enforcers are found in an expanding network of agencies with sector-specific expertise as well as in the US Department of Justice. Beyond federal powers, state law may afford data subjects regulatory protection and causes of action for legal redress. Many states have created formal units charged with privacy oversight. State Attorneys General often cooperate in joint enforcement actions against companies that experience data breaches or violate consumer privacy rights. Coordinated and comprehensive privacy regulation combined with active enforcement and sizable fines establish a strong deterrent to motivate compliance with US privacy and security requirements – perhaps even stronger than in the EU.

Assessing US privacy protections within the structure of EU data protection law is necessarily complex and challenging. But both systems are rooted in the adoption of the Fair Information Practice Principles. In some respects, such as data security and data breach notification, the US system may even be considered stronger; and – viewed as a whole and in substance rather than form – the US privacy regime is effectively consistent with the EU's.

The US system is designed to target, in particular, the protection of sensitive data, such as financial, health, electronic communications, and children's data, while providing a baseline of protections for all other types of data through the general enforcement authority of the FTC, state Attorneys General, and other federal and state regulators. This complex body of law includes, by way of example of sectoral laws, the Electronic Communications Privacy Act (ECPA) (governing electronic communications), the privacy provisions of the Communications Act (governing personal information maintained by telecommunications providers), the Computer Fraud and Abuse Act (CFAA) (protecting against computer crimes), the Children's Online Privacy Protection Act (COPPA) (governing the collection of personal data from children online and parental notice and consent), the Family Educational Rights and Privacy Act (FERPA) (governing educational records), the Fair Credit Reporting

Act (FCRA) (governing consumer reports including those used to make critical eligibility determinations), the privacy and security provisions (Title V) of the Gramm-Leach-Bliley Act (GLBA) (governing financial information), and the privacy and security provisions of and regulations issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA) (governing health and insurance information).

Enforcement by the FTC and by other public and private actors is authorised by, among other laws, Section 5 of the Federal Trade Commission Act (prohibiting unfair or deceptive business practices and which is used to enforce principles of notice and choice as well as reasonable information security practices), state "Little FTC Acts" or state "UDAP" statutes (which also prohibit unfair or deceptive acts and practices) and negligence or privacy torts under state law (including causes of action to recover for "public disclosure of private facts" and "intrusion upon seclusion"). With this flexible and dynamic regulatory structure and the growing privacy practices on the ground, the US privacy regime fulfils the promise of privacy and data protections that closely align with those in the EU.

A comprehensive review of the US privacy legal regime also must extend beyond laws on the books to include the prevailing practices that serve to protect privacy and data protection rights. Virtually all US companies engaged in online commerce post privacy policies to inform consumers of their data practices and privacy commitments. US industries have developed detailed codes of conduct and privacy principles (which often, when issued publicly, take on legally binding force) to guide the processing of personal data, increase data security, and establish greater transparency and control for data subjects. US companies are led by a contingent of increasingly respected and senior privacy professionals trained in data privacy and security with a growing share of budgetary authority.

The report furnishes a template and a resource for applying the CJEU's "Essentially Equivalent" Test and to make the findings required by the *Schrems* judgment in order to approve a new, strengthened transatlantic data transfer framework for companies that bind themselves to adhere to the basic principles of Directive 95/46. Similarly, it furnishes evidence on which in individual cases a data protection authority or national court can find that the level of privacy and data protection in the US is equivalent to that of a particular Member State.

PART ONE:

THE "ESSENTIALLY EQUIVALENT" TEST OUTLINED BY THE CJEU CALLS FOR A THOROUGH AND BALANCED COMPARISON OF THE LEGAL ORDER IN BOTH THE EU AND THE US

1.1 The CJEU's "Essentially Equivalent" Test Requires A Level Of Protection That Is Not Identical To That Guaranteed In The EU Legal Order But That Is Essentially Equivalent In Practice And Effect

In *Schrems*,[8] the CJEU articulated the "essentially equivalent" test for adequacy in interpreting Article 25(6) of Directive 95/46,[9] which enables the European Commission to find that a third country ensures an adequate level of data protection. The CJEU interpreted the meaning of the term "adequate" in Article 25 and applied this interpretation to the validity of the Commission's Safe Harbour Decision (2000/520/EC).[10]

Reading Article 25(6) of Directive as consistent with Article 8(1) of the Charter,[11] the CJEU construed this provision as "intended to ensure that the high level of that protection continues when personal data is transferred to a third country."[12] To achieve this purpose, the CJEU ruled:

> "The term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental freedoms that is essentially equivalent[13] to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter."[14]

---

[8] CJEU 6 October 2015, Case C-362/14, *Schrems*, ECLI:EU:C:2015:650.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 1995 L281/31, as amended.

[10] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000/520/EC), *OJ* 2000 L215/7 (hereinafter, Safe Harbour Decision).

[11] Charter of Fundamental Rights of the European Union, *OJ* 2012 C326/395.

[12] *Schrems*, para. 71.

[13] Versions of the *Schrems* judgment in other languages use different definitions of these terms, but only the English version is authentic because English was the language of the proceedings before the referring Court. *See* Rules of Procedure of the Court of Justice of 25 September 2012 (*OJ* 2012 L 265), as amended on 18 June 2013 (*OJ* 2013 L 173), Articles 37(3) and 41.

[14] *Schrems*, para. 73.

Given the large number of persons potentially affected by an Article 25(6) Decision, the Commission's review under the "essentially equivalent" test should be "strict."[15]

The CJEU explained this test for adequacy in terms that are especially relevant to the differences between the US and EU legal systems and the ways these systems address privacy and data protection. The CJEU made clear that the third country "cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order" and that "the means to which that third country has recourse … for the purpose of ensuring such a level of protection may differ from those employed within the European Union …."[16] The CJEU underscored this latitude by referring to paragraph 141 of the Advocate General's opinion,[17] which states that after a "global assessment" the Commission can find a third country's level of protection adequate "even though the manner in which that protection is implemented may differ from that generally encountered within the European Union."[18]

Rather than dwell on differences in form, the CJEU focused on the substance of the protection. In assessing adequacy, the Commission must focus not only on "the content of the applicable rules in that country resulting from its domestic law or international commitments," but also on "the practice designed to ensure compliance with those rules."[19] Different means of protection may be found adequate if they "prove, *in practice*, effective" to ensure essentially equivalent protection.[20]

The Court also ruled that the Commission must "check periodically" whether the finding of adequacy is "still factually and legally justified,"[21] taking account of "the circumstances that have arisen after that decision's adoption."[22]

1.2 The CJEU Holds That The Safe Harbour Decision Should Have Contained Findings And Statements On The Limitations To US Surveillance, But Itself Makes No Such Assessment

Having articulated what is required to determine the adequacy of data protection in a third country under Article 25(6), the CJEU then turned to assess whether the Commission's Safe Harbour Decision met these requirements. To understand how the CJEU's judgment should be applied in future decisions under Article 25(6), it is important to analyse precisely what the CJEU did decide, and what it did not decide.

---

[15] *Id.* para. 78.

[16] *Id.* para. 74.

[17] Opinion of A-G Bot of 23 September 2015, Case C-362/14, ECLI:EU:C:2015:627.

[18] *Id.* para. 141.

[19] *Schrems*, para. 75.

[20] *Id.* para. 74 (emphasis added).

[21] *Id.* para. 76.

[22] *Id.* para. 77.

Because the CJEU's authority under Article 267 of the Treaty on the Functioning of the European Union (TFEU) is limited to answering questions regarding the interpretation and validity of EU laws presented to the CJEU by EU Member State courts, the CJEU did not engage in any fact-finding of its own. The CJEU did not reach any conclusions regarding the US legal order or the extent to which that legal order lacks rules "intended to limit any interference" with data privacy rights.[23] Instead, the CJEU found that Decision 2000/520/EC and the Commission's subsequent review of the Safe Harbour Framework failed to address these questions.[24]

Thus, the CJEU simply concluded that the Commission had failed to meet its burden under Article 25(6). As the Court articulated this burden in paragraph 96, the Commission "must find, duly stating reasons" that a third country in fact meets the "essentially equivalent" test.[25] The Commission failed to do so because it "*did not state*, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments."[26]

More specifically, Annex I to the Safe Harbour Decision provided that "the applicability of the safe harbour principles may be limited … to the extent necessary to meet national security, public interest, or law enforcement requirements,"[27] paralleling the derogation in Articles 3(2) and 13 of Directive 95/46/EC. According to the CJEU, this limitation in the Safe Harbour Decision "enables interference" with fundamental rights of EU data subjects, yet the decision *does not contain any finding* regarding the existence of rules adopted by the United States intended to limit any interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security,"[28] nor does the decision "refer to the existence of effective legal protection against interference of that kind."[29]

In addition, against the background of the CJEU's conclusion that the Commission must check periodically whether its finding of adequacy is "still factually and legally justified,"[30] the CJEU also took note of the Commission's communications regarding review of the Safe Harbour Framework in 2013.[31] The Court did not draw any

---

[23] *Id.* para. 88.

[24] *Id.* paras. 88–89.

[25] *Id.* para. 96.

[26] *Id.* para. 97 (emphasis added).

[27] Safe Harbour Decision (2000/520/EC), *OJ* 2000 L215/7, Annex I.

[28] *Schrems*, para. 88 (emphasis added).

[29] *Id.* para. 89.

[30] *Id.* para. 76.

[31] *Id.* para. 90. *See also* "Rebuilding Trust in EU-US Data Flows, accompanied by the "Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection

explicit conclusions from this reference, but the implication is that the Commission should have taken some further decision with regard to the Safe Harbour Framework in response to its review.

It is because of this absence of findings and statements in the Safe Harbour Decision that the CJEU held that the Safe Harbour Decision is invalid "without there being any need to examine the content of the safe harbour principles."[32] It is essential to recognise that, while the CJEU set out general principles for the "level of protection … within the European Union" in paragraphs 91 to 95 of its judgment, it did not undertake any comparison with the US and thus provides no conclusion as to whether US laws in force today are "essentially equivalent" to the level of protection guaranteed in the EU legal order today.[33]

That comparison is a task that will have to be carried out by the European Commission for an Article 25(6) decision on any new transatlantic data transfer framework. A similar comparison[34] will have to be carried out by DPAs faced with a claim from a data subject about infringement of their rights and freedoms in relation to a transfer of their personal data to the US, or a request from a company submitting transfer instruments to a DPA for approval under national laws implementing Directive 95/46.

1.3 To Apply The "Essentially Equivalent" Test, The Full EU Benchmark Must Be Established, Taking Account Of The Boundaries Of The EU Legal Order, The Margin Of Discretion Granted To EU Member States, And International Trade Law Obligations

The comparison that the *Schrems* judgment now demands of the Commission and DPAs calls for measuring the rules and practices in a third country against the "level of protection … within the European Union" or "in the EU legal order."[35] This comparison cannot be carried out without establishing what is the level of protection

---

(COM(2013)846 final, discussed in *Schrems*, paragraphs 11–16) and the Commission Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM (2013)847 final, discussed in *Schrems* paragraphs 17–25).

[32] *Schrems*, para. 98.

[33] *Id.* para. 96.

[34] As discussed in Section 1.4.2 below, the "essentially equivalent" test can yield different results depending on the entity carrying out that test and the Member States involved.

[35] There is no indication in the *Schrems* judgment that the terms "in the EU legal order" and "within the European Union" have a different meaning. Both terms presumably refer to the concept of the (E)EC/EU legal order established by the Treaties, ("ordre juridique"), which is separate from the legal orders of the Member States. This concept was established in Case 6/64, *Costa v. ENEL*, ECLI:EU:C:1964:66, ECR p. 1160, and recalled in Opinion 2/2013, ECLI:EU:C:2014:2454, para. 157: "As the Court of Justice has repeatedly held, the founding treaties of the EU, unlike ordinary international treaties, established a new legal order, possessing its own institutions, for the benefit of which the Member States thereof have limited their sovereign rights, in ever wider fields, and the subjects of which comprise not only those States but also their nationals (see, in particular, judgments in *van Gend & Loos*, 26/62, ECLI:EU:C:1963:1, p. 12, and *Costa v. ENEL*, 6/64, ECLI:EU:C:1964:66, p. 593, and Opinion 1/09, ECLI:EU:C:2011:123, para. 65)."

in the EU legal order. Otherwise there can be no benchmark by which to judge the level of data protection in a third country.

In the *Schrems* judgment, the CJEU laid out basic principles under its jurisprudence that have to be met by the European Union when it promulgates legislation that enables interference with fundamental rights.

However, these principles do not go beyond stating that *some* standards and limitations need to be set, and that the principles of necessity and proportionality must be respected. The CJEU did not address fully the boundaries of the "EU legal order" and the limits it places on various institutions.

In particular, the CJEU did not address the margin of discretion granted to EU Member States when they engage in the difficult exercises of balancing fundamental rights to privacy with possibly conflicting interests requiring free movement of data[36]; when they balance fundamental rights with pursuing "legitimate objectives, such as national security"[37]; or when they balance fundamental rights with measures taken in the "fight against international terrorism in order to maintain international peace and security" or the "fight against serious crime in order to ensure public security."[38] In this respect, it may be noted that the CJEU recalled in *Digital Rights Ireland* that Articles 7 and 8 of the Charter do not contain all the fundamental rights that are relevant here. The Charter also contains Article 6 which "lays down the right of any person not only to liberty, but also to security."[39]

The international trade law obligations of the EU and its Member States are another part of the EU legal order that affects how third countries are treated. The CJEU did not address the impact of these obligations on third country adequacy determinations.

This section reviews the principles of EU law set out in the *Schrems* judgment as well as these additional dimensions, including the standards for Member States set out in the case law of the European Court of Human Rights (ECtHR) and the boundaries of the EU legal order, including international trade law. Taken together, these bodies of law establish the "level of protection of fundamental rights … in the EU legal order" (the EU Benchmark).

1.3.1 The CJEU's Basic Principles Of Protection For Fundamental Rights And Freedoms

The CJEU laid out five basic principles in paragraphs 91 to 95 of the *Schrems* judgment. These principles are binding on the European Union when it takes action. As discussed in more detail below Part 1.3.2, these principles are not automatically

[36] *Schrems*, para. 42.

[37] *Id.* para. 88.

[38] CJEU 8 April 2014, Joined Cases C-294/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, para. 42. (*Digital Rights Ireland*).

[39] Article 6 of the Charter reads as follows: "Everyone has the right to liberty and security of person."

transferable to Member State laws, given that these states retain significant sovereignty in matters of national security, and the European Union must respect their laws regarding public security. They are applicable to Member States when they implement Union law, so that they would apply where DPAs act under Article 28 of Directive 95/46, which obliges DPAs to investigate claims from individuals regarding the lawfulness of data processing under national laws to protect recognised public policy goals such as national security allowed for in Article 13 of Directive 95/46.

First Principle*: *Clear And Precise Rules Imposing Minimum Safeguards Against Risks Of Abuse And Unlawful Access by Public Authorities

In paragraph 91, the CJEU held that EU legislation enabling interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter "must lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards …." The purpose of this precision and safeguards is to protect "against the risk of abuse and against any unlawful access and use of that data."[40] The Court added that "[t]he need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data."[41]

This first principle is largely procedural, focused on the quality of laws. The principle does not address the substantive standards contained in such rules and safeguards.

Second Principle*: *At The EU Level, Derogations And Limitations to Protection Must Apply Only In So Far As Is Strictly Necessary

In paragraph 92, the CJEU held that "protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary." This is a general reference to the principles of necessity and proportionality, which can be applied to a specific situation only once a particular policy aim has been determined, and the measures to attain that aim are assessed. Part 1.3.3 below discusses the more detailed rules for assessing proportionality in individual situations set out in the case law of the ECtHR.

Third Principle*: *Storage Of All The Personal Data Of All Persons Whose Data Has Been Transferred, Without Any Differentiation, Limitation, Or Exception And Without Objective Criteria To Limit Public Authorities' Access To Data Or Subsequent Use, Would Be Disproportionate

Building on its application of the principle of proportionality in *Digital Rights Ireland*, the CJEU stated in paragraph 93 that mass storage of data without any limitations regarding public authorities' access or subsequent use would be disproportionate:

[40] *Schrems*, para. 91.

[41] *Id.*

> "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail."

The CJEU cited *Digital Rights Ireland* to the same effect and, in fact, substantially paraphrased that judgment in the language above.[42] The statement packs together a number of elements that also incorporate aspects of other principles: (1) "storage of *all* the personal data of *all* the persons" whose data is transferred; (2) the absence of "any differentiation, limitation or exception being made in light of the objective pursued," which closely resembles the second principle above; (3) the absence of "an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use," which parallels the first principle; and (4) "for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail."

This third principle provides a "checklist" of the types of minimum limitations or safeguards on interference with data protection rights that must be put in place. A similar checklist appears in the political agreement on the General Data Protection Regulation.[43]

***Fourth Principle*: Public Authorities Must Not Have Access To Personal Data On A Generalised Basis**

In paragraph 94, the CJEU held that "[i]n particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic

[42] The CJEU used almost identical terms in separate paragraphs in *Digital Rights of Ireland,* holding that it would be disproportionate to retain, "in a generalized manner, all persons and all means of electronic communications as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime," *id.* para. 57; any "substantial and procedural conditions relating to the access of the competent national authorities to the data and their subsequent use," *id.* para. 60; "any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued," *id.* para. 62; or any "prior review carried out by a court or an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary," *id.*

[43] Interinstitutional File 2012/0011 (COB), No. 15039/15, 15 December 2015. See Article 21(2) of the Draft Data Protection Regulation (corresponding to Article 13 of Directive 95/46), which provides that Union or Member State law which restricts the scope of data privacy rights on recognised public policy grounds must "contain specific provisions at least, where relevant, as to the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the safeguards to prevent abuse or unlawful access or transfer; the specification of the controller or categories of controllers, the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing and the risks for the rights and freedoms of data subjects; the right for data subjects to have a general indication about the restriction, unless this may be prejudicial to the purpose of the restriction."

communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."

This fourth principle follows logically from *Digital Rights Ireland.* It provides that public authorities' access to personal data must not be unlimited; there cannot be "generalised" access to "all" data stored of "all persons whose data is transferred."[44]

Fifth Principle: ***There Must Be Some Possibility For An Individual To Pursue Legal Remedies Permitting Access, Rectification Or Erasure Of Personal Data***

In paragraph 95, the CJEU held that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."

Thus, the fifth principle obliges the EU, when it promulgates EU laws that enable interference with fundamental rights, to ensure that data subjects can have access to a tribunal to submit claims of violation of their fundamental rights.

Such rights to redress are not absolute.[45] As discussed in Part 1.3.2 below, Article 13 of Directive 95/46 permits Member States to take measures limiting the right of data subjects to be informed of data processing and limiting their rights to access their personal data in a number of circumstances, including where such limitations are necessary and proportional to protect national or public security.

1.3.2 The EU Legal Order Respects Member State Sovereignty in Setting Security And Other Recognised Public Policy Aims, Requiring Only That Measures Interfering With EU Rights Are Necessary And Proportionate

Establishing the EU Benchmark requires scrutiny of the division of powers between EU and its Member States, and of the interaction of the Charter and the Treaty on European Union.

Both *Digital Rights Ireland* and *Schrems* concerned laws promulgated by the EU legislator (Directive 2006/24/EC and Decision 2000/520/EC, respectively). Therefore, the Charter was directly relevant to the application and interpretation of these two instruments of EU law, pursuant to Article 51 of the Charter, which provides that "the provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union." As clarified by *Schrems*,[46] EU legislation must be fully compliant with the Charter.

---

[44] *Schrems*, para. 94.

[45] Generally, as the CJEU noted in its Grand Chamber judgment of 9 November 2010 in Cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraph 48: "the right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society (see, to that effect, Case C-112/00 *Schmidberger* [2003] ECR I-5659, paragraph 80 and the case-law cited)".

[46] *Schrems*, para. 91.

By contrast, Member States are bound to the Charter "only when they are implementing Union law" as provided in Article 51[47] of the Charter and CJEU Opinion 2/13.[48] The Charter is not applicable outside of the bounds of EU law.

In turn, the protection of national security is substantially outside the bounds of EU law. Pursuant to Article 4(2) of the Treaty on European Union, the EU must respect each Member State's "essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State." The CJEU has itself recognized that each Member State has retained the freedom to determine the requirements of public policy and public security in accordance with its own sovereign needs.[49]

The exercise of this freedom is subject to limits where Member State measures interfere with rights derived from the EU legal order, including free-movement rights and fundamental rights. Such interfering measures are subject to certain conditions laid down in the case law. They must be (i) applied in a non-discriminatory manner, (ii) justified by overriding requirements of public policy or public security, (iii) suitable for securing the attainment of the aim they pursue, and (iv) proportionate, *i.e.*, they do not go beyond what is necessary to attain the stated aim.[50] The last of these conditions – proportionality – is the most important in practice since, in matters of surveillance, the necessity of measures to protect national security or public safety is often assumed.[51] *Schrems* and *Digital Rights Ireland* clearly strengthen these limits, but they do not alter the contours of the EU legal order.

In its treatment of Member State essential functions, Directive 95/46[52] follows these contours: Member States set their policy goals, and EU law sets limits only to judge the necessity and proportionality of interference with rights derived from EU law:

- Article 3(2) confirms the primacy of Member States to make public policy choices: "This Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law … and in any case to processing operations

[47] Article 51 of the Charter provides: "(1) The provisions of this Charter are addressed to the institutions … of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties. (2) The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties."

[48] CJEU 18 December 2013, Opinion 2/13, ECLI:EU:C:2014:2454, para. 102.

[49] *See e.g.*, CJEU 10 July 2008, C-33/07, *Ministerul Administraţiei v. Jipa*, ECLI:EU:C:2008:396, para. 23.

[50] *Id.*

[51] *See, e.g.*, *Digital Rights of Ireland*, paras. 42–49.

[52] This approach is maintained in the political agreement on the General Data Protection Regulation. *See supra* note 43, at art. 21.

concerning public security, defence, State security … and the activities of the State in areas of criminal law."

- Article 13 lays down a necessity-and-proportionality test: "Member States may adopt legislative measures to restrict the scope of [data protection] when such a restriction constitutes a *necessary measure* to safeguard (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, … [and] (g) the protection of the data subject or of the rights and freedom of others."

The latitude that Member States enjoy under the EU legal order is enlarged by the comity that EU Member States must accord one another under the EU legal order. As noted by the CJEU in Opinion 2/13, "the principle of mutual trust" requires Member States "to consider all the other Member States to be complying with EU law and particularly with the fundamental rights recognised by EU law."[53] Accordingly, Member States may not "demand a higher level of national protection of fundamental rights from another Member State than that provided by EU law," nor may they "check whether that Member State has actually, in a specific case, observed the fundamental rights guaranteed by the EU."[54]

The principle of mutual trust also is reflected in Directive 95/46. Recital 3 to Directive 95/46 declares that "personal data should be able to flow freely from one Member State to another" and, while Article 25 provides that Member States must verify the level of protection in a third country before permitting data transfers, no such verification is required for transfers within the EU. As a result, data subjects in the EU are not protected against transfers to Member States whose surveillance laws may not meet the principles outlined in *Schrems* or ECtHR standards discussed below.[55]

Arguably, the "essentially equivalent" test would go beyond the boundaries of the EU legal order to the extent it includes areas of law such as national security that are not part of EU law. Directive 95/46 nevertheless provides a basis to invoke EU law: the reference to "national security" in Article 13 above, read in conjunction with Article 28, which states that DPAs shall "hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply."

It follows that, with respect to national security, the rights of EU data subjects within the EU may be limited on the grounds set out in Article 13 of Directive 95/46, and the main guarantee that data subjects have is that the "legislative measures to restrict the scope" of their rights must be "necessary" and proportionate. Rights of legal

[53] CJEU, Opinion 2/13, para. 191.

[54] *Id.*

[55] This does not mean that Member States can infringe fundamental rights without being challenged. For example, if Member State A considers that Member State B fails to fulfill its obligations under the TFEU (including failures to respect fundamental rights protected by EU law), Member State A can commence infringement proceedings before the CJEU or request the Commission do so.

redress may be limited in practice, as well, since Article 13 permits Member States, where necessary, to limit the right of the data subject to be informed of the processing of his or her data and to have access to that data. These limits make up part of the EU Benchmark.

1.3.3 ECtHR Case Law Confirms That Member States Have A Margin Of Discretion That Depends On The Degree Of Consensus Among ECHR Member States, And That EU Member States Comply With The Charter When They Stay Within This Margin Of Discretion

The EU legal order also is shaped by the European Convention on Human Rights (ECHR).[56] The case law of the ECtHR clarifies and supplements the case law of the CJEU, and informs the interpretation and application of the Charter by EU institutions and by Member States. The key provision in this respect is Article 52 of the Charter, which provides that "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the scope of those rights shall be the same as those laid down by the said Convention."[57]

The CJEU has confirmed in a number of judgments that the interpretation of concepts in the Charter and interpretation of corresponding concepts by the ECtHR are the same. In *Digital Rights Ireland*, the CJEU quotes ECtHR case law several times – in defining the terms "interference with a fundamental right"[58]; the need for clear and precise rules,[59] especially in case of automatic processing; and, crucially, in setting the standard for judicial review of compliance with the principle of proportionality and the margin of discretion ("the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference").[60]

Thus, ECtHR case law helps to clarify and supplement the CJEU case law on the scope of rights and the boundaries of the EU legal order. The ECtHR case law quoted in paragraph 54 of *Digital Rights Ireland* clarifies reasons for the *Schrems* principle that laws must be clear and precise. For example, the ECtHR has repeatedly stated that a law which interferes with fundamental rights "must enable

---

[56] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Rome, 4.XI.1950, available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[57] Charter, at art. 52.

[58] *Digital Rights Ireland*, para. 35 (citing ECtHR 26 March 1987, *Leander v. Sweden*, ECLI:CE:ECHR:1987:0326JUD000924881, § 48; ECtHR 4 May 2000, *Rotaru v. Romania,* ECLI:CE:ECHR:2000:0504JUD002834195, § 46; and ECtHR 29 June 2006, *Weber & Saravia v. Germany* (admissibility decision), ECLI:CE:ECHR:2006:0629DEC005493400, § 79).

[59] *Id.* para. 54 (citing ECtHR 1 July 2008, *Liberty & Others v. United Kingdom*, ECLI:CE:ECHR:2008:0701JUD005824300, §§ 62 & 63; *Rotaru*, §§ 57–59; ECtHR 4 December 2008 [GC] *S. & Marper v. United Kingdom*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99).

[60] *Id.* para. 55 (citing *S. & Marper*, § 102).

the individual to regulate his conduct" (for example to avoid being subject to the interference).[61]

The ECtHR case law quoted in paragraphs 54 and 55 of *Digital Rights Ireland* confirms that ECHR Member States have the power to interfere with fundamental rights on recognized public policy grounds to ensure the security of their population, provided such interference does not go beyond what is "necessary in a democratic society." In turn, these Member States have a margin of discretion to decide what is necessary in their democratic society.

The width of this margin depends greatly on the degree of "consensus" among the Member States on a given issue. This degree of consensus is generally determined by comparing the laws of the ECHR Member States.[62] When there is wide divergence among the Member States' laws as shown in Part 2.1, each Member State will have a significant margin of discretion. As the ECtHR put it, "where there is no consensus … either as to the relative importance of the interest at stake or as to the best means of protecting it, the margin will be wider."[63]

Given the importance of the ECtHR's case law on surveillance, the key judgments are recalled here. The starting point for analysing the ECtHR case law on government surveillance is Article 8 ECHR, which provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The seminal judgment of the ECtHR dealing with the compatibility of secret electronic surveillance with Article 8(2) ECHR is *Klass & Others v. Germany*,[64] in which the Plenary Court ruled that EU Member States "must be able" to undertake secret surveillance of "subversive elements" to counter threats to the security of their citizens effectively.[65] Member States have a "certain discretion" to choose the forms

---

[61] This principle of "foreseeability" does not mean that individuals need to know when governments would intercept their communications. It only relates to the *circumstances* in which governments might intercept their communications. *See Weber & Saravia*, § 93; *Leander*, § 51).

[62] See, *e.g.*, *S. & Marper*, §§ 45–49, in which the ECtHR proceeds to analyse the laws regarding the compulsory taking of fingerprints in all of the Council of Europe member States.

[63] *See id.* § 102. Similar wording has been used in a series of cases since ECtHR 4 December 2007 [GC], *Dickson v. United Kingdom*, ECLI:CE:ECHR:2007:1204JUD004436204, § 78.

[64] ECtHR [Plenary Court] 6 September 1978, *Klass & Others v. Germany*, ECLI:CE:ECHR:1978:0906JUD000502971.

[65] *Id. §* 48. See also Article 4(2) TEU, Article 8 ECHR, Article 52 Charter, Articles 3(2) & 13 of Directive 95/46, and, most recently, ECtHR 12 January 2016, Application No. 37138/14, *Szabó &*

of surveillance to counter such threats, and the ECtHR stated specifically that it is "not for the Court" to determine the best policy.[66] To ensure that the infringements upon data privacy rights do not go beyond what is "necessary in a democratic society," a Member State must put in place sufficient safeguards against abuse.[67] In *Klass,* the ECtHR confirmed that ideally oversight should be carried out by a judge, but a committee of parliament with broad enough representation could be considered sufficiently independent.[68]

In *Weber & Saravia v. Germany,* the ECtHR once again reviewed the German G10 law, but this time with regard to "strategic monitoring,"[69] which was distinguished from "individual monitoring," *i.e.*, monitoring of individuals who "suspected of planning or having committed" certain grave offences.[70] Strategic monitoring was done using "catchwords," with interception limited to persons who "had to have used catchwords capable of triggering an investigation into the dangers listed in section 3(1)," which include an armed attack, terrorism, trafficking in arms and certain sensitive technology, imports of substantial quantities of drugs, counterfeiting of money and money laundering; or persons who "had to be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoids such dangers."[71]

In ruling that the case against Germany was inadmissible, the *Weber* court confirmed that Member States have a "fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security," and that

---

Vissy v. Hungary, ECLI:CE:ECHR:2016:0112JUD003713814, § 68 ("[I]t is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents.") , and § 80, in which the *Szabó* Court confirms that the observations made in § 48 of *Klass v. Germany* "are equally valid in the present case."

[66] *Klass*, § 49 (collecting further references), confirmed in ECtHR 4 December 2015 [GC], *Roman Zakharov v. Russia*, ECLI:CE:ECHR:2015:1204JUD004714306, § 232. *See also* ECtHR Research Division, National Security and European Case-Law, 2013, p. 4 ("Member States are recognized to have certain – even a large – measure of discretion when evaluating threats to national security.").

[67] See the minimum safeguards formulated in *Szabó*, § 56: "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed."

[68] *Klass*, § 56.

[69] *See Weber & Saravia,* § 4 ("Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany ….").

[70] *Id.* ("In contrast, so-called individual monitoring, that is, the interception of telecommunications of specific persons, serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed.").

[71] *Id.* § 97.

"adequate and effective guarantees against abuse" were in place in Germany "to ensure that measures were not ordered haphazardly, irregularly or without due and proper consideration."[72] These guarantees included prior authorisation of interception requests by the President of the Federal Intelligence Service – an executive branch official – and the G10 commission; limitations on further use; provisions on destruction of data that were no longer needed; and notifications to data subjects in certain cases.[73]

In *Liberty & Others v. United Kingdom*, the ECtHR dealt with the UK government's access to "all commercial submarine cables having one terminal in the UK and carrying external commercial communications in Europe" so that "any person who sent or received any form of telecommunication outside the British Islands … could have had such a communication intercepted."[74] The key issue was not that the government had the technical ability to intercept communications; rather, it was that the "legal discretion to the executive for the physical capture … was virtually unfettered,"[75] whilst the arrangements "to safeguard against abuse of power" were "not contained in legislation or otherwise made available to the public."[76]

Notably, the applicant mentioned the United States as an example of a country that had published "detailed information" on systems similar to the UK arrangements "for filtering and disseminating intercepted material."[77] The *Liberty* court in turn referred to the German G10 Act as an example of a system that provides a higher level of foreseeability by providing that monitoring could be carried out "only with the aid of search terms which served … the investigation of the dangers described in the monitoring order …."[78]

In *Klass,* the ECtHR stated that it will generally trust Council of Europe member States to abide by their laws,[79] but "the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system."[80] Therefore, the more "prone to abuse" a surveillance method, the higher

---

[72] *Id.* § 115.

[73] The German Constitutional Court noted that "in cases in which data were destroyed within three months there was justification for never notifying the persons concerned … if the data had not been used before their destruction." *Id.* § 136.

[74] *Liberty*, § 64.

[75] *Id.*

[76] *Id.* § 66.

[77] *Id.* § 45.

[78] *Id.* § 68.

[79] See *Klass*, § 59. See also Opinion 2/13, para. 192: " Member States … may … not demand a higher level of national protection of fundamental rights from another Member State than that provided by EU law, but, save in exceptional cases, they may not check whether that other Member State has actually, in a specific case, observed the fundamental rights guaranteed by the EU."

[80] *Klass*, § 59.

the requirements will be in terms of *ex ante* authorisation by a court or independent body, *ex post* oversight, and measures to prevent unwarranted use of data.[81]

With regard to legal redress, the ECtHR has recognised since *Klass* that secret surveillance can work only when it is secret: "the fact of not informing the individual … is this very fact which ensures the efficacy of the 'interference.'"[82] Therefore, direct legal redress will be available "only in exceptional cases."[83]

The assessment of surveillance methods in EU Member States based on this case law requires a holistic view of both the surveillance methods, the safeguards against abuse, and remedies provided by national law. This holistic view was explicitly mentioned in *Klass*[84]; in *Weber*[85]; and more recently in *Kennedy v. United Kingdom*: "The assessment depends on *all the circumstances of the case*, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."[86]

The need for a holistic view of the threat, the surveillance methods, and the safeguards has been confirmed in the two most recent judgments of the ECtHR: the Grand Chamber judgment of 4 December 2015 in *Roman Zakharov v. Russia*, and the judgment of 16 January 2016 in *Szabó & Vissy v. Hungary*.

In *Zakharov,* the ECtHR Grand Chamber dealt with technical measures granting intelligence services direct access to the content of all mobile phone communications. The ECtHR noted several factors created risks of abuse, including authorities having "an almost unlimited degree of discretion in determining which events or acts constitute […] a threat"[87]; the absence of rules on discontinuation of intelligence surveillance when no longer necessary[88]; and shortcomings in the system of prior authorisation by judicial authorities, which were deprived of the power "to assess whether there is a sufficient factual basis to suspect the person," and were not instructed "to verify the existence of a "reasonable suspicion." In addition,

---

[81] *See* ECtHR 4 December 2015 [GC], *Roman Zakharov v. Russia*, ECLI:CE:ECHR:2015:1204JUD004714306, §§ 269–71 (discussing broad access to mobile telecommunications); *Szabó & Vissy*, § 73.

[82] *Klass*, § 58.

[83] *Id.* § 70. Germany did, however, provide the possibility of complaining to the G10 Commission, *id.* § 21, and obtaining review by the Constitutional Court, which is able to decide if national security permits communication of information to the data subject, *id.* § 23.

[84] *Klass*, §§ 49–50.

[85] *Weber & Saravia*, § 106.

[86] ECtHR 18 May 2010, *Kennedy v. United Kingdom*, Application No. 26839/05 [2010] ECHR 682, § 153 (emphasis added). The need for assessing all the measures of a Member State as a whole was confirmed again in *Zakharov*, § 232, and in *Szabó & Vissy*, § 57.

[87] *Zakharov*, § 248.

[88] *Id.* § 251.

the authorities had "an unlimited degree of discretion" to use an "urgent procedure," which provided for *ex post* review by a court, but without the power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained … is to be kept or destroyed."[89] In view of these shortcomings, the ECtHR ruled that the system was "prone to abuse" and decided to "examine with particular attention whether the supervision arrangements … are capable of ensuring that all interceptions are performed lawfully."[90]

The supervision arrangements, however, were not adequate. First, intercepting agencies were not obliged to keep records,[91] and with the exception of the initial authorisation, all supervision was kept within the executive branch of government, or involved prosecutors who were not sufficiently independent[92] and did not have full access to documents. In addition, interceptions would be inspected only in case of a complaint.[93] Finally, the subjects of interception were deprived "of the effective possibility of challenging interceptions retrospectively."[94] In its conclusions, the ECtHR noted that "the shortcomings in the legal framework … appear to have an impact on the actual operation of the system of secret surveillance …. The examples submitted … indicate the existence of arbitrary and abusive surveillance practices, which appear to be due to the inadequate safeguards provided by law."[95] In this respect, the Court referred to reports about surveillance information sold in return for bribes.[96] The overall conclusion was that the system did not meet the "quality of law" requirement as it was incapable of keeping the "interference" to what is "necessary in a democratic society."[97] The *Zakharov* judgment closely followed the reasoning in previous cases. One noteworthy statement, however, is that notification of surveillance following the termination of surveillance did not necessarily include situations where "data are deleted" without being used.[98]

The most recent judgment is *Szabó*, which dealt with the secret intelligence powers of Hungary's Anti-Terrorism Task Force permitting a far-reaching combination of surveillance measures, including "secret house search and surveillance with recording, opening of letters and parcels, as well as checking and recording the contents of electronic or computerized communications, all this without consent of

---

[89] *Id.* § 266.

[90] *Id.* § 271.

[91] *Id.* § 272.

[92] *Id.* § 280.

[93] *Id.* § 281.

[94] *Id.* § 300.

[95] *Id.* § 303.

[96] *Id.* § 197.

[97] *Id.* § 236.

[98] *Id.* § 287.

the persons concerned."[99] For intelligence surveillance (Section 7/E3 surveillance), the exercise of these powers was subject to "the condition that the necessary intelligence [could not] be obtained any other way. Otherwise, the law does not contain any particular rules on the circumstances in which this measure can be ordered."[100] Decisions authorising such surveillance were provided within the executive branch of government, and could be ordered for "person(s) concerned identified by name or as a range of persons, and/or any other information capable of identifying such person or persons."[101] The ECtHR expressed concern about "the absence of any clarification" as to how this category "is to be applied in practice," and the Court considered the category "overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons 'concerned' and the prevention of any terrorist threat."[102]

In Section 73, the ECtHR stated that "a measure of secret surveillance can be found in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation." It must be noted that these criteria are not self-standing criteria that, on their own, can lead to the ECtHR condoning or condemning a national system. First, in the same Section 73, the ECtHR noted that a measure that does not correspond to these criteria will be "prone to abuse," and, as noted in *Zakharov*, this means that the safeguards must be assessed with "particular attention."[103] Second, in the same section, the ECtHR noted the absence of prior judicial authorisation in Hungary, which would have served "to limit the law enforcement authorities in interpreting the "broad terms" mentioned above. Third, there were insufficient additional safeguards to prevent abuse. To the contrary, surveillance warrants could be repeatedly prolonged[104] (§ 74); supervision was "eminently political"[105] (§75); surveillance had "never been subjected to judicial control"[106] (§76); and reporting obligations to a parliamentary committee did not convince the ECtHR "that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance," especially since "it does not appear that the committee has access in detail to relevant documents."[107] (§82). Finally, there was no "subsequent notification of surveillance measures" that could have

[99] *Szabó*, § 9.

[100] *Id.* § 12.

[101] *Id.* § 17 (quoting Section 57 of the Act no. CXXV of 1995 on the National Security Services).

[102] *Id.* § 67.

[103] *See also id.* § 78.

[104] *Id.* § 74.

[105] *Id.* § 75.

[106] *Id.* § 76.

[107] *Id.* § 82.

contributed to the effectiveness of remedies.[108] Given the absence of any effective remedial measures, the Court concluded that there had been a violation of Article 8 ECHR.

It follows from the above that there is no single recipe of oversight measures that can ensure necessity and proportionality for all secret surveillance measures. And indeed, as set out in more detail in Part 2.1, EU Member States have chosen widely varying rules for secret surveillance.

Based on the requirement in Article 52(3) of the Charter that the scope of rights under the Charter shall be "the same" as those laid down in the Convention, it stands to reason that the margin of discretion under the Charter must be the same as the margin of discretion set out in the ECtHR case law.[109] In this respect it is worth noting that the draft General Data Protection Regulation, as it currently stands, rephrases the proportionality test in terms very similar to those used by the ECtHR: "a necessary and proportionate measure in a democratic society to safeguard" recognised public policy goals.[110]

Therefore, the EU Benchmark must reflect that Member States comply with the Convention and the Charter when they stay within the margin of discretion permitted under ECtHR case law.

1.3.4 In Practice, The "Essentially Equivalent" Test Means That US Laws And Practices Must Meet The Basic Principles Enunciated By EU Jurisprudence And, With Regard To Proportionality, Must Stay Within The Margin Of Discretion Accorded To EU Member States By The ECtHR

Taking the five basic principles in *Schrems* together with the judgments of the ECtHR, especially as the latter pertain to surveillance in general and signals intelligence in particular, the safeguards called for under EU legal order relating to surveillance can be summarized as follows:

1. *Specific legal authority*: Surveillance measures must be based on clearly stated legal authority. The legal bases or purposes for surveillance must be clearly spelled out. These purposes must be for legitimate aims of a serious nature with an objective reasonable basis in facts. There must be objective criteria by which to limit the discretion of authorities.

2. *Limited scope*: The amount of data collected or subject to retention requirements must not go beyond what is necessary to accomplish the purpose of the surveillance and cannot be generalized or indiscriminate.

---

[108] *Id.*

[109] Article 52(3) of the Charter provides that "this provision shall not prevent Union law providing more extensive protection". However, there is no such EU law, at least not in the area of national security. Indeed, Article 4(2) TFEU would require explicit approval from EU Member States to relinquish sovereignty in this regard.

[110] *See supra* note 43, at art. 21.

Discriminants must be established with due care and consistent with the specified purposes for surveillance. The period of retention must be reasonable and finite.

3. *Oversight*: There should be some combination of executive, legislative, judicial, and expert oversight for approval and review of surveillance measures.

4. *Legal remedies and redress*: The public should be informed about surveillance laws and have some opportunity for access and rectification, and for judicial redress. If necessary for legitimate aims of surveillance, surveillance can be secret, in which event greater oversight or more general legal redress are necessary.

These four criteria, therefore, provide the criteria to establish the EU Benchmark. The EU legal order requires laws in EU Member States to fulfill these criteria with concrete measures. With regard to the degree of interference, Member State laws must be "necessary within a democratic society," which means these laws must stay within the margin of discretion set out in the case law of the ECtHR. This margin of discretion must be applied on the basis of a comparative review of Member State laws so the "degree of consensus" can be determined for different types of surveillance. The EU Benchmark therefore must reflect the "bandwidth" within which Member States must stay.

1.4 Application Of The "Essentially Equivalent" Test Must Take Into Account Differences In Decisionmaking Under Article 25, Essential Procedural Requirements, And International Obligations

In applying the "essentially equivalent" test to determine the adequacy of privacy and data protection safeguards in the legal order of a third country in the context of particular data transfer mechanisms, the Commission and data protection authorities must meet certain requirements of EU law. First, they must comply with Article 25 of Directive 95/46, which prescribes different decisions for the Commission and for supervising authorities. Second, the manner in which those bodies make their decisions must meet essential procedural requirements. And third, their decisions must take into account the international obligations of the EU and the Member States.

In addition, Article 25 of Directive 95/46 and the *Schrems* judgment make clear that determining whether a third country provides an adequate level of protection is not an abstract question. The CJEU calls on the European Commission (or a supervisory authority as the case may be) to make "findings, duly stating reasons," which must be based on a complete examination of laws and international commitments in force, and on practices and their effect. If the Commission or a Member State makes a finding that a third country "does not ensure an adequate level of protection" pursuant to Article 25(3) or (4), such a finding will have to take account of the full dimensions of the EU legal order. Only then can the decision ensure equal treatment.

1.4.1 Differences Between Commission Decisions Under Article 25(6) And Individualised Adequacy Decisions Under Article 25(2) Give Rise To Different Application Of The "Essentially Equivalent" Test

There are procedural differences between a Commission adequacy determination relating to a third country pursuant to Article 25(6) of Directive 95/46 and determinations by DPAs or national courts (or, companies in "self-assessment" countries, such as the UK[111]) must carry out with respect to specific transfers or sets of transfers under Article 25(2).

When the European Commission prepares a Decision under Article 25(6), it will have to assess not only the level of protection ensured by the third country's laws and practices, but also compare them to the level of protection in the EU legal order as a whole. It will also have to take into account the additional level of protection granted by individual company commitments, such as a promise to adhere to the Safe Harbour Principles.

When a DPA or a national court assesses data transfers to the US by a specific company, Article 25(2) of the Directive requires a more focused test than the general test under Article 25(6). In such individual cases, Article 25(2) requires a comparative assessment of "all the circumstances surrounding a data transfer operation." This includes not only the nature of the data and the purpose and duration of the proposed processing, but also the country of origin and country of final destination, and the rules of law, including general and sectoral rules, as well as professional rules and security measures in the third country.

As a first step, the determination must assess the data protection laws and surveillance laws and practices applied in the particular (exporting) Member State. Under Directive 95/46, it is these laws (rather than the EU legal order as whole) that establish the actual level of data protection in that Member State.

Second, "the nature of the data" must be assessed. The nature of data can affect the "rules of law, both general and sectoral," applicable before, and especially after the transfer to the US; as discussed in Part 3.3.1, particular US sectoral protections may apply to the data once they arrive in the US (for example, the Fair Credit Reporting Act (FCRA) for consumer credit reporting data, or the Health Insurance Portability and Accountability Act (HIPAA) for health data). The nature of the data can also affect the risk of surveillance; not all data is the same in this regard, and a large proportion of the 4,000 companies that have relied on the 2000 Safe Harbour Framework do not transfer personal information of types (such as communications) that are targets of surveillance. In addition, some types of records – such as health research – may present strong public interest reasons to permit a transfer due to their potential to better human life, without regard to the risk of surveillance.

[111] In the UK, the Information Commissioner's Office has provided detailed guidance on application of the adequacy assessment with criteria divided into two categories: "general adequacy criteria" and legal adequacy criteria. *See* Information Commissioner's Office, *Sending personal data outside the European Economic Area (Principle 8)*, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

Third, the impact of the transfer of the data to the US is also affected by the location where the data are being transferred, because it can trigger the application of specific state laws in the US. Hence, a thorough determination should assess the privacy and data protections of states with jurisdiction over the data. If the state of destination is California, for example, one of the more than 100 California state level laws containing data protection provisions may apply, as further discussed in Part 3.3.1.

A fourth step is to assess the safeguards, including any Binding Corporate Rules (BCRs) or other contractual clauses, put in place by the company to ensure compliance with the data protection principles set out in Chapter II of Directive 95/46. While, under Article 26(2), such safeguards can – indeed, are intended to – enable data transfers even where the third country does not ensure an adequate level of protection, in the US they serve to reinforce a high level of privacy rules and practice, backed up (as noted in Part 3.3.1) by a vigorous private enforcement climate.

If, as this report concludes, the level of protection in the US in the case of secret surveillance is essentially equivalent to the EU Benchmark, an exporting Member State cannot legitimately argue that the transfer will lower the level of protection without specific evidence as to why the transfer, in the specific situation of that specific company, will expose the data subject to a reduction in the level of protection for their personal data.

And even if the level of protection in the US for the data of that specific company would be lower than the EU Benchmark, a general prohibition on the data flows to the US still could not be imposed without evidence that the level of protection in the exporting Member State itself meets the EU Benchmark, and that the exporting Member State also objects to data transfers to other countries that are in a situation comparable to the US. If these requirements are not met, the exporting Member State would be discriminating against companies that do business with the US, and this would potentially infringe the international commitments discussed below in Part 1.4.3.[112]

1.4.2 Application Of The "Essentially Equivalent" Test Must Be Based On Correct, Complete, And Accurate Facts

The first requirement for proper application of the "essentially equivalent" test – whether in the general context of Article 25(6) or an individualised determination under Article 25(2) (as discussed above) – is that it is based on facts that are correct, complete, and substantiated. For the European Commission, the obligation to assess thoroughly all of the relevant facts pertaining to all of the factors listed in Article 25(2) of Directive 95/46 was highlighted by the *Schrems* judgment. Hence, it forms an "essential procedural requirement" within the meaning of the TFEU.[113]

---

[112] *See infra*.

[113] TFEU, art. 263, para. 2. See, by analogy, CJEU 24 October 2013, Case C-510/11 P, *Kone and Others v. European Commission*, ECLI:EU:C:2013:696, para. 28, in which the CJEU confirmed the general obligation of the Commission to properly establish the relevant facts:

For supervising authorities, the CJEU confirmed in *Schrems* that they must act with "all due diligence" when taking decisions pursuant to Article 28 of the Directive.[114] Generally, the obligation to carefully establish the relevant facts before taking administrative and judicial decisions affecting citizens and companies is firmly embedded in the legal traditions of all Illustrative Member States, and it is reflected in Article 41 of the Charter and the EU Code of Good Administrative Behaviour.[115] Moreover, a failure to establish the relevant facts could contribute to a finding that discrimination is arbitrary or unjustified within the meaning of GATT or GATS.[116]

The obligation to properly establish the facts means, first, that a determination cannot be based simply on press reports, especially those that been retracted or proved wrong. Likewise, a determination cannot be based on mere allegations, much less those that have proven to be inaccurate or unsubstantiated. It follows directly from the language of Article 25(2) of the Directive ("the laws in force"), referred to in paragraphs 70 and 75 of *Schrems*, that the obligation to properly establish the facts also means, relying on information that is relevant and not outdated. With regard to the US, this means that all recent changes in the laws and practices in the US must be taken into account:[117] every "essentially equivalent" test must be *ex nunc*.

1.4.3 The "Essentially Equivalent" Test Cannot Result In A Test That Is Stricter For Transfers To The US Than For Transfers To Other Member States Or Other WTO Countries Outside The EU

The international commitments of the EU form a part of the EU legal order that have been reflected in previous Commission adequacy decisions under Article 25. They must be reflected in future decisions of the Commission and DPAs.

When the European Commission prepared the Safe Harbour Decision in 2000, it requested advice from the Article 31 Committee.[118] On 31 May 2000, this Committee published its "Text On Non-Discrimination,"[119] which stated:

> "[T]hird countries have raised concerns that enforcement actions in the EU may be more severe vis-à-vis third country entities than they are vis-à-vis EU

> "Courts must, among other things, not only establish whether the evidence relied on is factually accurate, reliable and consistent but also ascertain whether that evidence contains all the information which must be taken into account in order to assess a complex situation and whether it is capable of substantiating the conclusions drawn from it."

[114] *Schrems*, para. 63.

[115] European Commission, *Code of Good Administrative Behaviour* (2000), http://ec.europa.eu/transparency/code/_docs/code_en.pdf.

[116] *See infra* Part 1.4.3.

[117] *See infra* Part 2.2.1.

[118] Article 31 of Directive 95/46 provides that such a Committee shall be set up to assist the Commission.

[119] Advice from the Article 31 Committee of 31 May 2000, Text on non-discrimination.

> data controllers and that there may also be discrimination between the entities from different third countries. The Committee is confident that these concerns will prove to be unfounded …. *[T]he Directive's enforcement should, in the Committee's view, be impartial* both as between different third countries and as between third countries' and EU entities."[120]

In Recital 4 to the Safe Harbour Decision, as in its other adequacy decisions,[121] the Commission noted that these decisions "should be enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail nor constitute a disguised barrier to trade taking into account the Community's present international commitments."

The "present international commitments" referred to in Recital 4 are set out in the WTO's General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS). Within their scope of application, GATT and GATS require the EU and its Member States to grant, as a rule, "Most Favoured Nation Treatment" (MFN) and "National Treatment," and they must also "administer measures in a reasonable way."[122] This essentially means that, as a rule, the EU and its Member States may not accord less favourable treatment to US goods, US services, and US service providers than they do to like EU goods and suppliers, or to other third countries that are GATT or GATS members. When the EU or its Member States do restrict MFN or National Treatment, such restrictions may not amount to "arbitrary or unjustifiable discrimination."[123]

[120] *Id.* (emphasis added).

[121] *E.g.*, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (2000/518/EC), *OJ* 2000 L215/1, recital (4); Commission Decision of 31 January 2011 pursuant to Directive 95/46?EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (2011/61/EU), *OJ* 2011 L27/39, recital (4); and Commission Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (2013/65/EU), *OJ* 2013 L28/12, recital (4).

[122] GATS Articles II, XVII, XVI:2(a); GATT 1994, Articles I:1; III:4; X:3(a).

[123] GATS Article XIV(c)(ii) ("Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures… necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to… the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts"); GATT 1994, Article XX(d).

Discrimination is arbitrary or unjustifiable if a WTO Member does not provide some degree of certainty that the application of the measure will be applied in a fair and just way by the designated domestic bodies.[124] Therefore, arbitrary or unjustifiable discrimination would arise if a Member State knowingly and without any rational reason subjects data flows to the US to higher standards than data flows to other Member States or to other countries covered by an "Article 25(6) decision."[125]

Examination of the US legal order therefore must take into account recent Article 25(6) decisions in which the European Commission has recognized that third countries are entitled to restrict data privacy rights on public policy grounds, provided that the public policy grounds are "similar in spirit" or "reflect" the provisions of Directive 95/46. Restrictions of data protection rights permitting surveillance may be acceptable even if "there is no exact corresponding exception in the Directive." In Opinion 11/2011, for example, the Article 29 Working Party assessed a principle of New Zealand law permitting an agency to collect personal data without respecting the principle of fairness where "[t]he agency believes, on reasonable grounds, that compliance would prejudice the purposes of the collection."[126] The Article 29 Working Party took a favourable view of this exception which was likely to be used in connection with monitoring and surveillance activities even though there was "no corresponding exception in the Directive":

> *"(viii) The agency believes, on reasonable grounds, that compliance would prejudice the purposes of the collection*. Although there is no exact corresponding exception in the Directive, this exception reflects the exceptions provided for in article 13(a) to (f) and is likely to be used in connection with monitoring and surveillance activities, in particular in the employment and law enforcement areas."

Compliance with GATT and GATS obligations would not permit applying a stricter standard to United States goods, services, or service providers without properly substantial grounds.

---

[124] See Appellate Body Reports, US – Shrimp, para. 181 and EC – Seal Products, para. 5.328, stating that there is arbitrary or unjustifiable discrimination where exporting Members can in no way be certain that the relevant provisions or guidelines were applied in a fair and just manner by the appropriate governmental agencies of the importing Member.

[125] See Appellate Body Reports, Brazil – Retreaded Tyres, paras. 229 & 246 and EC – Seal Products, para. 5.306, stating that there is arbitrary or unjustifiable discrimination when the reasons given for the discrimination bear no rational connection to the objective of the measure.

[126] Principle 4 of the New Zealand Privacy Act "covers the issue of fairness by providing that an agency may not collect personal information: (a) By unlawful means; or (b) By means that, in the circumstances of the case, -- (i) Are unfair; or (ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned." Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf.

PART TWO:

COMPARISON OF THE LEGAL ORDERS ON GOVERNMENT SURVEILLANCE SHOWS THAT US SURVEILLANCE OF EUROPEAN PERSONAL DATA TRANSFERRED TO THE US IS NOT "MASS AND UNDIFFERENTIATED" AND IS CONSISTENT WITH THE LEGAL ORDER WITHIN THE EU

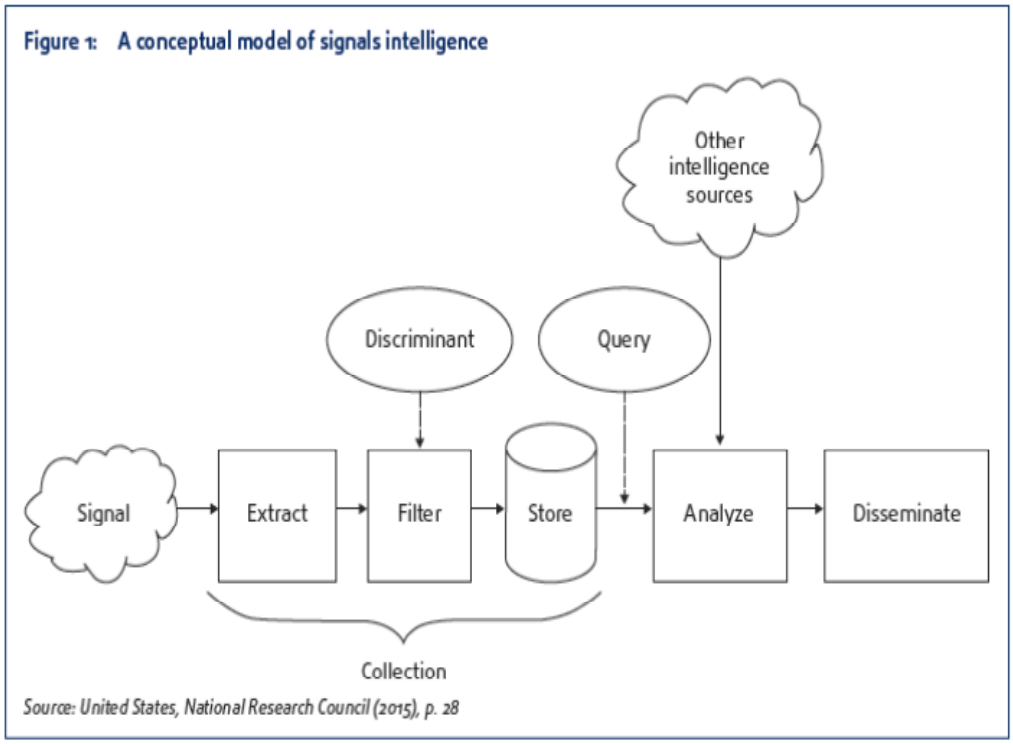
Part One demonstrates that a decision under Article 25(2) or 25(6) of Directive 95/46 must take full account of the EU legal order (including the interferences to data protection permitted under EU law) and that the standard applied to the United States cannot, as a rule, be stricter than the standard applicable to EU Member States or to WTO member countries (and in particular the third countries that are subject to an Article 25(6) Decision). This chapter turns to comparison of the EU and US legal orders in the context of government surveillance.

This part presents the results of a preliminary overview of surveillance laws in a sample consisting of eight Member States, four of the largest ones and four others: Belgium, France, Germany, Italy, Ireland, Poland, the Netherlands, and the United Kingdom (Illustrative Member States). It also benefits from the recent analysis across all Member States by the European Union Agency for Fundamental Rights (FRA),[127] as well as other, less-recent comparative reviews.

This report then looks at how US surveillance laws fit within this bandwidth of Member State laws. In conducting the comparison, the report focuses on US laws most likely to affect data of EU citizens transferred to the US and the analogous laws in the Illustrated Member States. These are laws affecting electronic communication and, in particular, those laws affecting what the FRA categorized as "signals intelligence," comprising the collection, processing, and analysis of information transmitted or stored in digital form. The FRA used the following conceptual model of signals intelligence[128]:

[127] Surveillance by intelligence services : fundamental rights safeguards and surveillance and remedies in the EU (November 2015) (FRA Report), http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

[128] The FRA's model was derived from a model published by the US National Research Council in a review of surveillance technologies undertaken at the request of President Obama. *See* United States, National Research Council, *Bulk Collection of Signals Intelligence: Technical Options* 28 (2015), available for download at http://www.nap.edu/download.php?record_id=19414#.



The ECtHR has conducted some examination of collection of signals intelligence under the ECHR. In *Weber & Saravia v. Germany*, the ECtHR ruled that Member States have a "fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security" through signals intelligence.[129] The ECtHR does require that "there exist adequate and effective guarantees against abuse,"[130] but using "catchwords" or "search terms" (*i.e.*, selectors or discriminants) is a recognized method to maintain the proportionality of the interference.[131]

The examination of Illustrative Member State signals intelligence laws and other key surveillance laws follows the criteria for the EU Benchmark established in Part 1.4. Parts 2.1 and 2.2 below examine how the Illustrative Member States and the US each implement these criteria to provide guarantees against abuse and maintain proportionality. Part 2.3 then conducts a direct comparison to establish that safeguards against abuse of surveillance under the US legal order meet the "essentially equivalent" test.

[129] ECLI:CE:ECHR:2006:0629DEC005493400, § 106.

[130] *Id.*

[131] *Id.*; see also *Liberty v. United Kingdom*, ECLI:CE:ECHR:2008:0701JUD005824300, § 68, in which the German model of applying search terms was held up as a model for the United Kingdom: "[T]he G10 Act stated that the Federal Intelligence Service was authorized to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order."

2.1 The EU Legal Order On Surveillance Reflects Wide Discretion As To The Necessity Of Surveillance And Safeguards To Limit Interference With Rights And Freedoms

2.1.1 Introduction

The Illustrative Member States whose surveillance laws are examined in this section are Belgium, France, Germany, Italy, Ireland, the Netherlands, Poland and the UK. Together, these countries encompass more than two-thirds of the citizens of the EU.

This section of the report looks at the laws of these Illustrative Member States respecting government surveillance by intelligence services and criminal justice systems in light of the four criteria above, distilled from the *Schrems* judgment and the ECtHR case law: (i) the specific legal authority for the surveillance measures; (ii) limits on the scope of data that may be collected and retained; (iii) oversight of the surveillance measures; and (iv) legal remedies and forms of redress available where surveillance measures may breach data protection and privacy rights.[132] These criteria must be respected to justify state measures that enable interference with human rights in pursuit of legitimate goals such as state security or national security.

For each one of these criteria, this section considers the various ways the laws of the Illustrative Member States address key aspects of the criteria. The object of this overview is to look concretely at how these Member States implement their surveillance laws and give force to the EU fundamental principles of necessity and proportionality.

As more fully discussed below, these principles are expressly referred to in some form in most of the Illustrative Member States' surveillance laws, and some have proposed legislation with a view towards conforming their laws with these principles.[133] The focus of this overview is on the specific measures the Illustrative Member States take to provide such adequate and effective guarantees and comply with the broad principles in their laws.

As set out in more detail in Part 1.3.3 above, it has been well established since the ECtHR's Plenary Court judgment of 6 September 1978 in *Klass* that EU Member States must be able to undertake secret surveillance to effectively counter threats to the security of their citizens.[134] They have a wide margin of discretion to set the level

[132] *Schrems*; *see also supra* Part 1.3.4.

[133] In France, for example, the principle of proportionality, in particular with respect to the risks to privacy, secrecy of correspondence and inviolability of the home; and encouraging the implementation of less intrusive surveillance measures where the same outcome can be achieved, were presented by the French Government as being the guiding concepts in the implementation of surveillance measures pursuant to the recently adopted Intelligence Law No. 2015-912 of 24 July 2015 on Intelligence (2015 Intelligence Law). The aim of the 2015 Intelligence Law was to fill a legislative gap and provide a legal framework for the intelligence services activities in France. Likewise, in the UK, the Regulation of Investigatory Powers Act 2000 (RIPA) was implemented to consolidate UK surveillance laws and bring the laws into line with the obligations under the ECHR (as defined below) including the principles of necessity and proportionality. RIPA Explanatory Notes.

[134] *Klass*, § 48: "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to

of protection for their citizens in terms of national security and public safety, to evaluate threats,[135] and to choose the forms of surveillance to counter such threats.[136] The threats to security cannot be defined in advance, and the surveillance instruments to be used can therefore vary over time as well.

The ECtHR has assessed several types of potentially intrusive surveillance measures, including direct access of intelligence services to all communications of a certain type, *e.g.*, all phone conversations between two Member States,[137] or technical access to all mobile phones.[138] The ECtHR does not condemn any type of surveillance methods or measures as such. Rather, the ECtHR assesses if such measures are "prone to abuse" and what measures are taken by the state to prevent such abuse.[139] This assessment of the surveillance practice as a whole (*i.e.*, including safeguards)[140] determines whether a Member State limits interference with fundamental rights to what is "necessary in a democratic society" within the meaning of Article 8 ECHR.

The comparative overview that follows shows a broad consensus (upheld by the ECtHR) that national security and public safety can be protected by means of electronic surveillance.

Each of the Illustrative Member States authorises and regulates various forms of surveillance by agencies for the purposes of intelligence and internal security under the heading of "national security" or "state security" as well as other interests of the state. Each also authorises surveillance by the criminal justice system for criminal justice purposes to investigate and prosecute serious crimes. The majority of the Illustrative Member States use advanced forms of surveillance, and they are

---

counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court therefore has to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications." *See also* Article 4(2) TEU, Article 8 ECHR, Article 52 Charter, Articles 3(2) and 13 of Directive 95/46.

[135] ECtHR, Research Division, *National Security and European Case-Law* 4 (2013) ("Member States are recognized to have certain – even a large – measure of discretion when evaluating threats to national security.").

[136] *Klass*, § 49 ("As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in the field."); *id.* (collecting further references).

[137] *Liberty*, § 64.

[138] *Zakharov*, § 270.

[139] *Id.* §§ 270–271.

[140] *Kennedy*, § 153 ("[P]owers to instruct secret surveillance of citizens are only tolerated under Article 8 [of the] ECHR to the extent that they were strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.").

technically capable of intercepting any kind of communication in their territory. The four largest Illustrative Member States (France, Germany, Poland, and the UK) and the Netherlands explicitly permit certain types of surveillance that are not targeted at identified suspected individuals, and these countries can apply "keywords" or "selectors" to large communications data flows crossing their territory.

For the publicly-known surveillance programmes,[141] each Illustrative Member State limits the use of surveillance through prior approvals – either from judicial authorities or from high-level government ministers. Each has various forms of *post-hoc* oversight. The standards required for approval of surveillance, the mechanisms of oversight, the permitted scope of surveillance, and the ability to seek effective and meaningful remedies for abuses of surveillance authority all vary significantly.

After this overview, the next section of the report will conduct a similar overview of the legal order for surveillance in the US measured against the same criteria. Then Section 2.3 will assess the range of variation among the measures taken in the Illustrative Member States to establish the EU Benchmark and apply this benchmark to the US legal order.

2.1.2 Specific Legal Authority

> *Surveillance measures must be based on clearly stated legal authority. The legal basis or purposes for the types of surveillance undertaken must be clearly spelled out. These purposes must be for legitimate aims of a serious nature with objective basis in facts. There must be objective criteria by which to limit the discretion of authorities.*

All of the Illustrative Member States have detailed laws that enable surveillance by government bodies for intelligence and internal security, as well as judicial (or judicially supervised) surveillance for criminal justice or law enforcement purposes. In all Illustrative Member States surveillance of internal communications (*i.e.*, communications originating from and received within the relevant Illustrative Member State) is carried out for internal security purposes either by law enforcement or by the intelligence services (or components of the military or other agencies that perform intelligence activities). The intelligence services of all the Illustrative Member States also engage in surveillance of external communications (*i.e.*, communications either originating from or received in a country other than the relevant Illustrative Member State). Criminal justice surveillance is carried out by police services.

In some of the Illustrative Member States, such as France, government surveillance is governed by a section of the Internal Security Code implementing two pieces of legislation, the 2015 Intelligence Law and Law No. 2015-1556 of 30 November 2015, concerning surveillance measures for international electronic communications. In others, the surveillance framework is more complex and is composed of a number of laws. This is the case in Germany, Ireland, and Poland. These laws often cover

[141] FRA Report, *supra* note 127, at 17. This report discusses only the forms of surveillance that are known publicly. There have been reports of secret surveillance programs in Illustrative Member States that are not regulated by law.

specific sectors such as telecommunications or police forces. Regardless of the form or scope of such laws, all are published in either the relevant Member State Official Journal or a similar publication, or codified or enacted as public statutes.

A Wide Range of Purposes Permitting Surveillance

The purposes for which surveillance measures may be undertaken vary among the Illustrative Member States but all permit surveillance by national intelligence agencies in the interests of "national security" or "state security." These terms are not defined in the EU legal order, and in *Esbester v United Kingdom*[142] the European Commission HR judged that "national security" cannot be defined comprehensively. As summarised by the ECtHR's Research Division, "Member States are recognized to have certain – even a large – measure of discretion when evaluating threats to national security."[143]

Indeed, the lack of a clear definition is seen as an advantage in some Illustrative Member States. According to *the UK*'s Secret Service the lack of a definition ensures the necessary flexibility is retained in order to adapt to changing circumstances.[144] The Article 29 Working Party consider it "necessary to take account of the political situation at the time the 'choice' is made, as well as the relevant actors," when determining whether a surveillance measure falls within the ambit of national security.

Although *Ireland*'s legislation is principally intended to deal with interceptions on a domestic basis,[145] it has perhaps the broadest national security authority. Against the backdrop of the security situation in Northern Ireland in recent decades, Ireland has long asserted the need and ability to intercept communications "in the interests of the security of the State" as well as "for the purpose of criminal investigation."[146] The legislation does not spell out these purposes in particular detail, and much discretion is left to the relevant authorities.

Italy also broadly authorises surveillance by its External Intelligence Agency "to defend the independence, integrity, and Security of the State," and by its Internal Security Agency "to protect internal security and democratic institutions from any threat, criminal aggression, act of terrorism or activity aimed at subverting the constitutional order," but provides some limit by requiring a strong demonstration of necessity as described below.

---

[142] ECtHR 2 April 1993, *Esbester v United Kingdom*, ECLI:CE:ECHR:1993:0402DEC001860191.

[143] ECtHR, Research Division, *National Security and European Case-Law* 4 (2013).

[144] MI5, UK Secret Service, *What Is National Security*, https://www.mi5.gov.uk/home/about-us/what-we-do/protecting-national-security.html (last accessed on 19 Jan. 2016).

[145] The Criminal Justice (Mutual Assistance) Act 2008 provides mechanisms for the Irish authorities to authorize interceptions based on requests from foreign law enforcement agencies.

[146] Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 (as amended), Articles 4 and 5.

Among the Illustrative Member States, *France* has the most comprehensive list of security interests that can be protected by means of surveillance measures. The 2015 Intelligence Law spells out a number of specific security interests relating to "fundamental interests of the Nation."[147] These are:

> "[N]ational independence, territory integrity, and national defence; major interests of foreign policy, execution of European and international commitments of France and prevention of any form of external political interference; major economic, industrial and scientific interests of France; terrorism prevention; prevention of attacks to the republican institutions, actions leading to the maintenance or reconstitution of groups dissolved under Article L. 212-1; collective violence that could seriously harm public peace, prevention of organised crime and prevention of the spread of weapons of mass destruction."

Even where laws in Illustrative Member States, other than Ireland, Italy, and France, refer broadly to "national security" or "state security," they also include specific categories similar to those in French law. *Germany* limits the use of "strategic intelligence" – interception of telecommunications traffic to or from Germany and other countries (as distinguished from "individual measures") – to detecting and averting the danger of, *inter alia*, an armed attack against Germany, terrorism, arms proliferation, money counterfeiting that undermines the stability of the EURO, money laundering, human trafficking of substantial importance, cyber terrorism and cybercrime, and smuggling of narcotics of substantial importance into the EU.[148]

In *Poland*, the Internal Security Agency may implement surveillance measures to identify, prevent, detect and prosecute perpetrators of crimes which include:

> "[E]spionage, terrorism, illegal disclosure or use of classified information and other crimes affecting the security of the state; those affecting the state's economic interests; the corruption of public officials, where it can threaten the security of the state; crimes with regard to the production and marketing of goods, technologies and services of strategic importance for national security; the unlawful manufacture, possession and trade of weapons, munitions and explosives or weapons of mass destruction; and the trafficking of narcotic drugs and psychotropic substances, in international trade."[149]

In addition to national security interests, in Belgium, France, Poland, and the UK, surveillance is authorized in various terms for the economic interests of the nation.[150]

---

[147] Internal Security Code, Article L. 811-3.

[148] Act on Restricting the Privacy of Correspondence, Posts and Telecommunications [Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Article 10-Act)] 26 June 2001, 13 August 1968, Section 5.

[149] Act on Internal Security Agency and Foreign Intelligence Agency of 24 May 2002, Article 5.

[150] Belgium – surveillance is authorised where relevant for "the scientific and economic potential of the State" - Intelligence and Security Services Act, 30 November 1998, Article 7-1°; France – surveillance is authorised where in the defence and promotion of "major economics, industrials and scientific interests of France" - Internal Security Code, Article L. 811-3; Germany – surveillance is authorised to

The Polish Constitutional Tribunal, however, recently found the ground of the "state's economic interests" was not specific enough as it was not a defined concept and it was not clear in relation to what offenses this ground could relate.[151] In so doing, the Tribunal established among other requirements a judicial limit on the purposes of surveillance, holding that surveillance measures must be used exclusively for the purpose of detecting, investigating and preventing serious crimes.[152]

A Wide Range of Acts Permitting Law Enforcement Surveillance

With regard to criminal justice surveillance, three of the Illustrative Member States (France, Poland, and the UK) have provisions expressly authorising the intelligence services to conduct surveillance for prevention or detection of crimes of specified kinds or gravity. In *France*, the authorisation of administrative surveillance for the prevention and detection of crime is limited to the "prevention of organised crime and the spread of weapons of mass destruction."[153] In *Poland*, intelligence surveillance for the prevention and detection of crime is limited to "the unlawful manufacture, possession and trade of weapons, munitions and explosives or weapons of mass destruction; and the trafficking of narcotic drugs and psychotropic substances, in international trade."[154] In *the UK*, surveillance is authorised for the "prevention and detection of crime,"[155] although the crime must be considered "serious" to justify the interception of communications or intrusive surveillance.[156] Surveillance on these grounds includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.[157] No distinction is made as to which authorities can rely on these grounds to carry out the surveillance measures.

"prevent severe terrorist crimes intended to significantly impair or destroy the fundamental economic structures of a State or an international organization and which, given the nature or consequences of such offences, may seriously damage a State or an international organization" - Law on the Establishment of a Federal Criminal Police Office, 8 March 1951, Section 4a (2); Poland – surveillance is authorised to identify, prevent and detect crimes which "affect the State's economic interests" – Article 5 of the Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002; UK – surveillance is authorised where it is necessary "for the economic well-being of the country" – RIPA, §§ 22(2), 28, 32 & 49. Note that Article 8 ECHR specifically refers to the "economic well-being of the country."

[151] Decision of the Polish Constitutional Tribunal, 30 July 2014, case K 23/11.

[152] *Id.*

[153] Internal Security Code, Article L. 811-3.

[154] Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002, Article 5.

[155] RIPA, §§ 22(2), 28 & 49.

[156] *Id.* §§ 5(3) & 32. Surveillance is intrusive if it is covert and carried out in relation to an activity in a residential premises or private vehicle. Intrusive surveillance must involve the presence of an individual or be carried out using a surveillance device, defined as "any apparatus designed or adapted for use in surveillance." *Id.* § 48(1).

[157] *Id.* § 81(5).

In other Illustrative Member States, (Belgium, Germany, Ireland, Italy, and the Netherlands) surveillance for prevention and detection of crime is authorized only in provisions governing the activities of law enforcement. In *Belgium*, surveillance measures may only be used in the context of an ongoing criminal investigation in respect of certain types of serious criminal offence including, for example, acts of terrorism. In *Germany*, the German Code of Criminal Procedure permits surveillance by law enforcement in relation to the "investigation of serious criminal offences."[158] In *Ireland*, surveillance by the Commissioner of the Garda Siochána (Irish police force) is authorized for the "prevention, detection, investigation or prosecution of a serious offence."[159] In *Italy*, surveillance as a means to gather evidence and preventive surveillance can be authorized only in respect of serious crimes.[160] In *the Netherlands*, the police may conduct surveillance pursuant to the Criminal Procedure Code providing there is a link to a criminal offense, with the gravity of the offense determining what surveillance measures may be used.

2.1.3 Limited Scope

The amount of data collected or subject to retention requirements must not go beyond what is necessary to accomplish the purpose of the surveillance and cannot be generalized or indiscriminate. Discriminants must be established with due care and consistent with the specified purposes for surveillance. The period of retention must be reasonable and finite.

Illustrative Member States Gather All Types of Data

The types of data covered by the surveillance laws in each of the Illustrative Member States broadly include images, sounds, traffic data (*i.e.*, data relating to the transmission of a communication), subscriber data (*i.e.*, data held by or obtained from a communications service provider), usage data (*i.e.*, data relating to the use made by a person of a communication service), and the content of communications.

In several of the Illustrative Member States there are no statutory distinctions among types of data acquired. However, the surveillance laws in Belgium, France, Poland, and the UK apply different terms to describe "metadata" – traffic, subscriber and

---

[158] *See e.g.*, Code of Criminal Procedure §§ 100a, 100c, 100f, 100g & 100h.

[159] A "serious offence" is defined as an offence: (a) "for which a person aged 21 years or over, of full capacity and not previously convicted may be punished by imprisonment for a term of 5 years or more; " and (b)(i) "that involves loss of human life, serious personal injury or serious loss of or damage to property or a serious risk of any such loss, injury or damage; (ii) that results or is likely to result in substantial gain; or (iii) the facts and circumstances of which are such as to render it a specially serious case of its kind; and includes an act or omission done or made outside the State that would be a serious offence if done or made in the State: Provided, however, that an offence consisting of an attempt, conspiracy or incitement to commit an offence shall not be a serious offence unless the offence which is the subject of the attempt, conspiracy or incitement is itself a serious offence." Interception of Postal Packets and Telecommunications Messages (regulation) Act, 1993, Article 1.

[160] See, for surveillance as a means to gather evidence, Code of Criminal Procedure, D.P.R. n. 447 of 22 September 1988, Article 266. For preventive surveillance, see Implementing Provisions of the Code of Criminal Procedure, Legislative Decree n. 271 of 28 July 1989, Article 226, and Code of Criminal Procedure, D.P.R. n. 447 of 22 September 1988, Articles 51/3-bis & 407/2(a).

usage data[161] - and treat this data distinctly from other forms of data, in ways that make it more easily available.

In *Belgium*, "identifying data" is typically captured via "specific intelligence methods." Unlike the "extraordinary intelligence methods," which capture the content of communications, the "specific intelligence methods" do not require a prior authorisation from the regular oversight body (the BIM-controlecommissie).[162] Likewise, in Poland, there is no requirement to obtain the approval of the District Court prior to collecting the "telecommunications data" (as there is for other data).[163]

In *France* "connection data" is distinguished from data collected through security interceptions and tapping. Pursuant to Article L. 822-2 of the Internal Security Code, the latter form of data must be destroyed 30 days after collection (albeit subject to exceptions where, for example, the data is encrypted[164]), whereas connection data can be retained for four years.[165]

In *the UK*, while the interception of communications requires the issuance of a warrant by the Secretary of State, the acquisition of "communications data" can be authorized by a "designated person" (i.e. persons holding a prescribed office in a relevant public authority).[166] In addition, the scope of the purposes for which communications data can be obtained extends considerably beyond the purposes for which other types of data can be obtained and includes where it is necessary "in the interests of public health and safety, to assess or collect tax, to prevent death or personal injury or for any other purpose specified in an order made by the Secretary of State."[167] RIPA also places no restrictions on the use of communications data other than where such data is obtained pursuant to an interception.

Targeted And Non-Targeted Surveillance

In considering how to distinguish between mass surveillance and targeted surveillance, the European Union Agency for Fundamental Rights looked at differences between surveillance that "presupposes prior suspicion of a targeted

[161] Referred to as "identifying data" under Belgian law, "connection data" under French law, and "communications data" under English law. In Polish surveillance laws, there is no single term used for metadata, and instead reference is usually made to the Articles in the Telecommunication Act, which list the types of metadata. The only collective reference used is in the Police Act (Article 20c), in which metadata is referred to as "telecommunications data" and, as such, this report will adopt this terminology.

[162] Act on Special Intelligence Methods by the Intelligence and Security Services, 4 February 2010.

[163] Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002, Article 28 (1).

[164] Internal Security Code, Article L. 822-2-I°.

[165] *Id.*, Article L. 854-5. The Internal Security Code provides for longer retention periods up to 8 years for data obtained from international electronic communications (*i.e.*, emitted from abroad or received abroad).

[166] RIPA, § 22(3).

[167] *Id.* § 22(2).

individual or organisation" and surveillance measures that "start without prior suspicion or a specific target, which is defined after collection and filtration of certain data."[168]

The discussion below first looks at how the Illustrative Member States treat first the targeting of specific individuals or organizations, and then targeting based on collection and filtration of data.

Surveillance Not Targeted At Specific Individuals Or Organisations

Five Member States (France, Germany, Poland, the Netherlands, and the UK) permit interception of external communications that is not targeted at specific individuals.[169] In *France*, the 2015 Intelligence Law permits the government to oblige telecommunications providers and ISPs to set up automatic processing, based on predefined parameters that could detect a terrorist threat.[170] These parameters are predefined in an authorisation granted by the Prime Minister; the 2015 Intelligence Law does not provide clarity as to what these parameters may be. This law also authorises traffic signals intelligence and IMSI catchers, which allow the capture of data of any person located in a determined geographic area without that person's knowledge.[171]

In *Germany*, a Parliamentary Control Panel (described more fully below in Part 2.1.4) is responsible for approving important aspects of the strategic telecommunications surveillance undertaken by the Federal Intelligence Service (the "BND"). This surveillance consists of surveillance of telecommunications traffic externally from and to Germany using specific format or content-related keywords.[172]

In addition to specifying the keywords to be used by the BND, the written order approving the surveillance measure must specify the geographic region, the transmission paths that are subject to the surveillance measure, and the percentage of the overall transmission capacity to be monitored on the external

[168] FRA Report, *supra* note 127, at 17 ("[I]f a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted." (quoting United States, National Research Council, *supra* note 128, at 33.

[169] The interception of external communications that is not targeted at specific individuals may take place in other Illustrative Member States but the surveillance laws in those Member States do not provide sufficient details to enable a legal analysis of the procedure to be carried out.

[170] Internal Security Code, Article L. 851-3.

[171] *Id.*, Article L. 851-6.

[172] Article 10-Act, 13 August 1968, §§ 5 & 8. Although a literal interpretation of the Article 10-Act would permit the BND to perform signals intelligence activities abroad between two foreign countries or within one single foreign country without the intercepted signals being connected to Germany (except for the actual data processing), this provision has not been applied to such activities.

telecommunications transmission paths. The BND may not monitor more than 20% of this capacity.[173]

The keywords used must relate to the specific threat identified and must not go beyond the scope of the order. Keywords using identifiers that lead to a targeted detection of specific telecommunications lines or that concern the core sphere of private life may not be used. However, the latter restrictions do not apply to telecommunications outside Germany – including in other EU Member States – provided such communications do not involve German nationals.[174] Likewise, if the interception measure is intended to avert an existing danger for life or limb of a person (*i.e.*, a Section 8-measure), the keywords may contain identifiers that lead to the identification of a specific telephone number or another identifier of the telecommunications line of the person abroad.[175]

Certain measures not targeted to specific individuals or organizations are also permitted pursuant to the German Code of Criminal Procedure to the extent these are aimed at identifying potential suspects or a group of potential suspects. The measures include the automatic comparison and transmission of personal data, the collection and processing of traffic data and the use of IMSI catchers.[176]

In *the Netherlands*, the implementation of surveillance not targeted to specific individuals or organizations is permitted via the use of keywords pursuant to Article 27(1) and Article 27(3) of the Intelligence and Security Services Act 2002, without the prior authorisation of the relevant minister.[177] Once the information is gathered, the list of keywords to be used for the "selection" of the data requires prior authorisation, and this can be granted by the relevant minister for a renewable period of one year, as opposed to a renewable period of three months where keywords are not used (as set out in Article 27(5)).

In *Poland*, the Foreign Intelligence Agency is permitted to carry out signals intelligence[178] activities outside of Poland, which are not targeted to specific individuals or organizations.

In *the UK*, there is no requirement to specify an identifiable person or premises in a warrant which relates to the interception of an external communication (*i.e.*, a

[173] *Id.* § 10(4); for further information regarding the interpretation of the 20% cap *see* Prof. Dr. Matthias Bäcker, Strategische Telekommunikationsüberwachung auf dem Prüfstand, Kommunikation & Recht 9/2014, 556 (558).

[174] *Id.* § 5(2).

[175] *Id.* § 8.

[176] Code of Criminal Procedure, Sections 98a, 100g and 100i.

[177] Intelligence and Security Services Act 2002, 7 February 2002, Article 27. Theoretically, any Minister can approve surveillance. However, in practice this will usually be the Minister of Justice and Security, the Minister of Home Affairs or the Minister of Defence. In any case, it is required that the relevant Minister in each specific case takes the responsibility for authorisation.

[178] Signals intelligence is intelligence-gathering via the interception of communication and electronic signals.

communication either sent and/or received from outside of the UK).[179] According to the UK Parliament's Intelligence and Security Committee, the Government's Communications Headquarters uses mass surveillance "to investigate the communications of individuals already known to pose a threat or to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security."[180]

The surveillance measures in all of the Illustrative Member States may inadvertently capture the data of third parties who are not the target of the surveillance. However, this is explicitly addressed in the surveillance laws only of some of the Illustrative Member States.

In *France*, the electronic communications of an individual connected to a person under administrative surveillance who is deemed likely to provide the services with relevant information, may also be intercepted.[181]

In *Germany*, the Act on the Protection of the Constitution permits the Federal Office for the Protection of the Constitution in certain circumstances to deploy technical measures to determine the location of an active mobile phone or to determine the device or card number of an active mobile phone. Personal data of a third party captured in the course of such measure may be collected if for technical reasons the collection cannot be avoided and if necessary to achieve the purpose of the measure. However, the personal data captured is subject to an absolute ban on use, and it must be deleted immediately after completion of the measure.[182]

In *Italy*, where a third party communicates with the target of certain surveillance measures, it is likely that the third party's contribution to the specific communication will become public during subsequent legal proceedings.[183]

In *the UK*, there is no specific reference in RIPA to the capture of third-party data but paragraph 3.1 of the Communications Code states that consideration must be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation.

Surveillance Targeted At Specific Individuals Or Organisations

All Illustrative Member States permit targeted surveillance (*i.e.*, surveillance of specific, identified individuals or organisations) including to prevent a crime where

---

[179] RIPA §§ 8(4) & 8(5).

[180] Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* 25 (12 March 2015).

[181] Internal Security Code, Article L.852-1-I°.

[182] [Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG)], 20 December 1990, § 9(4), http://www.gesetze-im-internet.de/bverfschg/index.html.

[183] Code of Criminal Procedure, D.P.R n. 447 of 22 September 1988, Articles 266 to 271.

one has not already been committed. The threshold level of suspicion for targeted surveillance required in each of the Illustrative Member States varies and in some instances is not provided for, as in Poland and the UK.

In *Belgium*, only to the extent that the surveillance is carried out by law enforcement do the surveillance laws expressly refer to a required level of suspicion. To this end, the Special Methods of Investigation Act states only where there is a "serious indication" that the individual is involved in a criminal offense (that may or may not have already taken place) can that individual be targeted.[184] In respect of surveillance measures carried out by the intelligence services, the surveillance laws do not explicitly refer to a required level of suspicion. The intelligence services are permitted to carry out surveillance to the extent an activity "threatens or potentially could threaten," for example, the internal or external interests of the state.[185]

In *France*, the level of suspicion for administrative surveillance is not explicitly referred to in the surveillance laws beyond a requirement that the surveillance be justifiable. Surveillance measures can be implemented where, for example, an individual's behaviour may pose a threat to certain fundamental interests such as, national security (*i.e.*, there is no requirement for the crime to have been committed already). In respect of judicial surveillance, there is however, no restriction as to the individuals who may be subject to surveillance, provided the surveillance measure aims at transcribing correspondence that is useful for the discovery of the truth as part of an investigation of felonies and misdemeanour for which the penalty is at least two years' imprisonment.[186] The Cour de cassation, the highest judicial body, confirmed that individuals may be subject to interception even if they are not necessarily the individuals against whom there is *prima facie* evidence of guilt.[187]

In *Germany*, the Code of Criminal Procedure requires "initial suspicion" for the implementation of surveillance measures against targeted individuals. This means that the facts must indicate that a criminal offence has taken place. The majority of types of surveillance are permissible only if the investigation of the facts or the determination of the whereabouts of the suspect would otherwise be rendered substantially more difficult or impossible.[188] In addition, interceptions of individual telecommunications under the Article 10-Act (Section 3-measures) also require a certain level of suspicion, while none of the German laws covering strategic

[184] Act on Special Methods of Investigation and Certain Other Methods of Investigation, 6 January 2003, Article 4.

[185] Intelligence and Security Services Act, Articles 7 & 8.

[186] Criminal Procedure Code, Article 100.

[187] Case Bull. crim. 1990, No. 286 of the Criminal Chamber of the Judicial Supreme Court, 17 July 1990; Case Bull. Crim. 1991 No. 465 of the Criminal Chamber of the Judicial Supreme Court, 9 December 1991.

[188] *See e.g.*, Code of Criminal Procedure, §§100a (1) No. 3, 100c (1) No. 4, 100f (1) & 100h (1).

communications surveillance (as distinguished from "individual measures") expressly refer to a threshold level of suspicion.

In *Ireland*, for surveillance justified by state security concerns or for the prevention of serious crime there must be "reasonable grounds for believing that particular activities that are endangering or likely to endanger the security of the State" are taking place or are proposed. In addition, there must be a "reasonable prospect that the interception … would be of material assistance."[189]

In *Italy*, with respect to surveillance as a means to gather evidence in ongoing criminal investigations, there must be a "serious indication" that the crime has been committed.[190] The level of suspicion for preventative surveillance (*i.e.*, surveillance carried out before a criminal investigation is initiated or in some cases a crime is committed) is not explicitly referred to beyond a requirement that the available findings of the investigation justify the surveillance.[191]

In *the Netherlands*, the intelligence services can implement surveillance measures where the actions of individuals or organizations lead to a "serious suspicion" that those actions pose a risk to the democratic rule of law, national security, or other important interests of the state.[192] This implies that the surveillance measures can be implemented in advance of the action taking place.

Duration Of Surveillance

The duration for which surveillance measures can be authorized varies among the Illustrative Member States depending on a number of factors, including, for example, the type of data collected, the surveillance measure implemented, and the purpose for the surveillance.

In *Belgium*, the Intelligence and Security Services Act, only specifies a duration for which "extraordinary intelligence methods" can be authorised. The duration is two months, and this can be renewed for a further two months by the head of the intelligence services, after having obtained the advice of the supervisory body (BIM-controlecommissie).[193]

In *France* and the *UK*, the period for which the authorisation is granted depends on the type of data being acquired. For example, in France, an authorisation for the acquisition of connection data by the intelligence services is usually granted for a period of four months whereas an authorisation for interception of "real-time"

---

[189] Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 (as amended), § 5.

[190] Code of Criminal Procedure, D.P.R. n. 447 of 22 September 1988, Article 267.

[191] Implementing Provisions of the Code of Criminal Procedure, Legislative Decree n. 271 of 28 July 1989, Article 226.

[192] Intelligence and Security Services Act 2002, 7 February 2002, Article 6(2)(a).

[193] Article 18/10 §§2 & 5 of the Intelligence- and Security Services Act.

connection data is usually only granted for two months and only where it is for the prevention of terrorism.[194] In the UK, warrants authorising the interception of communications are usually valid for three months and can be renewed by the Secretary of State for a further three months when issued in pursuit of a serious crime, or six months where issued on national interest or economic well-being grounds.[195] Authorisations in respect of communications data are valid for a maximum of one month but can be renewed for a further month.[196]

In *Germany*, the authorisation for the intelligence services to intercept communications is normally valid for a renewable three-month period, regardless of whether measures for the purpose of intelligence or law enforcement are concerned.[197] However, acoustic surveillance of the private home must be limited to a renewable period of one month.[198]

In *Ireland*, authorisations to intercept communications may be granted for a maximum of three months, extendable for a maximum of three months at a time.[199]

In *Italy,* the authorisation for surveillance varies according to the purpose of the surveillance. For surveillance used to gather evidence in a criminal investigation, authorisation is limited to 15 days or 40 days in cases where there is a serious likelihood of the crime being committed and where the surveillance is absolutely indispensable to continue the investigation.[200] In both instances the duration can be extended by the Judge of Preliminary Investigations. In contrast, preventative surveillance may be authorised for a term of 40 days, which can be extended for additional terms of 20 days by the Chief Prosecutor (for law enforcement) or the General Prosecutor of the Court of Appeal of Rome (for the intelligence services).[201]

In the *Netherlands*, the duration of the authorisation for surveillance by the intelligence services varies according to the type of surveillance. For example, the tapping of non-cable-bound telecommunications can be authorized for a renewable

[194] Internal Security Code, Articles L. 821-4 & L. 851-2. The duration of surveillance may be extended for data obtained from international electronic communications to four months or one year, depending on the type of data. Internal Security Code, Articles L. 854-2-II° & L. 854-2-III°.

[195] RIPA § 9.

[196] *Id.* § 23.

[197] *See e.g.*, Article 10-Act, §§ 8(1) & 10(5); BKAG § 20l (4); Code of Criminal Procedure Section 100b (1).

[198] Code of Criminal Proceeding, § 100d.

[199] Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, § 2(5).

[200] Code of Criminal Procedure, Article 267.

[201] Implementing Provisions of the Code of Criminal Procedure, Legislative Decree n. 271 of 28 July 1989, Article 226 and Law Decree 27 July 2005, n. 144, converted by Law 31 July 2005 n. 155, Art. 4.

period of three months. However, to the extent keywords are used, the authorisation can be granted for a period of one year.[202]

In *Poland*, an authorisation for "operational control" by the intelligence services can be granted for a maximum of three months but this can be extended for a further three months with the consent of the Attorney General and the District Court in Warsaw.[203] In justified cases, where in the course of "operational control" the intelligence services uncover new circumstances important for the prevention or detection of a crime or for establishing the identity of a perpetrator and obtaining evidence of a crime, an authorisation for "operational control" can be extended for a further specified period with the consent of the Attorney General and the District Court in Warsaw.[204]

Professional Secrecy

The concept of professional secrecy, or legal professional privilege as it is referred to in Ireland and the UK, introduces a specific limitation on the scope of surveillance. In *Kopp v Switzerland*,[205] the ECtHR accepted that "when national security is at stake there are no conversations for which surveillance should be prohibited but monitoring of this kind must be adequately supervised."[206] In Ireland and the UK, legal professional privilege and confidentiality are based on common law principles and are described as a fundamental feature of the rule of law. In the other Illustrative Member States, professional secrecy is based upon statute or other professional codes. In most of the Illustrative Member States the concept of professional secrecy is limited by one or more factors, for example, the professions covered or the type of surveillance for which the concept applies.

Belgium, France, Germany, Italy, the Netherlands, and the UK impose statutory limitations for accessing communications that are subject to professional secrecy. However, the extent of these limitations varies among the Illustrative Member States, and these are not always applicable to all surveillance measures.

In *Belgium*, intelligence agencies are permitted to make use of or exploit communications that are subject either to the professional secrecy of a lawyer or doctor, or the secrecy of a journalists' sources only in exceptional circumstances.[207]

In *France*, members of the parliament, judges, lawyers, and journalists cannot be subject to administrative surveillance measures in France for activities they pursue in

---

[202] Article 27 of the Intelligence- and Security Services Act.

[203] Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002, Article 27 (8).

[204] *Id.*, Article 27 (9).

[205] ECtHR 25 March 1998, *Kopp v Switzerland*, ECLI:CE:ECHR:1998:0325JUD02322494.

[206] ECtHR, *National Security and European Case-Law*, *supra* note 143, at 10.

[207] Act on Special Intelligence Methods by the Intelligence & Security Services, 7 February 2010, Article 2-2°-2.

accordance with their mandate or profession.[208] For judicial surveillance there are restrictions on intercepting telephone communications of members of the parliament, judges, and lawyers in certain circumstances.[209]

In *Germany*, an exemption for professional secrecy is not consistently applied. For example, there is an exemption found in Section 3 of the Article 10-Act,[210] but there is no equivalent exemption in Sections 5 and 8 of the Article 10-Act, which refer to strategic telecommunications surveillance.

In *Italy*, communications subject to professional secrecy cannot be recorded where the surveillance is authorised as a means of gathering evidence in criminal investigations.[211] However, there is no equivalent exemption for surveillance conducted to investigate certain serious crimes by the police or the intelligence agencies.[212]

In *the Netherlands*, data collected pursuant to the Criminal Procedure Code cannot be the subject of surveillance measures where such data is subject to professional secrecy unless the person profiting from the professional secrecy is the subject of the investigation. A recent summary judgment issued by the general court of The Hague ordered the Dutch State (i) to introduce a prior authorisation procedure before an independent body for the tapping of communications covered by legal privilege[213]; and (ii) to introduce an independent review before any data collected can be transferred to other government bodies (such as the public prosecutor).[214]

In *the UK*, there is no professional secrecy exemption in RIPA. In the recent case of *Belhadj & Others*,[215] the Investigatory Powers Tribunal[216] found that the UK Government's regime for the interception, analysis, use, disclosure, and destruction of legally privileged communications contravened Article 8 of the ECHR. Subsequently, provisions addressing professional secrecy were included in the amended Codes of Conduct published by the UK's Home Office in 2015.

---

[208] Internal Security Code, Articles L. 821-7 and L. 854-3.

[209] Criminal Procedure Code, Article 100-7.

[210] *See e.g.*, Article 10-Act, 13 August 1968, § 3(b).

[211] Code of Criminal Procedure, D.P.R. n. 447 of 22 September 1988, Articles. 200, 268 & 271.

[212] Implementing Provisions of the Code of Criminal Procedure, Legislative Decree n. 271 of 28 July 1989, n. 144, of 27 July 2005, converted by Law n. 155 of 31 July 2005.

[213] Rb. Den Haag, ECLI:NL:RBDHA:2015:7436, 1 Juli 2015, r.o. 4.13 and 4.14.

[214] *Id.* at 4.18.

[215] *Belhadj & Others v the Security Service, SIS, GCHQ, Home Office & FCO* (2015) IPT/13/132-9/H.

[216] The Investigatory Powers Tribunal is established under RIPA § 65(1).

Data Minimization

The principle of data minimization (*i.e.*, that the collection of data should be limited to what is directly relevant and necessary to accomplish a specified purpose) is not explicitly referred to in the surveillance laws of any of the Illustrative Member States. However, in the surveillance laws of Ireland, Poland, and the UK, there are indirect and limited references to the principle, as referred to below, and it is important to note that to the extent the surveillance activities are subject to applicable data protection laws, the processing of personal data will be subject to the general data protection principle of data minimization. Further, all the Illustrative Member States require that the surveillance should not be excessive in the circumstances.

In *Ireland*, communications obtained via surveillance must not be copied to a greater extent than is necessary.[217] Similarly, in the UK, the number of people who can access intercepted material (including communications data where such data is obtained pursuant to an interception of communications) and the extent to which the intercepted material is disclosed and copied is restricted to the minimum that is necessary.[218]

In *Poland*, the data minimization principle seems to apply following collection, to the extent that the intelligence services are required to destroy all information obtained via "operational control" that is not relevant for the purpose for which it was initially obtained.[219]

Retention And Storage

While the surveillance laws in the majority of the Illustrative Member States have differing provisions on retention of data, as discussed further below, none of the Illustrative Member States in their surveillance laws provide for specific statutory safeguards relating to the actual security of the data obtained via authorized surveillance measures beyond, in some instances, a general requirement to store such data securely.

Only in *France* and *Germany* do the surveillance laws include prescriptive retention periods, which vary according to the type of data collected. In *France*, the retention periods vary from 30 days for data collected via interception of communications (subject to a limited number of exceptions including where, for example, the data is encrypted) to six years for encrypted data.[220] However, these limits apply only with respect to administrative surveillance. In addition, in France the National Commission of Control of the Intelligence Techniques (CNCTR) can recommend the

[217] Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, § 12(1)(b)(i).

[218] RIPA § 15(2).

[219] Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002, Article 27 (16).

[220] Internal Security Code, Article L. 854-5. The Internal Security Code provides for longer retention periods up to 8 years for data obtained from international electronic communications (*i.e.*, emitted from abroad or received abroad).

interruption of surveillance and the destruction of the data collected.[221] In *Germany*, specific storage periods are provided for only in certain cases. For example, the personal data of minors must be deleted after five years, but this limit does not apply where additional findings are obtained after the minor reaches the age of 16.[222]

In *the Netherlands,* data acquired through tapping of non-cable-bound telecommunications[223] (*i.e.*, via a wireless connection) can be stored for a maximum of one year. However, there are no further prescribed retention periods and other categories of data are subject to a general requirement of retention only for as long as necessary for the purpose or objective sought. Retaining data for as long as necessary also applies in the other Illustrative Member States, except that in Poland there is no requirement for the intelligence agencies to delete data acquired from communications service providers once it is no longer necessary to retain such data.[224]

All of the Illustrative Member States (with the exception of Ireland) require the destruction of surveillance data following the expiry of the applicable retention period, if there is one. None of the surveillance laws specifies irreversible destruction.

On 8 April 2014, the CJEU in *Digital Rights Ireland* assessed the validity of Directive 2006/24/EC, which obliged EU Member States to provide for retention of data by telecommunication providers for between 6 and 24 months. The CJEU declared that Directive invalid for enabling interference with fundamental rights without providing, at the same time, measures to limit retention to the minimum necessary, to prevent abuse and to ensure data security. Because of this absence, the interference was not a proportionate instrument to pursue the legitimate aim of fighting crime.[225]

The *Digital Rights Ireland* judgment does not formally require Member States to repeal national laws adopted as a result of the Directive, and neither the Charter[226] nor the ECtHR would prohibit national laws permitting data retention in a system that limits retention to the extent necessary and provides for sufficient safeguards against abuse.

---

[221] Internal Security Code, Article L. 833-6.

[222] The Act on the Protection of the Constitution, 27 September 1950, § 11.

[223] The Intelligence and Security Services Act 2002 lays down specific rights to implement surveillance measures for "non-cable-bound telecommunications." This relates specifically to telecommunications that take place through the use of satellites. A legislative proposal amending the Intelligence and Security Services Act aims to introduce measures allowing the bulk surveillance of cable-bound communications. This rationale for this proposal is that, at present, 90% of internet traffic makes use of cable.

[224] Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002, Article 28.

[225] Joined cases C-293/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and C-594/12, Kärntner Landesregierung, Judgment of 8 April 2014.

[226] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Five of the Illustrative Member States still provide for retention of data by telecommunication providers despite the *Digital Rights Ireland* judgment and decisions by some national courts invalidating some of these data retention laws for failing to comply with that judgment.[227]

Other Illustrative Member States have acted to add safeguards to their data retention laws. In *Germany*, the former law on data retention was annulled in 2010 by the German Federal Constitutional Court on the basis that it violated the German Basic Law,[228] and the German Federal Council reintroduced a revised law on the retention of traffic and location data on 6 November 2015.[229] Consistent with the *Digital Rights Ireland* judgment, the new law provides for shorter retention periods and a detailed list of the types of data that can be stored.[230]

In both *Belgium* and the *Netherlands*, the existing data retention legislation has been declared invalid and new data retention laws have been proposed but not yet adopted. Similarly, the English High Court in the recent case of *Davis MP and Watson MP v. Home Secretary*[231] ruled that Sections 1 and 2 of the Data Retention and Investigatory Powers Act 2014 are incompatible with Articles 7 and 8 of the ECHR as these sections failed to provide adequate safeguards in respect of access to and use of communications data. The ruling was suspended until 31 March 2016 to give UK legislators time to implement appropriate safeguards. However, following an appeal by the UK government, the case has been referred to the CJEU.[232]

Other Member States have not acted to conform their laws with the *Digital Rights of Ireland* judgment. Of the Illustrative Member States, France, Ireland, Italy, and Poland do not appear to have taken any action. In Ireland, in particular, the Communications (Retention of Data) Act 2011 remains in effect with all the provisions identified in the CJEU judgment as grounds for the Directive's invalidity.[233]

---

[227] France – Code of Post and Electronic Communications; Ireland – Communications (Retention of Data) Act 2011; Italy – Legislative Decree n. 109 of 30 May 2008; Poland – Telecommunications Act of 16 July 2004; UK - Data Retention and Investigatory Powers Act 2014.

[228] BVerfG, 1 BvR 256/08, BVerfGE 125, 260-385 of 2 March 2010.

[229] Bundesrat Beschluss, zum Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten Ds 492/15 938 Sitzung, 6 November 2015 (Entwurf, Deutscher Bundestag, 18. WP, Ds. 18/5088, 9 June 2015, amended by Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz, Deutscher Bundestag, 18. WP, Ds. 18/6931, 14 October 2015).

[230] Deutscher Bundestag, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten of 9 June 2015 ("New Law on Data Retention"), WP 18, Ds. 18/5088, p. 12.

[231] *David Davis MP & Tom Watson MP v. Home Secretary* [2015] EWHC 2092 (Admin).

[232] *Secretary of State for the Home Department v. Davis MP & Others*, [2015] EWCA Civ 1185.

[233] This report does not assess minimization measures and safeguards that may be present in other laws in these Member States.

Sharing Of Data

Of the Illustrative Member States, only the surveillance laws in France, Germany, the Netherlands, and the UK make specific reference to sharing of data collected pursuant to surveillance measures.

In *France*, once the authorisation of the administrative surveillance measures has been granted, access to and use of the data by national authorities is permitted so long as the access and use are in line with the goals set out in Article L. 811-3 of the Internal Security Code.[234]

In *Germany*, personal data acquired pursuant to strategic telecommunications intelligence can be shared with foreign intelligence services in certain circumstances.[235] Likewise, such data can be shared with certain German authorities[236] providing specific criteria are fulfilled. For the transfer of personal data acquired pursuant to a Section-5 measure,[237] the transfer is permitted only if necessary for the fulfilment of the recipient's duties, and use of the data by the recipient is restricted to the purpose for which it was transferred.[238] Personal data acquired pursuant to a Section-8 measure[239] can be transferred in order to prevent a crime, providing actual indications to justify the suspicion that someone is planning or committing a criminal offense, which is likely to contribute to the development or maintenance of the danger to life or limb of a person abroad.[240]

Under the Dutch Intelligence and Security Services Act 2002, when the "proper task performance" so requires, the gathered data can be shared broadly including with other ministers, administrative bodies, persons, or agencies, and with foreign intelligence or security services.

In *the UK*, RIPA has a similar provision on sharing of data, which applies in respect of the interception of communications. It provides that the number of people who can access the intercepted material and the extent to which the intercepted material is disclosed and copied should be restricted to the minimum necessary. There is no

---

[234] Internal Security Code, Articles L. 822-3 & L. 854-6.

[235] Article 10-Act, 13 August 1968, § 7a.

[236] The applicable German authorities include the Chancellor's Office, the constitutional protection authorities of the federal and state governments and the Military Counterintelligence Service, the Federal Office of Economics and Export Control, authorities carrying out preventive Police and law enforcement activities and the Federal Office for Information Security.

[237] A Section-5 measure is surveillance implemented to detect and avert the danger of, *inter alia*, an armed attack against Germany, international terrorism, arms proliferation, smuggling of narcotics of substantial importance into the EU, money counterfeiting that undermines the stability of the Euro, money laundering, human trafficking of substantial importance, and cyber terrorism or cybercrime.

[238] Article 10-Act, 13 August 1968 §§ 7(5) & 7(6).

[239] A Section-8 measure is surveillance implemented where necessary to detect or avert an existing danger to life or limb of a person abroad, by which the interests of Germany are directly affected.

[240] Article 10-Act, 13 August 1968 § 8(6).

guidance on what should be considered necessary.[241] In addition, there is no restriction on sharing data obtained from service providers with foreign governments.

2.1.4 Oversight

There should be some combination of executive, legislative, judicial and expert oversight for approval and review of surveillance measures.

In the majority of the Illustrative Member States, there is some combination of executive control, legislative review, judicial review, and expert bodies that monitor surveillance measures both before and after implementation. The systems of the Illustrative Member States vary greatly, and in several of the Member States supervisory control is exercised by non-judicial bodies.[242]

Across the Illustrative Member States, there is a patchwork of judicial and non-judicial processes for prior authorisation for certain surveillance measures, and within Member States, these can vary depending on the type of surveillance measure and type of data captured.

There are often specific exemptions from prior authorisation, for example, in Belgium where no prior authorisation is required to carry out "ordinary intelligence methods" or "specific intelligence methods." Likewise, in the Netherlands the intelligence services are permitted to receive and record non-cable bound, untargeted, cross-border telecommunications without a prior authorisation.

In addition, all Illustrative Member States have provisions allowing some surveillance in exigent circumstances without prior authorisation, provided it is limited, authorized, or subject to prompt review.

In comparison to prior authorisation, the level of post-implementation review varies considerably among the Illustrative Member States depending on, the surveillance measures used, and the types of data collected.

In *Belgium*, under the Act on Special Methods of Investigation (which governs the investigative powers of law enforcement),[243] surveillance measures may be authorized only by the public prosecutor or, as the case may be, by the investigating judge (in the context of an ongoing criminal investigation). Once an investigation is closed, the Chamber of Incrimination will review the legality of the surveillance

[241] RIPA § 15(2).

[242] Since *Klass,* § 56, the ECtHR has taken the position that "although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control." See also *Zakharov*, § 275, and the list of bodies considered acceptable by the Court in § 278 of that same judgment, including bodies composed of members of parliament of both the majority and the opposition; persons qualified to hold judicial office. By contrast, political appointees involved in surveillance, and prosecutors were not considered to be sufficiently independent.

[243] Act on Special Methods of Investigation and Certain Other Methods of Investigation, 6 January 2003.

measures. Where an investigation proceeds to a criminal trial, the criminal judge is also competent to review the legality of the surveillance measures used. In instances where surveillance measures were used but no prosecution was made, the public prosecutor must send the relevant file to the Board of Public Prosecutors for their review.

The Special Intelligence Methods Act (which governs the investigative powers of the intelligence and security services in Belgium) provides for two separate control mechanisms. The first is a regular oversight body (BIM-controlecommissie), which consists of three members (a representative of the public prosecutor, a judge, and an investigation judge, who presides); they supervise the legality of the surveillance methods used and adherence to the principle of proportionality. The second is the Permanent Committee on the Intelligence and Security Services (Permanent Committee I), which monitors the appropriate implementation of the special intelligence methods both before and after implementation.

The BIM-controlecommissie grants prior authorisation for "extraordinary intelligence methods" (*i.e.*, those that apply in the case of a serious threat and may involve the interception of contents of communications). If the BIM-controlecommissie does not give authorisation within four days, then the methods are assumed prohibited. No prior authorisation is required with respect to "ordinary intelligence methods" or "specific intelligence methods," but in cases of the latter, the intelligence services must provide the BIM-controlecommissie with a list of all the methods used in the preceding month.

During an investigation, the BIM-controlecommissie has the right to enter the premises of the intelligence and security services to hear their employees. When the BIM-controlecommissie establishes an infringement of the Special Intelligence Methods Act, it will prohibit further use of the relevant data and will inform the Permanent Committee I of its findings.

The Permanent Committee I monitors compliance with the Special Intelligence Methods Act both during and at the end of the surveillance. The investigations by the Permanent Committee I may be initiated in several ways, including on its own initiative, at the request of the "Committee for the protection of the private life" (Commissie voor de bescherming van de persoonlijke levenssfeer),[244] or following a complaint from an interested party. The Permanent Committee I reports to the judicial authorities (gerechtelijke overheden), and its activities are supervised by the Belgian Senate. Investigations of the Permanent Committee I may result in the suspension of the surveillance measure or the subsequent use of data, or the destruction of such data. Reports made by the Permanent Committee I are publicly available.

In *France*, the implementation of surveillance measures in connection with criminal proceedings must be granted in advance and in writing by either the investigating judge (juge d'instruction) or the liberty and detention judge (juge des libertés et de la

[244] The Committee for the protection of the private life is an independent body established by the Belgian Parliament. The Committee consists of 16 members, of which the President of the Parliament is a permanent public official.

détention) based on a finding that the measures are useful to the discovery of the truth.[245]

The implementation of surveillance measures for the intelligence services are subject to the prior authorisation of the Prime Minister, although the standards the Prime Minister must apply are not specified. The Prime Minister's decisions are subject to prior, non-binding review by the CNCTR.[246] In an emergency the Prime Minister may grant an authorisation without first consulting the CNCTR, although the CNCTR must be informed of such a decision as soon as possible together with the basis of the emergency.[247]

The CNCTR, an administrative authority that is independent from the executive, was established under the 2015 Intelligence Law to ensure that surveillance measures are carried out lawfully in France.[248]

When giving an opinion on the implementation of a surveillance measure, the CNCTR assesses whether the request has been lodged according to the correct procedure and whether the request respects the right to privacy and the principle of proportionality.[249] Should the CNCTR consider a surveillance measure unlawful, it can recommend that the surveillance be interrupted and the collected data destroyed. The Prime Minister must immediately inform the CNCTR about how the recommendation was followed up. If the CNCTR takes issue with the Prime Minister's response to its recommendation, it can bring the case before the Council of State (a judicial authority).[250] The CNCTR also has a right of permanent and general access to all data collected, as well as some general powers such as issuance of public reports or general comments to the Prime Minister.[251]

The CNCTR publishes an annual report summarizing its activities. It gives information on the number of: (i) requests and opinions delivered; (ii) claims submitted; (iii) recommendations to the Prime Minister and positive answers given to

[245] Criminal Procedure Code. Article 100.

[246] The CNCTR comprises nine members: two members of the National Assembly (Assemblée nationale), two members of the Senate (Sénat), two members of the Council of State (Conseil d'Etat), two judges of the Judicial Supreme Court (Cour de cassation), and one expert in electronic communications. The President of the CNCTR is appointed by the President of the Republic among the members of the CNCTR belonging to the Council of State or Judicial Supreme Court. *See* Internal Security Code, Article L. 831-1.

[247] Internal Security Code, Article L. 821-5.

[248] *Id.*, Articles L. 833-1 & L. 833.2.

[249] Article L. 833-5 combined with Article L. 801-1 set the main principles of administrative surveillance: legitimate authority, legal procedures, justified goals linked with fundamental interests of France, and the principle of proportionality.

[250] *Id.*, Article L. 833-8.

[251] *Id.*, Article L. 833-2.

those recommendations; (iv) general opinions delivered on request to the government; and (v) challenges before the Council of State.[252]

In *Germany*, the use of strategic telecommunications intelligence is subject to the approval of the Federal Ministry of the Interior, whereby the relevant telecommunications connections are determined in advance by both the Federal Ministry of the Interior and the Parliamentary Control Panel (PKGr).[253] In cases of emergency, the competent federal ministry can make a preliminary determination of the relevant telecommunications connections. The consent of the PKGr's Chairman and deputy (as opposed to the entire PKGr) has to be obtained immediately as this preliminary determination will be null and void if the preliminary approval is not obtained within three days and if the consent of the entire PKGr is not provided within two weeks.

Other than in cases of emergency, the German Federal Ministry of the Interior must inform the G-10 Commission of any surveillance order prior to its execution and at least on a monthly basis. In cases of imminent danger ("exigent circumstance"), an order may be executed prior to informing the G-10 Commission.

To the extent an information request is deemed not permissible or necessary, the Federal Ministry of the Interior is required to revoke its order immediately. In cases where data has been captured in the meantime, such data must not be used and must be deleted immediately. If a surveillance measure has been completed, the G 10-Commission decides whether the person concerned can be notified.

Surveillance measures carried out pursuant to the Article 10-Act are subject to the supervision of the PKGr and the G-10 Commission. The members of the G-10 Commission are appointed by the PKGr. The G-10 Commission in turn operates in lieu of a court to assess the legality and necessity of surveillance measures; it is an independent body in that it must not receive instructions from the intelligence services or any other public body in the course of its decision-making. The G-10 Commission's power of review extends to the entire processing of personal data obtained by the Federal intelligence services pursuant to the Article 10-Act. In principle, the G-10 Commission is exclusively competent to monitor the data processing of the services under its supervision. However, it can request the Federal Commissioner for Data Protection to provide an opinion on data privacy-related issues although, these opinions are non-binding recommendations in so far as they relate to surveillance.[254]

The PKGr is responsible for scrutinizing the intelligence services' work at a Federal level. It also receives reports every six months from the Federal Ministry of the Interior on the implementation of the Article 10-Act, and it reports annually to the

---

[252] *Id.*, Article L. 833-9.

[253] The members of the Parliamentary Control Panel are appointed by the Bundestag at the beginning of each legislative period, requiring a majority vote for each elected member. It is currently composed of nine members who belong to parties represented in the Bundestag. The ratio of the members corresponds to the ratio of the parties in the Parliament.

[254] Article 10-Act, 13 August 1968, § 15(5).

Bundestag on the implementation and nature and scope of measures adopted under the Act. The PKGr can request access to, *inter alia*, records and files of the intelligence services, may conduct interviews of members of the intelligence services, and has access to all departments of the intelligence services. In exercising its supervisory duties, the PKGr may entrust an expert to carry out studies upon approval by a majority of two thirds of its members.

In *Ireland*, the system in the Criminal Justice (Surveillance) Act 2009 (which regulates surveillance authorized under the Interception Act) is subject to direct judicial control – applications for authorisations must be made and justified to the courts.

In contrast, the authorisation system under the Interception Act remains outside prior judicial control and is instead under the political control of authorisation by the Taoiseach (Prime Minister). This is despite a significant political scandal in 1983 (one of the contributing factors to the adoption of the Interception Act) in which the government was found to have authorised the tapping of journalists' phones around the time of a potential political leadership challenge.[255]

A Designated Judge (a judge of the Irish High Court) with a general oversight function is in charge of writing an annual report for submission to the Taoiseach.[256] In addition, a judge of the lower Circuit Court is empowered as a Complaints Referee to investigate complaints by members of the public who believe their communications have been intercepted. The Complaints Referee has the power to investigate, quash any invalid interception, report the matter to the Taoiseach, and recommend compensation. As individuals typically do not know (and are not entitled to know) whether they have been the subject of surveillance and therefore may have no basis on which to contact the Complaints Referee, this Designated Judge system does not appear to have produced effective oversight in practice.

In *Italy*, surveillance measures conducted in connection with criminal investigations are overseen by the Judge of Preliminary Investigations and the Public Prosecutor. Prior authorisation for the surveillance is granted by the Judge of Preliminary Investigations upon the request of the Public Prosecutor. In cases of emergency, the Public Prosecutor can provisionally authorise the surveillance, subject to confirmation by the Judge of Preliminary Investigations. If the Judge of Preliminary Investigations does not provide such confirmation, the data is immediately erased and cannot be used.[257]

---

[255] *'Ireland's Watergate': How the Phone Tapping Scandal Would lEad to Haughey's Downfall … Eventually*, THE JOURNAL (27 Dec. 2013), http://www.thejournal.ie/what-was-the-phone-tapping-scandal-1983-1232800-Dec2013/.

[256] The reports for 2010, 2011, 2012 and 2013 are available and often constitute just one page, concluding that "the relevant State authorities are in compliance," without further elaboration or explanation of the powers assessed. *See, e.g.*, *Report of the Designated Judge Pursuant to Section 8(2) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and Section 67(1) of the Criminal Justice (Terrorist Offences) Act 2005* (2010), http://www.scribd.com/doc/58099350/Interception-and-Data-Retention-Annual-Report-2009-10.

[257] Code of Criminal Procedure, D.P.R n. 447 of 22 September 1988, Article 267.

Preventative surveillance carried out by the intelligence services is subject to oversight and prior authorisation by the General Prosecutor of the Court of Appeal of Rome. The General Prosecutor is part of the judiciary branch and therefore independent from other government branches.[258] The Prime Minister can authorise the Directors of the Secret Services to request the General Prosecutor to conduct preventive surveillance.

The Parliamentary Committee for the Security of the Republic (COPASIR) exercises political oversight of preventative surveillance. The COPASIR's function is to ensure that the activities of the intelligence services are performed in compliance with the law and in the exclusive interest of the State and its institutions.[259] In this respect, the COPASIR must regularly inform the Parliament and may hold hearings with the Prime Minister, the General Directors of the Secret Services, and the intelligence services' agents. In addition, the COPASIR can request documents from the intelligence services and inspect their offices.[260]

The Prime Minister and the Department of Security Information (which oversees the activities of the intelligence services) have certain information obligations to the COPASIR. In particular, the Prime Minister reports on the activities of the intelligence services every six months, and must inform the COPASIR every time a prosecutor is denied access to information on state secrecy grounds.[261]

The Italian Data Protection Authority (the Garante) may also review from a data privacy perspective the surveillance measures and suggest remedies to the extent they are non-compliant with the applicable laws. However, these communications from the Garante are not binding. If the Garante's review was initiated at the request of a third party, the Garante must notify that party of the outcome of the review.[262] The Garante can also initiate reviews autonomously, and there are examples of the Garante having exercised this authority in the past.

In *the Netherlands*, the authorisation required in advance of conducting surveillance varies depending on the type of surveillance. For example, for the seizure of letters and other physical mail a prior court authorisation is required, whereas for targeted tapping of non-cable-bound telecommunications (*i.e.*, via a wireless connection), authorisation from the relevant minister is required. Conversely, for tapping of non-cable-bound cross-border telecommunications (*i.e.*, telecommunications that originate outside of the Netherlands), no prior authorisation is required.

To the extent the surveillance is conducted by the police, as a general rule, the public prosecutor can grant them prior authorisation for the surveillance. However, in certain instances, such as for the recording of communications through telephone

[258] Italian Constitution, Article 104.

[259] Law n. 124 of 3 August, Article 30.

[260] *Id.*, Article 31.

[261] *Id.*, Article 33.

[262] Legislative Decree n. 196 of 30 June 2003 (Data Protection Code), Article 160.

or other computerized devices, the prior authorisation of the judge of instruction (rechter commissaris) is required.[263] As such, the type of authorisation required depends on the intrusiveness of the surveillance implemented.

The general activities of the intelligence services (including the legality of surveillance measures used) are overseen by the Review Committee for the Intelligence and Security Services (CTIVD).[264] The CTIVD is an independent oversight body consisting of three members appointed by royal decree by the government from a list of candidates submitted by Parliament. The CTIVD is required to inform and advise the relevant ministers concerning investigations and decisions following complaints and has the power to demand direct access to data that has been gathered, hear individuals under oath, and access any property (excluding residential property) without authorisation.[265] The CTIVD is also required to publish an annual report.

As part of the supervision of collection and use of police data, the Police Data Act provides that the person responsible for this gathering and subsequent use is required to keep a written account of: (i) the purpose of the investigation; (ii) the data gathered; (iii) the authorisations obtained; (iv) the automated use of the data; (v) each subsequent use of the police data; (vi) the transfer of data to other agencies; (vii) indications that use of data has taken place in an unlawful manner; and (vii) any automated comparison of data.[266] The information is retained for periodic audits conducted by the Committee for the protection of personal data (College bescherming persoonsgegevens, CBP) and to respond to requests from individuals for their data.[267]

The CBP acts as an independent oversight body.[268] It consists at most of three people appointed by royal decree for a term of five years, which is renewable once, and it is assisted by an advisory committee. The CBP's supervisory powers are laid down in the Personal Data Protection Act apart from the internal supervision detailed above (*e.g.*, periodic audits), the CBP is responsible for external supervision of collection and use of police data.[269] The CBP has the authority to start investigations upon its own initiative, or it can be requested to do so. If an infringement is found,

[263] The judge of instruction is a single judge within a specific case. The judge takes a particular role within proceedings, *e.g.*, to take a decision in respect of the use of surveillance measures.

[264] The CTIVD (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten) was established in 2002 and assigned pursuant to the Intelligence and Security Services Act 2002.

[265] Intelligence and Security Services Act 2002, 7 February 2002, Articles 73–77.

[266] Police Data Act, 21 July 2007, Article 32(1).

[267] *Id.*, Articles 25 & 33.

[268] Personal Data Protection Act, 6 July 2000, Article 52.

[269] *Id.*, Article 35.

the CBP has the power to order a cease and desist, or to lay down an administrative fine.[270]

In *Poland*, prior authorisation for surveillance is granted by the Attorney General. In cases of emergency, where delay would cause loss of information or erasure or destruction of evidence of a crime and with the prior written consent of the Attorney General, the head of the Internal Security Agency may authorise surveillance by submitting an application to the District Court in Warsaw, requesting a decision on the matter. If the court does not approve the request within five days, the head of the Internal Security Agency must suspend the surveillance immediately. No prior authorisation is required to the extent the data collected is deemed indispensible for the performance of the intelligence services duties (*e.g.*, telecommunications data).[271]

In *the UK*, the authorisation required for surveillance measures varies depending on the surveillance measure and the type of data captured. For interception of communications, a warrant must be issued by the Secretary of State (usually the Home Secretary or the Foreign Secretary)[272] or, where the Secretary of State is absent, a senior official under the authority of the Secretary of State. Exceptions apply where both the sender and recipient consent to the interception or where the Secretary of State has issued regulations authorising interception by a system controller for specified lawful business practices.[273] The interception of external communications requires, in addition to a warrant, a certificate from the Secretary of State describing the material that may be examined and confirming the necessity of the interception.[274]

The acquisition of "communications data" (as the UK refers to metadata) does not require the issuance of a warrant, and a designated person holding a prescribed office within the relevant public authority seeking the data may grant an authorisation or give a notice to a communications service provider requiring it to obtain and disclose specified communications data. An authorisation will be required only in exceptional circumstances, for example where the provider is not capable of obtaining the communications data. The Secretary of State can restrict the types of data that may be accessed by a public authority as well as the purposes for which the data may be used.[275] The Protection of Freedom Act 2012 amended RIPA by inserting two new sections that now require the Magistrate Court's approval only with

[270] The CBP has in the past exercised this authority. For example, in 2015 the CBP commenced an investigation into the use of telephone numbers of people close to a football stadium following riots between fans. Text messages were sent to 17,000 people that were in the area of the stadium after requesting these telephone numbers from a telecommunications provider.

[271] Act on Internal Security Agency and Foreign Intelligence Agency, 24 May 2002, Article 28.

[272] Ian Brown, *Government Access to Private-Sector Data in the United Kingdom*, 2 INTERNATIONAL DATA PRIVACY LAW 230 (2012), http://idpl.oxfordjournals.org/content/2/4/230.full.pdf+html

[273] RIPA §§ 3 & 4(2).

[274] *Id.* § 8(4).

[275] *Id.* § 25(3).

respect to a local authority's issuance of an authorisation or notice to obtain communications data.[276]

Directed surveillance is covert but not intrusive (*i.e.*, it should be carried out in a public place or via a remote location) and must be authorized by a designated person.[277] Only those authorities listed in Schedule 1 of RIPA are permitted to carry out directed surveillance. Authorisations for intrusive surveillance may be granted by the Secretary of State or a senior authorising officer.[278] Depending on the senior authorising officer, prior approval for the authorisation may be required from the Office of Surveillance Commissioners.[279]

The office of the Interception of Communications Commissioner (IOCC) was established to review the exercise and performance of the powers and duties established under RIPA.[280] The IOCC reports directly to the Prime Minister at least twice a year and the Prime Minister presents a copy of the reports (which may be redacted) to Parliament.[281] The IOCC "cannot disclose the details of any individual warrant or communications data acquisition."[282] RIPA also provides for the appointment of an Intelligence Services Commissioner (ISC) to supervise the activities of the intelligence services. The ISC has similar reporting obligations to those of the IOCC. The Office of Surveillance Commissioners oversees the use of covert surveillance (including directed and intrusive surveillance) by all public authorities based in the UK, but does not oversee the intelligence services. The Office of Surveillance Commissioners also oversees the operation of Part III of RIPA (*i.e.*, access to protected electronic information which has, for example, been subjected to encryption). Notably, neither of these entities has within their remit a duty to oversee or review access to communications data (metadata).

The UK also has an Investigatory Powers Tribunal (IPT), which consists of ten Members appointed by Her Majesty The Queen, who must be senior members of the legal profession, including a President and Vice-President who both must have held high judicial office. The IPT has exclusive jurisdiction to hear and determine complaints about conduct in connection with covert techniques by a public authority regulated under RIPA or a wider human rights breach by the intelligence agencies. Indeed, the IPT is the only appropriate tribunal in relation to proceedings for actions incompatible with the ECHR. In addition, the First-tier Tribunal (Information Rights) hears appeals from individuals in respect of decisions issued by the Information

---

[276] *Id.* §§ 23A & 23B.

[277] Directed surveillance must be carried out for the purposes of a specific investigation or operation and be likely to result in the obtaining of information about a person's private or family life.

[278] RIPA § 32.

[279] *Id.* § 36.

[280] *Id.* § 57.

[281] *Id.* § 58(6).

[282] David Anderson Q.C., *A Question of Trust – Report of the Investigatory Powers Review* 119 (2015).

Commissioner's Office in response to a freedom of information request. This tribunal is independent of the government.

2.1.5 Legal Remedies And Redress

The public should be informed about surveillance laws and have some opportunity for access and rectification, and for judicial redress. If necessary for legitimate aims of surveillance, surveillance can be secret, in which event oversight or more general legal redress are necessary.

The EU legal order recognizes that, in the context of surveillance and investigations, the principle of access and rectification can be limited by the need to maintain the effectiveness of necessary surveillance measures. In practice, the available remedies in the Illustrative Member States vary significantly from judicial mechanisms with proceedings brought before the national courts to ones that use non-judicial bodies, such as DPAs, ombudsmen, and parliamentary committees.

In addition, pursuit of a legal remedy or redress in relation to national surveillance faces practical limitations. First, access to alternative non-judicial remedies is constrained by broad exemptions for national security and limited powers of DPAs or other remedial authorities in the field of national security. Second, the secret nature of most surveillance means that an individual is likely to be unaware of the factual basis for a claim. And third, a lack of information raises difficulties in terms of legal standing and obtaining evidence, and results in limited case law.

These limitations add to the role of effective oversight mechanisms to identify and rectify potential abuse of surveillance powers.

Preconditions To Remedial Action – Informing The Individual And Rights Of Access

The ECtHR has recognized that "the fact that persons concerned by such measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not 'necessary in a democratic society,' as it is the 'very absence of knowledge of surveillance which ensures the efficacy of the interference.'"[283] Indeed, legal frameworks in all the Illustrative Member States allow restrictions on access to knowledge of surveillance and the right of access to data on the basis of exemptions under national security laws. There is no uniformity on how these restrictions are applied.

In most of the Illustrative Member States, the national laws do not provide an obligation to inform the individual about surveillance activities or a right of access to their personal data held by surveillance bodies; in some, the obligation to inform and rights of access are explicitly restricted because of rules applicable to classified documents and official secrets; and only a small number of Illustrative Member States allow for indirect and restricted access through supervisory authorities. But even in those Member States, there are exceptions notably with regard to security surveillance outside the scope of law enforcement.

[283] *Weber & Saravia*, § 135 (citing *Klass*, § 58).

In *Belgium*, access to personal data must be refused if the data is classified pursuant to Article 3 of the Classification Act[284] (*i.e.*, for a variety of national interests). Similarly, in Ireland, data protection safeguards do not apply to personal data that in the opinion of the Minister for Justice or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State.[285] In addition, a telecommunications provider is prohibited under the Interception Act from disclosing information relating to requests for information made by the police or confirming whether such requests have been made.

In *Germany*, a general right to access and rectify data collected by a public authority explicitly excludes activities of the federal intelligence services.[286] Likewise, in *the Netherlands*, the intelligence services may set aside the obligations under the Dutch Personal Data Protection Act that relate to notification and access to data.[287]

In *Poland* and in *the UK*, the right to information and right to access are not expressly provided for in the surveillance laws, except that in the UK, the Communications Code explicitly acknowledges the exemption to subject access rights possible under Sections 28 and 29 of the Data Protection Act 1998 (*i.e.*, where personal data is processed for the purposes of the prevention and detection of crime or safeguarding national security). Section 28(2) of the Data Protection Act 1998 states that a ministerial certificate stating such an exemption is required will be conclusive evidence of this fact.[288] However, in the case of *Norman Baker MP v Secretary of State,*[289] the Information Tribunal (for national security appeals)[290] quashed a ministerial certificate, ruling that whilst it may be reasonable to refuse to release information where this would be prejudicial to national security, a blanket policy to this effect is unreasonable and applications should be considered on an individual basis. The reasoning for the quashing of the certificate included that "limited evidence as to the practice in other countries did not identify anywhere

---

[284] Act on the Classification and the Security Authorisation, Security Certificates and Security Advice (Classification Act), 11 December 1998, Article 3.

[285] Ireland Data Protection Act 1988 (as amended), § 1(4)(a).

[286] *See, e.g.*, BVerfSchG, 27 September 1950, § 27; The Act on the Military Counterintelligence Service [Gesetz über den militärischen Abschirmdienst (MAD-Gesetz - MADG)] 20 December 1990, § 13; the Act on the Federal Intelligence Service [Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG)] 20 December 1990, § 11 of the BNDG.

[287] Personal Data Protection Act, 14 January 2003, Article 43.

[288] Communications Code, paras. 7.5 and 7.6. The UK Anderson Report recommends that an Independent Surveillance and Intelligence Commission be created that would be in charge of informing an individual of an error on the part of the public authority or communication service provider and notifying individuals of their right to lodge an application to the IPT, on their own initiative or at the suggestion of the public authority or communication service provider. Anderson, *A Question of Trust – Report of the Investigatory Powers Review*, *supra* note 282, at 303.

[289] *Norman Baker MP v Secretary of State for the Home Department* [2001] U.K.H.R.R. 1275.

[290] In 2010 the Information Tribunal became part of the General Regulatory Chamber of the First-tier Tribunal (Information Rights). This Chamber hears appeals from notices issued by the Information Commissioner regarding breaches of UK data privacy laws.

where an identical unchallengeable exemption was permitted. Notably the practice in the [US] was more considerate of individual rights than the practice in the [UK] exemplified in these proceedings."[291]

In allowing for secrecy during and after the conduct of surveillance, the ECtHR has also stated that "as soon as notification can be made without jeopardizing the purpose of the surveillance after its termination, information should be provided to the persons concerned ...."[292] Several Illustrative Member States have provisions that allow notification of surveillance some time after it has occurred, at least with respect to law enforcement surveillance.

In Belgium, Germany, and the Netherlands, individuals are notified or information is provided at the end of the surveillance on the assumption that up to that time the threat to national security will persist throughout the surveillance period.

In *Belgium*, under the Special Intelligence Methods Act an individual is to be informed, upon request, five years after the surveillance has ended. In 2011 the Belgian Constitutional Court declared this provision unconstitutional and called for the intelligence services to take the initiative to inform the data subjects regardless of whether a subject has made such a request.[293]

In *Germany*, the Federal Data Protection Act (the BDSG)[294] provides for the right of access to personal data collected by a public authority and to seek the correction, erasure, and blocking of such data regardless of whether a data subject is a citizen.[295] In the context of criminal investigations in Germany, the investigating authorities have to provide information to a person concerned, upon request, unless otherwise regulated in the law.[296] One exception to this obligation applies to information requests on pending proceedings initiated less than six months before the request for information is filed. In addition, the German Code of Criminal Procedure requires investigating authorities to inform certain individuals concerned by a measure as soon as such notification does not endanger the purpose of the investigation; the life, physical integrity, and personal liberty of another person; or significant assets.[297] A similar provision is included in the Law on the Establishment of a Federal Criminal Police Office (the BKAG).[298] However, while the German Code

[291] Norman Baker, U.K.H.R.R. 1275, para. 113(i).

[292] ECtHR 28 June 2007, *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, ECLI:CE:ECHR:2007:0628JUD006254000.

[293] Belgium Constitutional Court No 145/2011, 22 September 2011.

[294] Bundesdatenschutzgesetz (BDSG), published on 14 January 2003 (Federal Law Gazette I page 66) was last amended by Article 1 of the law dated 25 February 2015, (Federal Law Gazette I page 162).

[295] BDSG, 14 January 2003, §§ 19 & 20.

[296] Code of Criminal Procedure, § 491.

[297] *Id.*, §§ 101(4) & (5).

[298] The Law on the Establishment of a Federal Criminal Police Office, 7 July 1997, § 20w (1) No. 7 & (2).

of Criminal Procedure also requires that the individual be informed about applicable legal remedies, the BKAG does not.

In *Italy*, where surveillance is used as a means to gather evidence in an ongoing criminal investigation, counsel for the subject under investigation is notified immediately.[299] However, there is no equivalent provision in the surveillance laws governing disclosure of preventative surveillance.

In *the Netherlands*, individuals are notified five years after the intelligence security services have carried out special surveillance measures, such as opening letters, intercepting telecommunications and intercepting non-cable bound telecommunications. However, the notification may be postponed if the data is still needed in the investigation.[300]

Of the Illustrative Member States, only in Germany do the surveillance laws distinguish between the obligation to inform an individual in a case of targeted surveillance as against the obligation to do so when an individual is targeted as a result of signals intelligence. In Germany, the obligation to inform does not apply to data that are immediately deleted after they have been captured through the use of selectors used in signals intelligence.[301]

Belgium, France, and Italy provide for limited and indirect access through inquiry by data protection authorities. In Belgium, a request for access can be made to the Privacy Commissioner.[302] The access to personal data must be refused when the data is classified according to Article 3 of the Classification Act (*e.g.*, if the data could harm the internal or external security of the state). However, the Privacy Commissioner cannot make binding decisions.

In *France*, where the processing of the personal data involves state security, defence or public safety, individuals have only a "right of indirect access." In practice, this means that the request to access and check the data must be made to the French Data Protection Authority (CNIL). After investigations, the applicant is informed that necessary investigations have been carried out; the extent that the CNIL establishes, with the agreement of the data controller, that the disclosure of data does not undermine the purposes for its collection, *i.e.*, the state security, the defence or public safety, the data may be disclosed to the applicant.[303]

In *Italy*, interested persons can seek the erasure of any data being used or stored illegally from the competent court or the Garante.[304]

---

[299] Code of Criminal Procedure, D.P.R. n. 447 of 22 September 1998, Article 268.

[300] The Intelligence and Security Services Act 2002, 7 February 2002, Article 47.

[301] FRA Report, *supra* note 127, at 65.

[302] Article 13 of the Access to Personal Data Act (Wet verstrekking persoonsgegevens).

[303] Law No. 78-17 on Information Technology, Data Files and Civil Liberties, 6 January 1978, Article 41.

[304] Legislative Decree n. 196 of 30 June 2003 (Data Protection Code), Articles 141 & 145.

Judicial And Non-Judicial Remedies

In the Illustrative Member States, the national courts present a means by which individuals can seek remedies for breach of their data protection and privacy rights in some cases (but generally individuals cannot sue to obtain access to their personal data gathered in security surveillance). The national laws and court procedures of the Illustrative Member States determine which courts (if any) are competent to review surveillance complaints. In addition, in some of the Illustrative Member States, forms of redress are available from non-judicial bodies such as DPAs, ombudsmen, and parliamentary committees. However, for non-judicial bodies there can be questions concerning their independence, particularly where they also have power to issue warrants and, in the case of DPAs, their powers over intelligence services often are limited and usually deal with administrative processes rather than the substantive basis for the surveillance.

Further, while redress from non-judicial authorities may be more accessible, faster, and cheaper, as there is less procedure than with the courts, the degree to which these bodies can provide an effective remedy depends on factors such as their specialized knowledge, powers to investigate, and whether their decisions are actually binding; in many cases non-judicial authorities only are able to make non-binding recommendations.

In *Belgium*, the Permanent Committee I was introduced to deal with national surveillance cases. The Permanent Committee I has a quasi-judicial function, investigating complaints and rules on the legality of intelligence measures; it has the power to order cessation when it observes that the surveillance measures are no longer useful, when the threat that justified the surveillance measure has subsided or when it has observed an "illegality."[305] The Permanent Committee I has specialized expertise in surveillance.

In *France*, any individual who wants to verify that surveillance measures against him or her were lawfully carried out may request the CNCTR conduct such verifications.[306] Once notified by the CNCTR that such verifications have been carried out, the individual may challenge the implementation of the surveillance measure before the Council of State, the highest administrative tribunal in France.[307] The Council of State checks if all of the legal procedures have been followed in the particular case, if the data collected is correct, and if the retention period has expired. It can then inform the applicant that all of the verifications have been made. If something unlawful has been undertaken, the Council of State can order measures to rectify this and provide the applicant with the requisite information without giving any information that would undermine the secrecy of national defence.[308]

---

[305] Intelligence and Security Services Act, 30 November 1998, Article 18/10.

[306] Internal Security Code, Articles L. 833-4 & L. 854-6.

[307] *Id.*, Article L. 841-1.

[308] See also discussion of "right of indirect access" via the CNIL, *supra* Part 2.1.5.

In *Germany*, Section 13 of the Article 10-Act provides that legal action against orders pursuant to Section 3 (individual measures) and Section 5 (strategic telecommunications intelligence) and their enforcement is not permitted prior to the notification of the person concerned. This means that an interested party may challenge the legality of an order and its implementation before a court only after being informed about the measure. In cases of strategic telecommunications intelligence (Section 5 and 8 of the Article 10-Act), notification takes place only if the personal data was not deleted immediately.[309] In 2013, approximately twelve judicial claims against individual measures (Section 3) were pending, while one legal action against strategic surveillance measures pursuant to Section 5 of the Article 10-Act was filed before the highest administrative court, the Federal Administrative Court.[310] No legal action has been reported in connection with Section 8 measures (*i.e.*, surveillance implemented where necessary to detect or avert an existing danger to life or limb of a person abroad, by which the interests of Germany are directly affected).[311]

With respect to non-judicial remedies, interested parties also can bring a complaint before the G-10 Commission if they suspect interferences by an intelligence service[312] with the right of privacy of correspondence, posts, and telecommunications. In 2013, the G-10 Commission received 21 such complaints linked to targeted surveillance, but found no violation. No complaints against strategic surveillance were reported.

In *Ireland*, as mentioned above, a Complaints Referee consisting of a lower Circuit Court judge is empowered to investigate complaints by members of the public who believe their communications have been intercepted. The Complaints Referee has power to investigate, quash any invalid interception, report the matter to the Prime minister, and recommend compensation. A Designated Judge of the High Court also exercises a more general oversight function.

In *Italy*, the Code of Criminal Procedure governs surveillance as a means to gather evidence in criminal investigations which is subject to oversight of the judge presiding over the investigation. A person under investigation has a right of access to the data collected and can petition the judge to see that the data is deleted on data protection grounds once no longer necessary in the context of the

[309] Article 10-Act, 13 August 1968, § 12 (2).

[310] *See* G 10-Commission Report 2013, at 8. In the meantime, the Federal Administrative Court issued a judgment in this case, rejecting the applicant's request to determine the illegality of the measure in question. See Decision of the Federal Administrative Court of 28 May 2014, BVerwG 6 CN 1.13. The court concluded that the applicant did not provide sufficient proof that he was affected by the strategic telecommunications intelligence measure, specifically, that the telecommunications connection of the applicant was detected in the course of the measure.

[311] Article 10-Act, 13 August 1968, § 8(1).

[312] *Id.* § 15(5)(1).

investigation.[313] A similar right exists where data is held by police and individuals also can seek damages for data that was processed illegally.[314]

The Garante may review how the intelligence services collect data and, where the collection is not in compliance with Italian data protection laws, may issue only non-binding recommendations to the intelligence services.[315] The scope and rules of the Garante's review of the intelligence service's files are regulated by a (non-public) memorandum of understanding signed in 2013 by the Garante and the intelligence services.[316]

In *the Netherlands*, under the Administrative Law Act individuals can bring proceedings against decisions that affect them directly. Individuals bring proceedings in the administrative authority with jurisdiction in their place of residence. Individuals also have the right to complain to the ombudsman about activities of ministers and persons employed by the intelligence services.[317] In addition, the CTIVD acts as an independent complaints advisory committee with complaints made first to the relevant minister who decides whether or not to send the complaint to the CTIVD which then investigates and provides an advisory opinion to both the relevant minister and the complainant.[318] Neither the ombudsman nor the CTIVD have remedial powers.

In *Poland*, individuals can bring a complaint to the Human Rights Defender, the constitutional authority for legal control and protection of individuals' rights and freedoms – irrespective of whether or not the individual is a citizen. The Human Rights Defender is an ombudsman, independent from other governmental authorities. In order to fulfil its tasks effectively, the Human Rights Defender is vested with investigative powers and the power to initiate civil and administrative proceedings. However, it does not have the power to impose sanctions.

In *the UK*, the IPT was established to deal with complaints from individuals against surveillance and consists of specialist lawyers; it is not a court and is strictly limited to assessing whether legislation has been complied with and authorities have acted reasonably.[319] There is no right of appeal against decisions of the IPT[320] and "the

---

[313] Code of Criminal Procedure, Articles 268, 269 & 271.

[314] Legislative Decree n. 196 of 30 June 2003 (Data Protection Code). Articles 15, 53, 141 & 145.

[315] *Id.*, Article 60.

[316] Presidency of the Council of Ministers, Press Release, 11 November 2013.

[317] Intelligence and Security Services Act 2002, 7 February 2002, Article 83(1).

[318] CTIVD (2015), at 19.

[319] The UK Independent Reviewer of Terrorism Legislation recommended that the IPT should have its jurisdiction expanded and given power to make declarations of incompatibility and that its rulings should be subject to appeal on points of law. Anderson, *A Question of Trust – Report of the Investigatory Powers Review*, *supra* note 282, at 305.

[320] RIPA §§ 65–68.

reasons for or explanation of the decision are not normally given."[321] Issues of national security are explicitly outside the mandate of the UK Parliamentary Commissioner for Administration[322] and oversight bodies in the UK have no remedial powers. Individuals can also appeal to the First-tier Tribunal (Information Rights) against a decision issued by the Information Commissioner's Office in respect of a freedom of information request.

2.2 US Surveillance Laws Embody A System Of Checks And Balances

2.2.1 Overview And Background

Government's power to conduct surveillance springs from two essential aspects of sovereignty: the duty to ensure domestic peace[323] and the right of self-defence.[324] Two separate arms of the government in the United States carry out these functions: (1) law enforcement, which includes the Federal Bureau of Investigation (FBI), as well as state and local police; and (2) intelligence services, which include the Central Intelligence Agency (CIA), the National Security Agency (NSA), components of the FBI, and a number of other agencies, many of which are not directly relevant to electronic communications.[325] These are referred to collectively in the US as the Intelligence Community.[326]

The government's surveillance powers, as in other democratic countries, are limited and controlled. A system of substantive and structural checks and balances limits the intrusion of government surveillance and subjects such surveillance to oversight for approval and review. These safeguards originate in protections for American citizens and people in the US in the federal constitution, particularly the First and Fourth Amendments,[327] and go on to include federal statutes – most notably, when it

---

[321] Anderson, *A Question of Trust – Report of the Investigatory Powers Review*, *supra* note 282, at 122.

[322] Parliamentary Commissioner Act 1967, 22 March 1967, § 5.

[323] *See, e.g.*, *Calvin's Case*, 77 Eng. Rep. 377, 382, 386 (1608); *United States v. United States Dist. Court*, 407 U.S. 297, 312 (1972) (*Keith*) ("[T]he most basic function of any government is to provide for the security of the individual and his [or her] property.").

Keith stands as a landmark decision in American surveillance law. The government in that criminal case sought to withhold records and logs relating to electronic surveillance on national-security grounds. The district court judge (by whose name the case is known) nonetheless ordered the records released. The Supreme Court affirmed, holding that domestic national-security investigations must comply with the Fourth Amendment. *Keith*, 407 U.S. at 320; *see generally* Trevor W. Morrison, *The Story of* United States v. United States District Court (Keith)*: The Surveillance Power*, in PRESIDENTIAL POWER STORIES 287–326 (Christopher H. Schroeder & Curtis A. Bradley, eds. 2009).

[324] *See, e.g.*, United Nations Charter, art. 51 (1945); *Nicaragua v. United States*, 1986 I.C.J. 14, paras. 35, 50 (recognising sovereign nations' right to self defence).

[325] The Office of the Director of National Intelligence (ODNI) oversees the Intelligence Community.

[326] 50 U.S.C. § 3003(4).

[327] The relevant provisions of the federal constitution bind *all* government actors in the United States, including state law-enforcement officials. *See* U.S. Const. art. VI, § 2, cl. 2 ("This Constitution, and the laws of the United States which shall be made in pursuance thereof … shall be the supreme law of

comes to electronic data, the Electronic Communications Privacy Act[328] and the Foreign Intelligence Surveillance Act of 1978[329] – and executive orders that bind the federal government.[330]

The First Amendment guarantees freedoms of speech, of the press, of association, and of religion.[331] It stems from the American founders' concerns with the use of official powers for religious and political persecution in Europe and in the colonies, and thus prevents gathering evidence and conducting prosecutions based solely on the exercise of those protected freedoms.[332]

The Fourth Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[333] This constitutional provision ensures "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[334] Today, it

---

the land."); *Ker v. California*, 374 U.S. 23, 32–33 (1963) (making reasonableness requirement of Fourth Amendment applicable to the states); *Mapp v. Ohio*, 367 U.S. 643, 657 (1961) (exclusionary rule); *Nat'l Ass'n for the Advancement of Colored People v. Alabama*, 357 U.S. 449, 460 (1958) (freedom of assembly); *Gitlow v. New York*, 268 U.S. 652, 666–67 (1925) (freedom of speech).

Each state, however, has its own constitution, which may provide additional limits to government power and protections for persons within its borders. *See, e.g.*, *Commonwealth v. Upton*, 476 N.E.2d 548, 554 (Mass. 1985) (requiring additional indicia of reliability to obtain a warrant than federal law requires); William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 498–502 (1977) (collecting cases).

[328] Pub. L. No. 99–508, 100 Stat. 1848 (1986). ECPA includes the Wiretap Act, 18 U.S.C. §§ 2510–2522, and the Stored Communications Act, 18 U.S.C. §§ 2701–2712.

[329] Pub. L. No. 95–511, 92 Stat. 1783 (1978) (codified, as amended, at 50 U.S.C. §§ 1801–1885c).

[330] *See, e.g.*, Exec. Order No. 12,333, 3 C.F.R. 200 (1981); Presidential Policy Directive/PPD-28 (2014) (PPD-28), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[331] U.S. Const. amend. I; *see also Keith*, 407 U.S. at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. *For private dissent, no less than open public discourse, is essential to our free society*." (emphasis added)).

[332] *See, e.g.*, *Quantity of Copies of Books v. Kansas*, 378 U.S. 205, 210–11 (1964); *Nat'l Ass'n for the Advancement of Colored People v. Button*, 371 U.S. 415, 433 (1963); *Smith v. People of Cal.*, 361 U.S. 147, 151 (1959).

[333] *Riley v. California*, 134 S. Ct. 2473, 2494 (2014).

[334] U.S. Const. amend. IV. These constitutional protections apply to United States citizens and those in the United States who have "developed sufficient connection with [the United States] to be considered part of [the national] community." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990). This includes foreign persons lawfully in the United States, particularly when government surveillance is conducted inside the United States. *See id.* at 271.

establishes generally that "a person has a constitutionally protected reasonable expectation of privacy."[335] The government therefore cannot, as a matter of course, trespass upon a protected privacy interest without "[p]rior review by a neutral and detached magistrate" and the issuance of a warrant.[336] Even in exceptional cases, these safeguards require that the conduct of surveillance – and all searches and seizures – are ajudged reasonable when they interfere with constitutionally protected privacy rights.[337]

Establishing that surveillance is "reasonable" – and, thus, permissible under the US legal order – depends on standards analogous to the principles of necessity and proportionality, though these same words are not expressly required in US jurisprudence; nonetheless, the application of US law is consistent with these principles in effect.

As a matter of constitutional law, in order to establish that surveillance is *necessary*, the government – with few exceptions[338] – must present a sufficient factual predicate to a neutral magistrate that shows that a person or group has probably committed, is committing, or will commit a crime (or, in the foreign-intelligence context, that the person fits within specifically-defined foreign intelligence purposes) to engage in most electronic surveillance.[339] Any form of surveillance in practical terms "is ordinarily [considered] unreasonable in the absence of individualized suspicion of wrongdoing."[340] No warrant can issue short of such demonstration, and thus, no surveillance may proceed for the purpose of gathering information for the use of law enforcement.[341]

Surveillance is *proportionate* under the US legal order when "the duty of Government to protect the domestic security" outweighs "the potential danger posed by

---

[335] *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *see also Bond v. United States*, 529 U.S. 334, 340–41 (2000) (adopting Justice Harlan's test).

[336] *Keith*, 407 U.S. at 318; *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 654 (1995) ("A search unsupported by probable cause can be constitutional, we have said, 'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'").

[337] *See also Berger v. New York*, 388 U.S. 41, 59–60 (1967) (holding that the interception of communications qualifies as a seizure); *see also supra* note 334 (describing reach of Fourth Amendment); *infra* text following note 345.

[338] *See, e.g., Kentucky v. King*, 536 U.S. 452, 460 (2011) ("One well-recognized exception applies when 'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment."); *id*. (noting that the need to provide "emergency aid," to pursue a fleeing suspect, and "to prevent the imminent destruction of evidence" satisfies this standard). The government "bear[s] a heavy burden when attempting to demonstrate an urgent need that might justify warrantless searches." *Welsh v. Wisconsin*, 466 U.S. 740, 749 (1984).

[339] U.S. Const. amend. IV; *Illinois v. Gates*, 462 U.S. 213, 237 (1983).

[340] *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000).

[341] *See, e.g.*, *Mapp*, 367 U.S. at 657 (establishing the exclusionary rule, which prevents prosecutors from introducing evidence collected in violation of the Fourth Amendment).

unreasonable surveillance to individual privacy and free expression."[342] The greater the protected privacy interest at stake, the stronger the government showing of necessity must be for it to be considered reasonable.[343] Moreover, surveillance that is so intrusive that it '"shocks the conscience" and violates the "decencies of civilized conduct'" can never be justified and is thus *per se* illegal.[344] No general necessity or national-security exemption exists to permit otherwise-unconstitutional surveillance programs, meaning that communications can be collected only within the constitutional structure, and private parties may not voluntarily conduct searches on the government's behalf to surmount these restrictions.[345]

These constitutional protections, by and large, apply to "US persons," a term that encompasses foreign citizens lawfully in the US, and also to their data transmitted to and stored on servers in the US. Beyond these constitutional requirements, statutes and executive orders impose additional restraints on the powers of law enforcement and the Intelligence Community to conduct surveillance, and many of these provisions apply comparably to US persons and to non-US persons (*i.e.*, citizens of other countries when they are located outside the US).

Development Of Electronic Surveillance Laws – Law Enforcement

Surveillance is a valuable and legitimate tool for crime prevention and prosecution, and it is therefore employed by American law enforcement. Both constitutional protections and physical limitations have constrained these activities sufficiently through much of American history. In the mid-twentieth century, when technological advances enabled surveillance on a more surreptitious and widespread basis,[346] the courts applied the Fourth Amendment to electronic surveillance,[347] and Congress enacted legislation to provide additional safeguards and oversight.

Congress passed the *Wiretap Act* as part of the Omnibus Crime Control and Safe Streets Act of 1968.[348] This act generally prohibits the interception of oral, wire, or electronic communications affecting interstate commerce and the use or disclosure

---

[342] *Keith*, 407 U.S. at 314–15.

[343] *See, e.g.*, *Terry v. Ohio*, 392 U.S. 1, 26–27 (1968) (weighing reasonableness of proposed search and seizure in light of privacy interests).

[344] *Cnty. of Sacramento v. Lewis*, 523 U.S. 833, 846 (1998) (quoting *Rochin v. California*, 342 U.S. 165, 172–723 (1952)).

[345] *Skinner v. Railway Labor Execs. Ass'n*, 489 U.S. 602, 614 (1989) (Fourth Amendment protects against private party intrusions "if the private party acted as an instrument or agent of the Government").

[346] *Cf. United States v. Jones*, 132 S. Ct. 945, 958 (2012) (noting that "a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner" would be the common-law equivalent of a GPS tracker); *see also* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1318–20 (2004) (noting abuses of wiretaps by Presidents Franklin Roosevelt through Richard Nixon).

[347] *See, e.g.*, *Keith*, 407 U.S. at 318; *Berger*, 388 U.S. at 59–60; *Katz*, 389 U.S. at 354.

[348] Pub. L. No. 90–351, 82 Stat. 197 (codified, as amended, at 18 U.S.C. §§ 2510–2522).

of such communications.[349] It nonetheless permits law-enforcement officials – federal, state, and local – to conduct these activities under certain limited conditions. Specifically, these officials must obtain a "Title III warrant" from a neutral magistrate to intercept or interfere in any way with a real-time communication when any one party is located in the United States.[350] To secure such a warrant, the government must submit an affidavit to a neutral magistrate that demonstrates (1) law enforcement has probable cause to believe that the intercepted communications will reveal evidence related to one of a few enumerated felonies (discussed below), (2) that other means of acquiring the communications have been exhausted, and (3) that the surveillance will be conducted in as limited a manner as possible.[351] Moreover, as a means of ensuring independent oversight, the act requires law enforcement and the courts to submit yearly public reports on the number of wiretaps nationwide and their usefulness,[352] and it has empowered committees in Congress and independent watchdogs within the executive branch to monitor the government's use of wiretaps between reports.[353]

In 1986, as electronic communications began to rise with the advent of personal computing, Congress enacted the *Electronic Communications Privacy Act* (ECPA).[354] This statute, particularly the *Stored Communications Act*, prescribes additional protections for the content[355] of such communications[356] and for other non-

[349] 18 U.S.C. §§ 2510(1), (2) & (12); 2511(1).

[350] *Id.* §§ 2516, 2518.

[351] *See* 18 U.S.C. §§ 2516–18; US Dep't of Justice, *Wiretap Report 2014*, http://www.uscourts.gov/statistics-reports/wiretap-report-2014.

[352] *See, e.g.*, US Dep't of Justice, *Wiretap Report 2014*, *supra* note 351.

[353] *See, e.g.*, 28 U.S.C. § 509 (note) (establishing the Department of Justice Privacy and Civil Liberties Office); 42 U.S.C. § 2000ee (creating and empowering the Privacy and Civil Liberties Oversight Board); *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (July 8, 2015); *Oversight of the U.S. Department of Justice: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (Jan. 29, 2014); *Video Laptop Surveillance: Does Title III Need to Be Updated: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (Mar. 29, 2010).

[354] Pub. L. No. 99–508 (1986). This statute, in part, provides statutory protections for privacy rights not protected by the Fourth Amendment. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (holding that a person does not have a reasonable expectation of privacy in data voluntarily shared with a third party). In ECPA, Congress also amended the Wiretap Act to apply explicitly to electronic communications.

[355] American law distinguishes between content and non-content communications; however, the definition of "content" is flexible and can change depending on the law at issue. For instance, in the law-enforcement context, "'contents' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The text and, potentially, the subject line of an email would be considered content, but the timestamp and the "to" and "from" lines may not be treated as content under this statute. In contrast, the Foreign Intelligence Surveillance Act of 1978 (FISA), which governs the Intelligence Community, defines "conten[t]" to "include[] any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n). Thus, the "to" and "from" fields of an email message, denoting sender and receiver, would qualify as content under FISA.

content personal data in which people are not considered to have a reasonable expectation of privacy for purposes of the Fourth Amendment, such as the "to" or "from" fields or the timestamp on an email.[357] The government must demonstrate "probable cause" to a neutral magistrate to access the contents of stored electronic communications, including email messages,[358] and it *must* otherwise initiate legal process – through a court order or subpoena – to compel disclosure of non-content personal data from telecommunications companies.[359]

In addition to the judicial approval and review outlined above, US law enforcement's surveillance activities are subject to various administrative controls as well as oversight from congressional committees and independent oversight boards. These are discussed in greater detail in Part 2.2.4 below.

Development Of Electronic Surveillance Laws – Intelligence

The United States, like many countries, conducts surveillance for foreign-intelligence purposes, exercising its "inherent right" as a sovereign country to "tak[e] measures necessary" to defend itself.[360] The Constitution places the authority to gather intelligence largely in the hands of the President as Chief Executive given the President's primacy in the conduct of foreign affairs and status as Commander in Chief of the armed forces.[361] This differs from law-enforcement powers, which are split between the federal government and the states.

---

[356] *See 1*8 U.S.C. § 2703(a); *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (determining that a warrant is necessary to search contents of emails under the Fourth Amendment). The text of ECPA purports to authorise government access to the contents of communications stored longer than 180 days without obtaining a warrant. *See* 18 U.S.C. §2703(d). In *Warshak*, a federal court of appeals concluded that such authorisation cannot be squared with the Fourth Amendment and that the government must obtain a search warrant. 631 F.3d at 288. The federal government has acceded to this ruling and now seeks a warrant before obtaining stored contents of communications. Members of Congress have introduced legislation that would codify the government's position. *See, e.g.*, Electronic Communications Privacy Act Amendments Act of 2015, S. 356, 114th Cong. (2015); H.R. 283, 114th Cong. (2015).

[357] *See* 18 U.S.C. §§ 2702(a), 2703(d); Fed. R. Crim. P. 17(c)(2). ECPA also includes the Pen Register Act, 18 U.S.C. §§ 3121 *et seq.* This provision governs the *targeted* collection of dialing, routing, addressing, or signaling information (*e.g.*, telephone numbers) of calls to and from a *particular* number. *Id.* § 3127(3). It does not permit, under any circumstances, the collection of "contents of any communication." *Id.* § 3127(3) & (4).

[358] 18 U.S.C. § 2703(a).

[359] *Id.* § 2702(a) ("Except [with legal process] – a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.").

[360] United Nations Charter, art. 51 (1945).

[361] U.S. Const. art. II, § 2, cl. 1 ("The President shall be Commander in Chief of the Army and Navy of the United States …."); *Totten v. United States*, 92 U.S. 105, 106 (1875) ("[The President] was undoubtedly authorized during the war, as commander-in-chief of the armies of the United States, to employ secret agents to enter the revel lines and obtain information respecting the strength, resources, and movements of the enemy."); *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) (noting that the President "is bound to resist force by force" in protecting the United States).

The executive branch exercised this authority largely without oversight until the 1970s.[362] After it emerged that presidents, the FBI, and the CIA ordered surveillance on political adversaries, civil-rights leaders, and anti-war activists – domestically and abroad[363] – Congress enacted the *Foreign Intelligence Surveillance Act of 1978*.[364] FISA criminalizes intentionally engaging in "electronic surveillance" except as prescribed under FISA.[365] The statute defines this term, in relevant part, as "the acquisition by an electronic, mechanical, or other surveillance device of":

> "[1] the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States,
>
> [2] the contents of any wire communication to or from a person in the United States ... if such acquisition occurs in the United States ...."[366]

This definition covers the interception of data on US territory that has been transmitted from Europe to the US.

As with the Wiretap Act and ECPA, Congress created exceptions to the general prohibition and permits the Intelligence Community to engage in specified electronic surveillance. It may collect, retain, and disseminate intercepted communications and data in accordance with the orders of a special court tasked with overseeing the Intelligence Community's compliance with applicable law – the Foreign Intelligence Surveillance Court (FISC).[367] The judges on this court are federal judges who have been previously nominated by the President and confirmed by the Senate and, therefore, have lifetime judicial tenure[368]; the Chief Justice of the United States appoints them to the FISC for a specific term of up to seven years.[369] They have authority to reject individual surveillance applications as well as broader authority to strike down government surveillance programs that violate constitutional and

---

[362] Robert S. Litt, Gen. Counsel, ODNI, *Privacy, Technology & National Security: An Overview of Intelligence Collection* (July 18, 2013) ("Prior to the passage of FISA in 1978, the collection of foreign intelligence was essentially unregulated by statutory law. It was viewed as a core function of the Executive Branch."), http://icontherecord.tumblr.com/post/57724442606/privacy-technology-national-security-an.

[363] *See* Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 346, at 1318–20 (recounting abuses discovered by Church Committee).

[364] Pub. L. No. 95–511, 92 Stat. 1783 (codified, as amended, at 50 U.S.C. §§ 1801–1885c).

[365] 50 U.S.C. § 1809(a); *see also* 18 U.S.C. § 2511(2)(e).

[366] *Id.* § 1801(f)(1)–(2). "'Wire communication' means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." *Id.* § 1801(l).

[367] 50 U.S.C. § 1803(a).

[368] U.S. Const. art. III, § 1.

[369] 50 U.S.C. § 1803.

statutory law.[370] Recently, this court has appointed several respected attorneys as *amici curiae*, with the necessary security clearance, to brief the court on any civil liberties concerns that may arise with the government's applications for surveillance approval.[371]

FISA places significant limits in the government's ability to conduct electronic surveillance. These provisions are known as "FISA Title I."[372] They require the Attorney General – the country's top law-enforcement official – to make an application to the FISC for a FISA warrant to intercept real-time communications.[373] The application must demonstrates, with particularity, facts showing that probable cause exists to believe that "the target of the [proposed] surveillance is a foreign power or an agent of a foreign power,"[374] and the government must assert that it seeks to conduct this surveillance for the purpose of obtaining "foreign intelligence."[375] To intercept real-time communications for intelligence-gathering purposes, the Attorney General – the country's top law-enforcement official – must make an application to the FISC that demonstrates, with particularity, facts showing that probable cause exists to believe that "the target of the surveillance is a foreign power or an agent of a foreign power,"[376] and the government must assert that it seeks to conduct this surveillance for the purpose of obtaining "foreign intelligence."[377]

---

[370] *See, e.g.*, Memorandum Opinion, [*Caption Redacted*], No. [Redacted], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011), http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf (finding portions of the government's Section 702 programme unconstitutional and in violation of statute); Charlie Savage, *Power Wars* 572 (2015) (describing Judge Bates's memorandum opinion).

[371] Pub. L. No. 114–23, § 401, 129 Stat. 279 (codified at 50 U.S.C. § 1803(i)(4)); FISC, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae; Cody Poplin, *Amicus Curiae for FISC Announced*, Lawfare (Dec. 1, 2015), https://www.lawfareblog.com/amici-curiae-fisc-announced.

[372] *See* 50 U.S.C. §§ 1801–1813.

[373] *Id.* § 1804(a).

[374] 50 U.S.C. §§ 1804(a), (d); 1805(a)(2); *see also* David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions* § 6.2 (2d ed. 2012) (noting additional requirements and that, unlike Title III Warrants, the government must identify the target of the surveillance in a FISA application).

[375] FISA defines "foreign intelligence information" as "information that relates to … the ability of the United States to protect against actual or potential attack … of a foreign power …; sabotage, international terrorism, or the international proliferation of weapons of mass destruction …; or clandestine intelligence activities" or "information with respect to a foreign power or foreign territory that relates to … the national defense or security of the United States; or the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e).

[376] 50 U.S.C. §§ 1804(a), (d); 1805(a)(2); *see also* David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions* § 6.2 (2d ed. 2012) (noting additional requirements and that, unlike Title III Warrants, the government must identify the target of the surveillance).

[377] FISA defines "foreign intelligence information" as "information that relates to … the ability of the United States to protect against actual or potential attack … of a foreign power …; sabotage, international terrorism, or the international proliferation of weapons of mass destruction …; or clandestine intelligence activities" or "information with respect to a foreign power or foreign territory

These protections, by and large, ensure that the most invasive surveillance – interception of real-time wire communications[378] – is specially targeted and constrained and that oversight is provided.

As in the law-enforcement context, however, the evolution of technology has given the government additional tools for which safeguards have not always kept pace. President Bush, for instance, ordered the Intelligence Community to use all options available to prevent another terrorist attack following September 11, 2001.[379] The Intelligence Community thus began (or accelerated previous efforts at) collecting and analyzing data in bulk and monitoring communications between individuals in the United States and people abroad.[380] Part of these efforts was the President's Terrorist Surveillance Program[381] under which the NSA eavesdropped on conversations in and passing through the United States without a warrant.[382] The NSA also operated a programme of bulk-collection of telephone metadata[383] – information such as the "originating and terminating telephone number" or "the time [and] duration of the call."[384]

---

that relates to … the national defense or security of the United States; or the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e).

[378] *See supra* note 366.

[379] *See* President George W. Bush, Address to the Nation (Sept. 20, 2001) ("We will direct every resource at our command—every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war—to the destruction and to the defeat of the global terror network.").

[380] *See, e.g.*, Savage, *Power Wars*, *supra* note 370, at 180–82; Privacy & Civil Liberties Oversight Board (PCLOB), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Section 702 Report) 16–17 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

[381] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (describing Terrorist Surveillance Program as based on the President's Commander-in-Chief powers and the Authorization for Use of Military Force).

[382] *Id.*; *See also Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143–44 (2013) ("In the wake of the September 11th attacks, President George W. Bush authorized the National Security Agency (NSA) to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States and a participant in 'the call was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization.'" (citation omitted)); Inspectors General's Unclassified Report on the President's Surveillance Program 1 (July 10, 2009), https://oig.justice.gov/special/s0907.pdf ("One of the activities authorized as part of the [President's Terrorist Surveillance Program] was the interception of the content of communications into and out of the United States where there was a reasonable basis to conclude that one party to the communication was a member of al-Qa'ida or related terrorist organizations.").

[383] *See* Savage, *Power Wars*, *supra* note 370, at 192–93.

[384] NSA Civil Liberties & Privacy Office, *Transparency Report: The USA FREEDOM Act Business Records FISA Implementation* 4 (Jan. 15, 2016). Contrary to some media reports, *see, e.g.*, Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, WASH. POST (June 15, 2013), https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html, the service providers did not generally provide the NSA with

Congress passed the *USA PATRIOT Act* in 2001,[385] updating various surveillance tools and making national-security investigations more efficient and effective.[386] The Bush Administration took an extensive view of these authorities,[387] but in 2005, authorisation for some of the tools, including emergency disclosure provisions, automatically expired.[388] Congress later imposed additional limitations once the full implications of these surveillance programs became known. The President and the Intelligence Community have since instituted further safeguards.

For purposes of data transfers from Europe to the US, two sets of safeguards and limitations – both within FISA – are relevant.

First, there is *Section 702* of the FISA Amendments Act of 2008, which governs the collection of the contents of stored communications in the US, *i.e.*, data transmitted to US servers belonging to foreign persons outside the US – and hence the personal data of EU data subjects that is transferred by data controllers for processing and storage in the US.[389] This type of surveillance was previously overseen only by the Intelligence Community itself, but has more recently been placed within FISA and requires approval of the FISC.[390]

Both the Attorney General and the Director of National Intelligence (DNI) – two cabinet-level officials – must now certify under oath to the FISC that "a significant purpose of the acquisition [of the content of communications] is to obtain foreign intelligence,"[391] that the acquisition will be done in accordance with court-approved

---

cellular location data – at the NSA's request. *See* Marcy Wheeler, *AT&T Pull Cell Location for Its "Mobility Cell Data*," EMPTYWHEEL (Aug. 15, 2015), https://www.emptywheel.net/2015/08/15/2015/08/15/att-pulled-cell-location-for-its-mobility-cell-data/.

[385] Pub. L. No. 107–56, § 215 (2001), 115 Stat. 272.

[386] *See* US Dep't of State, *Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States* 7–8 (Oct. 29, 2012), http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf.

[387] *See, e.g.*, Mem. from Jack L. Goldsmith, III, Ass't Att'y Gen., Off. of Legal Counsel, re: Review of the Legality of the STELLAR WIND Program (May 6, 2004), http://apps.washingtonpost.com/g/documents/national/a-memo-for-the-attorney-general-may-2004/1226/ (justifying use of the President's Terrorist Surveillance Program); US Dep't of Justice, *Legal Authorities Supporting the Activities of the Nat'l Sec. Agency Described by the President* (Jan. 19, 2006), https://epic.org/privacy/terrorism/fisa/doj11906wp.pdf.

[388] US Dep't of Justice, *USA PATRIOT Act: Sunsets Report* (Apr. 2005), https://epic.org/privacy/terrorism/usapatriot/Sunsets_Report_Final.pdf; Charles Doyle, *USA Patriot Act Sunset: Provisions That Expire on December 31, 2005*, Cong. Research Serv. (Jan. 2, 2004), https://epic.org/privacy/terrorism/usapatriot/RL32186.pdf.

[389] FISA Amendments Act of 2008, Pub. L. No. 110–261, § 702, 122 Stat. 2438 (codified at 50 U.S.C. § 1881a).

[390] The Protect America Act of 2007, Pub. L. No. 110–55, 121 Stat. 552, initially brought this type of surveillance under the FISC's umbrella. Shortly thereafter, Congress enacted the FISA Amendments Act to place the authorisation on a more permanent footing.

[391] 50 U.S.C. § 1881a(g).

targeting procedures,[392] and that court-approved minimization procedures will be followed to ensure that data is accessed, retained, and disseminated in a proper manner.[393] The FISC must conclude that the government's certifications are sufficient and that the targeting and minimization procedures meet statutory requirements.[394] Only then may the Attorney General and the DNI order telecommunications carriers and other communications providers to disclose stored communications.[395]

The Intelligence Community operates two programs pursuant to its Section 702 authorities: PRISM and Upstream. Under PRISM, the government "tasks" or sends "selectors" – email addresses or telephone numbers, never keywords or names – to an electronic communications service provider, such as a telephone company or email provider.[396] The service provider must then provide the government with all communications sent to or from that selector.[397] These specific requests do not involve the collection of "all personal data of all persons whose data is transferred to United States," as referred to in the *Schrems* judgment.[398]

The other programme that Section 702 authorizes is Upstream. Under this programme, the NSA collects emails and other electronic communications from "the providers that control the telecommunications 'backbone' over which communications transit[.]"[399] As with PRISM, the NSA sends selectors to the providers; the providers then capture all of the communications and transactions related to those selectors going forward.[400] For telephone communications (*e.g.*, text messages), the providers send the NSA communications "to" and "from" the selector.[401] For Internet transactions (*e.g.*, emails), they send communications "to," "from," and "about" the selector, meaning that emails including the selected email

---

[392] *Id.* § 1881a(d), (g).

[393] *Id.* §§ 1801(h), 1881a(e), (g).

[394] *Id.* § 1881a(i).

[395] 50 U.S.C. § 1881a(a), (h). These orders are called "directives."

[396] PCLOB, Section 702 Report, *supra* note 380, at 33–34.

[397] *Id.*

[398] *See* Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, 14–15 (Dec. 17, 2015), https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf; FRA Report, *supra* note 127, at 17 (recognising PRISM is "a targeted technology used to access court ordered foreign internet accounts"); Geoffrey Robertson QC, *Final Opinion*, para. 30 (14 January 2016) ("One factual error made by the Court in *Schrems* – seemingly as a result of the 'facts' found by the Irish court – was to describe the PRISM programme as a bulk or 'generalised' data collection. This is not the case, and confuses PRISM with the bulk collection of metadata ....").

[399] PCLOB, Section 702 Report, *supra* note 380, at 35; *see also* Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 17.

[400] PCLOB, Section 702 Report, *supra* note 380, at 35.

[401] *Id.* at 36.

address in the subject line or body of the email will also be collected.[402] NSA analysts may then query these filtered communications, using only foreign-intelligence related keywords, for relevant information.[403] Upstream differs from PRISM mainly in the time period covered, as it seeks communications in real-time instead of stored communications; of the communications acquired under Section 702, Upstream provides only ten percent.[404]Second, Congress has constrained the telephone metadata programme with the USA FREEDOM Act.[405] That programme, originally covered by *Section 215* of the USA PATRIOT Act, permitted the government to collect telephone metadata in bulk from US carriers. Now, the FBI – through the Department of Justice – must apply to the FISC for an order permitting the government to analyze the metadata connected to identified telephone numbers, which is stored by a telecommunications provider (as opposed to the data being collected in bulk and stored by the government).[406] This application must include a "specific selection term" that "identifies a person, account, address, or personal device, or any other specific identifier"[407] and contain "a statement of facts showing that: (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term … are relevant to [an ongoing national-security] investigation; and (ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism …."[408] If the court approves the specific selection term and grants the order, the telecommunications provider must produce the records linked to the specific selection term as well as records directly linked to those produced

[402] *Id.* at 36–37.

[403] Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 18–19; PCLOB, Section 702 Report, *supra* note 380, at 55.

The queries are monitored to ensure that they a not overbroad or related to improper purposes, "such as an analyst's query to find information about a girlfriend[.]" PCLOB, Section 702 Report, *supra* note 380, at 56; *see also* Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power On Love Interests*, WASH. POST (Aug. 24, 2013), https://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests.

[404] Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 17.

[405] *See, e.g.*, Pub. L. No. 114–23, § 109, 129 Stat. 268 (2015) (amending 50 U.S.C. § 1861).

[406] 50 U.S.C. § 1861(a). FISA previously required the government to obtain an order from the FISC requiring the carriers to turn over all metadata directly to the government for storage and analysis. Under the USA FREEDOM Act, the carriers now store the data (without a retention requirement separate from the US consumer-protecting communications regulations, *see* 47 C.F.R. § 42.6), and the Intelligence Community requests certain data to analyze. The government thus collects only targeted data; indeed, the USA FREEDOM Act explicitly forbids bulk collection under FISA.

[407] Pub. L. No. 114–23, § 107 (amending 50 U.S.C. § 1861(k)). This provision mirrors the requirement under Section 702 that the government provide a "selector." It has been reported that "only about three hundred new numbers" are added per year under this programme. *See* Savage, *Power Wars*, *supra* note 370, at 607. The FISC approves these new numbers. *Id.*

[408] Pub. L. No. 114–23 § 101 (amending 50 U.S.C. § 1861(b)(2)).

records.[409] These changes make bulk collection of metadata under FISA impermissible.

These programmes, as of July 2013, had led to 54 "success stories" for US national security and that of other countries – most of them within the EU.[410] Specifically, Senator Feinstein – who chaired the Senate Intelligence Committee – reported that these programmes have disprupted 13 events in the United States, 25 in Europe, five in Africa, and 11 in Asia.[411]

All communications and data collected under FISA (FISA Title I, Section 702, and Section 215) are subject to minimization procedures.[412] These procedures govern and limit the intelligence agencies' storage and dissemination of collected data.[413]

This trio of FISA provisions and their corresponding protections control the government's access to data in the US that has been transmitted from Europe to American persons, businesses, and servers. They generally do not govern the intelligence community's surveillance activities abroad or its collection of data not being sent to the United States. The executive branch undertakes these non-FISA, or "signals intelligence," activities pursuant to the President's inherent constitutional authority.[414] Nonetheless, the executive branch has issued two consequential, binding, and directly relevant orders – Executive Order 12,333 and Presidential Policy Directive/PPD-28 (PPD-28) – to prevent abuses that may stem from these national security powers and to protect the privacy rights of all.

Executive Order 12,333, originally issued by President Reagan and added to by subsequent presidents,[415] permits the Intelligence Community to collect information

---

[409] *Id.* § 101 (amending 50 U.S.C. § 1861(c)(2)); NSA Civil Liberties & Privacy Office, *USA FREEDOM Transparency Report*, *supra* note 384, at 5.

[410] PCLOB, Section 702 Report, *supra* note 380, at 109–10

[411] *Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs: Hearing of the S. Judiciary Comm.*, 113th Cong. (July 31, 2013) (statement of Sen. Feinstein).

[412] 50 U.S.C. §§ 1805(a)(3); 1861(c); 1881a(c).

[413] *See, e.g.*, NSA, *Minimization Procedures Used by the National Security Agency in connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702* (Feb. 2, 2015), http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; FBI, *Presidential Policy Directive 28 Policies and Procedures* (Feb. 2, 2015), https://www.fbi.gov/about-us/nsb/fbis-policies-and-procedures-presidential-policy-directive-28-1; CIA, *Signals Intelligence Activities Guidelines* (Feb. 2, 2015), http://www.dni.gov/files/documents/ppd-28/CIA.pdf; Off. of the Dir. of Nat'l Intelligence, *Minimization Procedures* (July 24, 2014), http://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[414] U.S. Const. art. II, § 2, cl. 1 ("The President shall be commander in chief of the Army and Navy of the United States, and of the militia of the several states, when called into the actual service of the United States."); *see supra* note 361. Due to the statutory restraints in FISA and the Wiretap Act, these activities cannot include "electronic surveillance" or an "intercept." 18 U.S.C. § 2511(2)(e).

[415] Exec. Order 12,333, 46 Fed. Reg. 59,941 (1981) (amended by Exec. Order 13,284 (2003), Exec. Order 13355 (2004), Exec. Order 13,470 (2008)). This Executive Order – and not the FISC – governs

"concerning United States persons" only for foreign-intelligence and counterintelligence purposes.[416] Further, the order requires the Intelligence Community to promulgate guidelines that govern the collection, processing, retention, and dissemination of foreign intelligence not collected pursuant to FISA.[417] These guidelines must be approved by the Attorney General, and they provide significant restraints on the Intelligence Community's acquisition and handling of both American and European data.[418]

President Obama has further expanded upon these limitations in PPD-28.[419] This directive sets a number of requirements for foreign intelligence and counterintelligence:

- "The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive";
- "Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities";
- "Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes."[420]

To reinforce these requirements (and consistent with the the recommendations of the UN Human Rights Council that national security intelligence not contravene human rights and that counter-intelligence surveillance is "used exclusively for these purposes"[421]), '"[signals intelligence] information about the routine activities of a foreign person' would not be considered foreign intelligence."[422] It prohibits the collection of signals intelligence to "suppres[s] or burde[n] criticism or dissent, or [to] disadvantag[e] persons based on their ethnicity, race, gender, sexual orientation, or religion."[423]

PPD-28 further sets out transparency requirements and retention limitations, and it declares that "these polices and procedures are to be applied equally to the personal

---

the collection, storage, and dissemination by the Intelligence Community of data that is not received, stored, or processed in the United States. It does not authorise the conduct of any surveillance.

[416] *Id.* §§ 1.12(b) (detailing responsibilities of NSA); 2.3 (collection limitations).

[417] *See, e.g.*, United States Signals Intelligence Directive USSID SP0018 (Jan. 25, 2011).

[418] *Id.*

[419] Presidential Policy Directive/PPD-28 (Jan. 17, 2014), http://fas.org/irp/offdocs/ppd/ppd-28.pdf.

[420] *Id.* § 1(a)–(b); *see also* Robert Litt, Gen. Counsel, ODNI, *Prepared Remarks on Signals Intelligence Reform at Brookings Institute* (Feb. 4, 2015) ("Signals intelligence will be collected only when there is a valid foreign intelligence or counterintelligence purpose.").

[421] FRA Report, *supra* note 127, at 18.

[422] Litt, *Prepared Remarks on Signals Intelligence Reform*, *supra* note 420.

[423] PPD-28 § 1(b); *cf.* FRA Report, *supra* note 127, at 13 (describing UN good practices).

information of all persons, regardless of nationality."[424] It requires application of minimization procedures comparable to those promulgated under Executive Order 12,333 to information on non-US persons, living outside of the United States.[425] The Intelligence Community, in the months following PPD-28's release, promulgated and released guidelines and procedures implementing the President's orders.[426]

As noted above, FISA's provisions govern the US intelligence agencies' collection, retention, and dissemination in the US of data transmitted to US persons and stored in US servers. That said, the extraterritorial protections provided by Executive Order 12,333 and, particularly, PPD-28 have not yet been emulated by other responsible actors on the world stage. "[E]very nation recognizes legal distinctions between citizens and non-citizens,"[427] In taking these steps to establish safeguards for non-citizens, the US has initiated new norms for protection of rights and freedoms and global rule of law among democratic nations.

President Obama's actions were based on the recommendations of a special review committee, appointed by the President, to conduct a thorough and unrestricted assessment of United States's intelligence and surveillance capabilities and the best means of maintaining public trust in the government's use of those tools.[428] This exceptional review process was in addition to the ongoing oversight by the Privacy and Civil Liberties Oversight Board (PCLOB), agency inspectors general, agency civil liberties officers, and outside groups.

With each of the above specific legal authorities and others, the United States government has limited the scope of its surveillance activities, as well as its processing, retention, and dissemination of collected data. It has imposed rigorous oversight for approval and review of each of these surveillance activities. And, in the event of government overreach, it has provided for legal remedies and redress so that Congress and individuals may hold the executive branch to account.

---

[424] *Id.* § 4(a)(i).

[425] *See id.* §§ 1(d), 4(a)(i); *see also* Robertson, *Opinion*, *supra* note 398, at para. 33 (noting that "the requirement under [Executive Order 12,333] that intelligence agencies use 'the least restrictive means feasible' applies to all intelligence gathering activities irrespective of the citizenship of the targets").

[426] *See, e.g.*, NSA, *Minimization Procedures Used by the National Security Agency in connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702* (Feb. 2, 2015), http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; FBI, *Presidential Policy Directive 28 Policies and Procedures* (Feb. 2, 2015), https://www.fbi.gov/about-us/nsb/fbis-policies-and-procedures-presidential-policy-directive-28-1; CIA, *Signals Intelligence Activities Guidelines* (Feb. 2, 2015), http://www.dni.gov/files/documents/ppd-28/CIA.pdf; Off. of the Dir. of Nat'l Intelligence, *Minimization Procedures* (July 24, 2014), http://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[427] Litt, *Privacy, Technology & National Security*, *supra* note 362.

[428] *See* President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; President Barack Obama, Remarks by the President in a Press Conference (Aug. 9, 2013), https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

With this background, this report looks in greater detail at these main US surveillance programs and authorities in light of the four criteria distilled from basic requirements of the EU legal order for surveillance, as described in Part One of this report and applied to EU surveillance in the preceding section. As with the EU legal order, it goes through each of these criteria to examine concrete safeguards to limit interference with rights and freedoms.

2.2.2 Specific Legal Authority

> *Surveillance measures must be based on clearly stated legal authority. The legal basis or purposes for the types of surveillance undertaken must be clearly spelled out. These purposes must be for legitimate aims of a serious nature with objective basis in facts. There must be objective criteria by which to limit the discretion of authorities.*

As discussed above, the US legal order authorizes both law enforcement and the Intelligence Community to conduct surveillance, but only within constitutional, statutory, and executive limits and only for specific purposes. These legal sources and justifications are available to the public and open to legal challenges. Together, they guide authorities' access, collection, analysis, storage, and dissemination of European citizens' data within the United States.

Law Enforcement

All sovereign powers share a responsibility to ensure the safety of those within their borders, and a basic function of the US government, like '"any government[,] is to provide for the security of the individual and of his [or her] property."'[429] Doing so means preventing criminal acts and punishing those who commit them.

Electronic surveillance is a response to "[t]he marked acceleration in technological developments[,] and sophistication in their use [that] ha[s] resulted in new techniques for the planning, commission, and concealment of criminal activities."[430] Congress has responded to this threat with the Wiretap Act and ECPA, which permit the "prudent and lawful employment of those very techniques which are employed against the Government and its law abiding citizens."[431] They make it possible "to combat successfully certain forms of crime."[432]

---

[429] *Keith*, 407 U.S. at 312 (quoting *Miranda v. Arizona*, 384 U.S. 436, 539 (1966) (White, J., dissenting)).

[430] *Id.*; *see also* Danny Yadron, Alistair Barr & Daisuke Wakabayashi, *Paris Attacks Fan Encryption Debate*, WALL ST. J. (Nov. 19, 2015), http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407; David E. Sanger & Nicole Perloth, *F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist*, N.Y. TIMES (Dec. 9, 2015), http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html.

[431] *Keith*, 407 U.S. at 312.

[432] *Dalia v. United States*, 441 U.S. 238, 252 (1979).

The Wiretap Act and ECPA set out the conditions that justify law enforcement's use of electronic surveillance to intercept or collect the contents of communications, *i.e.*, a finding of probable cause.[433] These statutes – read against the backdrop of the Fourth Amendment – provide the only means by which law enforcement may conduct electronic surveillance in the United States.

Obtaining a Title III warrant requires law enforcement to demonstrate to a neutral magistrate that probable cause exists to believe that the particular communications are relevant to a crime,[434] and that the crime being investigated is among an enumerated list of serious felonies, such as sabotage and espionage, offenses related to biological weapons, arson, kidnapping, murder, piracy, various forms of bribery, racketeering, human trafficking, and forced labour.[435] This link can be demonstrated by tying the target, the telephone number used, or another aspect of the communication to the crime. No matter how useful real-time interception of communications might be for investigations into lesser crimes, this type of interception is *per se* unavailable.

The requirement of probable cause for the issuance of a warrant ensures that the use of surveillance authority is reasonably necessary for the investigation of the serious crimes for which it is permitted. "[P]robable cause is a fluid concept – turning on the assessment of probabilities in particular factual contexts[,]" but it generally requires "a substantial basis for concluding that a search would uncover evidence of wrongdoing."[436] This standard requires, at a minimum, individualized examination of the government's information and reasons for the seizure of the communications by an independent court.[437] And the Wiretap Act demands that this information be expressed in detail.[438]

The Fourth Amendment mandates the same showing of probable cause (without being limited to certain crimes) to obtain the contents[439] of stored communications, such as emails and voicemails.[440] The government accordingly must show (and a neutral magistrate must find) that there is a substantial basis to believe that the communications to be collected relate to a crime.

---

[433] *See infra* at Part 2.3.3.

[434] Fed. R. Crim. P. 41.

[435] 18 U.S.C. § 2516(1).

[436] *Gates*, 462 U.S. at 236–37 (alterations omitted).

[437] *See* US Dep't of Justice, *Electronic Surveillance Manual: Procedures and Case Law Forms* 3–6 (2005), *available at* http://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf.

[438] *Id.*; *see also* 18 U.S.C. § 2518.

[439] *See supra* note 355 and accompanying text (describing distinction between content and non-content information).

[440] *Warshak*, 631 F.3d at 288 (6th Cir. 2010).

Collecting non-content information or metadata requires a lesser showing, but each avenue is subject to an oversight body. For instance, a Section 2703(d) order may be based on "reasonable suspicion"[441] to obtain stored metadata, a standard short of probable cause, but a neutral magistrate still must approve the collection.[442] A subpoena does not necessitate the *ex ante* involvement of the judiciary, but a grand jury of ordinary citizens controls the use of the information and the target of the subpoena may challenge its issuance.[443]

Each statute contains narrow exceptions to these collection requirements for exigent circumstances,[444] but the invocation of such circumstances simultaneously triggers further oversight.[445] For instance, the Wiretap Act permits "any investigative or law enforcement officer, specially designated by the Attorney General [or other high-ranking prosecutors], who reasonably determines that [certain] emergency situation[s] exis[t] … to authorize … interception," but such unilateral authorisation is contingent upon a successful application to a neutral magistrate within 48 hours.[446] If the application is subsequently denied, "the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of [the Wiretap Act]."[447]

No overriding "national security" or "executive privilege" exception exists that would permit ongoing large-scale surveillance by law enforcement without corresponding safeguards.

Intelligence Community

The President, as Chief Executive and commander-in-chief of the military and intelligence agencies,[448] has the responsibility and the power to thwart attacks on national security.[449] The President's powers under the Constitution therefore

---

[441] "Reasonable suspicion" and "probable cause" "are commonsense, nontechnical conceptions that deal with the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Ornelas v. United States*, 517 U.S. 690, 695 (1996). They "acquire content only through application," but the Supreme Court has described "reasonable suspicion" as having "a particularized and objective basis for suspecting the person stopped [or searched] of criminal activity." *Id.* at 696. "Probable cause," on the other hand, requires "known facts and circumstances … sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Id.*

[442] 18 U.S.C. § 2703(d).

[443] Fed. R. Crim. P. 17.

[444] *See* 18 U.S.C. §§ 2518(7)(a) (Wiretap Act); 2702(c) (ECPA).

[445] *See id.* §§ 2518(7)(b) (Wiretap Act); 2702(d) (ECPA).

[446] *Id.* § 2518(7).

[447] *Id.* § 2518(7)(b).

[448] U.S. Const. art. II, § 2, cl. 1 ("The President shall be commander in chief of the Army and Navy of the United States, and of the militia of the several states, when called into the actual service of the United States.").

[449] *Keith*, 407 U.S. at 310.

encompass the power to initiate surveillance. "Accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents is essential to informed decisionmaking in the areas of national defence and foreign relations,"[450] and the United States government must also protect "against those who would subvert or overthrow it by unlawful means."[451]

Accordingly, the United States, like other nations, has gathered intelligence throughout its history. Congress and various presidents have taken steps to circumscribe that power to ensure that privacy and civil liberties are considered, balanced, and protected.

Most significant among these safeguards is FISA Title I. This statute builds on the protections of the First and Fourth Amendments to the Constitution and permits "electronic surveillance" by the Intelligence Community only if a significant purpose is to obtain "foreign intelligence information."[452] This term is specifically defined to mean "information that relates to … the ability of the United States to protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction; or (C) clandestine intelligence activities by an intelligence service or network."[453] The term "foreign intelligence information" also includes "information with respect to a foreign power or foreign territory that relates to … the national defense or the security of the United States; or … the conduct of the foreign affairs of the United States."[454] Executive Order 12,333, which binds the intelligence agencies whether FISA applies or not, defines "foreign intelligence" even more narrowly to include only "information relating to the capabilities, intentions and activities of foreign powers, organizations or *persons*."[455] Read literally, the italicised text could encompass all non-US persons, but ODNI has directed that "Intelligence Community elements should permanently retain or disseminate [a foreign person's] information only if [it] relates to an authorized intelligence requirement [and] not *solely* because of the person's non-U.S. person status."[456] Moreover, the United States has also defined "intelligence related to national security" explicitly to include information involving "threats to the

[450] Exec. Order 12,333 § 2.1; *see also FRA Report*, *supra* note 127, at 13 ("Intelligence services play an important role in protecting national security and upholding the rule of law.").

[451] *Keith*, 407 U.S. at 310–11.

[452] 50 U.S.C. §§ 1804(a)(6)(A)–(B); 1805(a)(4).

[453] *Id.* § 1801(e)(1).

[454] *Id.* § 1801(e)(2).

[455] Exec. Order 12,333 § 3.4(d) (emphasis added); *see also id.* § 3.4(a) (defining "counterintelligence" to mean "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs").

[456] ODNI, *Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28*, at 5 (July 2014), http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

United States, its people, property, or interests [and] the development, proliferation, or use of weapons of mass destruction[.]"[457]

As in the law-enforcement context, the neutral magistrate (here, the FISC) must determine that probable cause exists to believe that the communications to be intercepted are linked to the approved purposes of foreign-intelligence surveillance.[458] Unlike the law-enforcement context, however, the government must also show that there is a substantial factual nexus between the proffered *target* (as opposed to the target *or* an identified facility, such as a telephone number) and a foreign power, organisation, or person.[459]

The Intelligence Community must similarly demonstrate that its proposed collection under Sections 702 and 215 are for valid foreign-intelligence purposes, [460] and with respect to Section 702, the NSA analysts must show that the targeted person is outside the United States.[461]

Although these definitions and concepts leave some elasticity to meet extraordinary threats to national security, some justifications for surveillance are placed entirely outside the US legal order: "The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[462] This provides protection to all persons' freedom of expression and guarantees equal protection. Moreover, "[t]he collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to US companies and US business sectors commercially."[463]

Finally, the Intelligence Community sets national priorities, through an interagency process involving the highest officials, in foreign-intelligence collection each year.[464] These priorities, encapsuled in the "National Intelligence Priorities Framework," focus the government's efforts and further place practical constraints and supervision on US surveillance activities.

---

[457] 50 U.S.C. § 3003(5)(B); *see also Cole v. Young*, 351 U.S. 536, 543 (1956) (defining "national security" as "those activities which are directly concerned with the Nation's safety, as distinguished from the general welfare.").

[458] *See* 50 U.S.C. § 1805(a); *Gates*, 462 U.S. at 237 (defining "probable cause").

[459] *See* 50 U.S.C. § 1804.

[460] *Id.* §§ 1861(a), (c); 1881a(a), (i)

[461] *Id.* § 1881a(a).

[462] PPD-28 § 1(b).

[463] *Id.* § 1(c).

[464] James Clapper, DNI, *National Intelligence Priorities Framework* (January 2, 2015), http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf; *see also* Litt, *Privacy, Technology & National Security*, *supra* note 362.

2.2.3 Limited Scope

The amount of data collected or subject to retention requirements must not go beyond what is necessary to accomplish the purpose of the surveillance and cannot be generalized or indiscriminate. Discriminants must be established with due care and consistent with the specified purposes for surveillance. The period of retention must be reasonable and finite.

The US legal order limits the scope of US surveillance even when it meets the legal and factual requirements that establish the necessary threshold. The Constitution, statutes, and binding executive pronouncements specifically constrain the ability of law enforcement and the Intelligence Community to collect, retain, access, and use personal information. This section addresses these limits on law enforcement and then those on the Intelligence Community.

Collection

The collection of personal information, whether through real-time interception of communications or access to stored contents of emails, is regarded by the US legal order as an interference with privacy. "Privacy and civil liberties [are] integral considerations in the planning of U.S. signals intelligence activities."[465] The United States has therefore taken steps to minimize the discretion of law enforcement and the Intelligence Community to collect the personal information of persons who are targets of surveillance, much less that of all other persons. This includes persons outside the United States.[466]

Law Enforcement

The Fourth Amendment's warrant and reasonableness requirements govern law-enforcement's ability to collect information. The Wiretap Act and ECPA layer on additional safeguards commensurate with the level of privacy invasion.

The probable-cause standard limits the targets of surveillance to those persons or facilities (*i.e.*, place, number, or device used) as to whom there is a factual basis to believe a connection to serious crimes exists.[467] This factual basis must be spelled out with particularity,[468] including the "*particular* offense that has been, is being, or is about to be committed," a "*particular* description of the nature and location of the facilities from which the communication is to be intercepted," and "a *particular* description of the type of communications to be intercepted."[469] This specificity

[465] PPD-28 § 1(b).

[466] "[N]o [other] country in the world that ha[s] significant surveillance capabilities ha[s] extended privacy protections, as a binding concept, to noncitizens abroad[.]" Savage, *Power Wars*, *supra* note 370, at 605.

[467] 18 U.S.C. § 2518(3).

[468] *Id.* §§ 2516(1)(b)–(e); 2518(1)(b) (requiring "full and complete statement of facts and circumstances").

[469] *Id.* § 2518(1)(b) (emphasis added).

requirement ensures that the interception or collection of communications is targeted.

Moreover, in seeking a Title III warrant to intercept real-time communications, law enforcement must also show that other, less-intrusive "investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[470] This too protects against over-collection of information.

Once the warrant issues, the protections continue. Interception authorisation, for example, remains in effect only for 30 days absent reapplication to a magistrate,[471] and law enforcement may only record and collect information relevant or likely relevant to the ongoing investigation or other criminal activity.[472] Law enforcement, pursuant to this latter provision, must undertake reasonable efforts to narrowly tailor their interceptions to the specific investigation at hand.[473] In practical terms, this requirement means that law enforcement must devise and employ procedures so as not to record non-pertinent conversations regarding, for instance, family matters; if such conversations are inadvertently collected, they may have to be deleted.[474] The minimization requirements in each case will likely be different, but one constant is that privileged communications between an attorney and client maintains their privileged character and, with very narrow exceptions, should not be recorded.[475]

Law enforcement's burden for obtaining stored contents of communications likewise imposes specificity and proportionality requirements. The Fourth Amendment requires the government to obtain a warrant – with all of its requirements – from a neutral magistrate before collecting the stored contents of communications.[476] Thus, a search warrant application, similar to one for a wiretap, must specifically identify the communications to be seized, so as to limit the intrusion into a person's private correspondence, and show that probable cause exists to believe the contents seized will be related to a crime.[477]

The government must issue legal process, demonstrating a legitimate law-enforcement interest in the information, to collect non-content personal data[478] that

---

[470] *Id.* § 2518(1)(c).

[471] *Id.* § 2518(5).

[472] *Id.* § 2518(5).

[473] *See Scott v. United States*, 436 U.S. 128, 138 (1978).

[474] *See, e.g.*, *United States v. Mansoori*, 304 F.3d 635, 646 (7th Cir. 2002) (detailing minimization order); *see also* Clifford S. Fishman, *The "Minimization" Requirement in Electronic Surveillance: Title III, the Fourth Amendment, and the Dread Scott Decision*, 28 AM. U. L. REV. 315, 327–29 (1979) (describing minimization strategies).

[475] 18 U.S.C. § 2517(4).

[476] *Id.* § 2703(a); *Warshak*, 631 F.3d at 288 (6th Cir. 2010).

[477] Fed. R. Crim. P. 41.

[478] *See supra* note 355 and accompanying text (describing distinction between content and non-content information).

has been shared with third parties.[479] The government must specifically show that "there are reasonable grounds" to believe that the information is "relevant and material to an ongoing criminal investigation"[480] to obtain a § 2703(d) order.[481] Such an order allows the government to collect the non-content information without providing notice to the target.[482]

Grand-jury and administrative subpoenas will also suffice to obtain non-content personal information and may issue, respectively, so long as a grand jury has been empanelled or an agency investigation is ongoing. The recipient of the subpoena – most likely, a service provider – may challenge the subpoena, however, before a neutral magistrate as "unreasonable or oppressive."[483] If the government cannot make a sufficient showing, it cannot obtain the requested information. Entities that are not service providers may release information upon a written request, but they are also free to demand that law enforcement issue legal process (*i.e.*, a subpoena) as well.[484]

Intelligence Community

FISA Title I, Section 702, Section 215, and various Presidential orders similarly limit the Intelligence Community's ability to collect foreign-intelligence information.

Under Title I of FISA, the government must show[485] probable cause to believe that the real-time communications it proposes to intercept contain foreign-intelligence information,[486] within the specific definitions and limitations discussed above. Only then will the FISC issue a FISA warrant.

Section 702 likewise limits the acquisition of the contents of communications. Under this section, the government:

---

[479] 18 U.S.C. § 2702(a).

[480] *Id.* § 2703(d).

[481] *See supra* note 442 and accompanying text (describing Section 2703(d) orders).

[482] 18 U.S.C. § 2703(d).

[483] Fed. R. Crim. P. 17(c)(2); *see also United States v. R. Enters., Inc.*, 498 U.S. 292, 299 (1991) ("Grand juries are not licensed to engage in arbitrary fishing expeditions, nor may they select targets of investigation out of malice or an intent to harass. In this case, the focus of our inquiry is the limit imposed on a grand jury by Federal Rule of Criminal Procedure 17(c), which governs the issuance of subpoenas *duces tecum* in federal criminal proceedings. The Rule provides that '[t]he court on motion made promptly may quash or modify the subpoena if compliance would be unreasonable or oppressive.'").

[484] 18 U.S.C. § 2702(a).

[485] These applications go through multiple, assending levels of review within the FBI and the Department of Justice. Litt, *Privacy, Technology & National Security*, *supra* note 362.

[486] 50 U.S.C. § 1805(b).

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
>
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.[487]

The Intelligence Community, to this point, has promulgated targeting procedures that implement Section 702.[488] These procedures remain classified, but they have been reviewed and approved by the FISC[489] – and their existence demonstrates that collection under Section 702 is not indiscriminate.[490] They also have been presented to the PCLOB for pre-implementation review and comment,[491] and previous versions have been declassified and released to the public.[492]

---

[487] *Id.* § 1881a(b).

[488] *See, e.g.*, 50 U.S.C. § 1881a(d); NSA, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (July 28, 2014), http://www.dni.gov/files/documents/0928/NSA%20Section%20702%20Targeting%20Procedures.pdf; Affidavit of Richard H. Ledgett, Jr., Acting Dir., NSA (July 28, 2014), http://www.dni.gov/files/documents/0928/Affidavit%20of%20Acting%20Director%20NSA.pdf; Affidavit of James B. Comey, Dir., FBI (July 28, 2014), http://t.umblr.com/redirect?z=http%3A%2F%2Fwww.dni.gov%2Ffiles%2Fdocuments%2F0928%2FAffidavit+of+Director+FBI.pdf&t=ZjkyODczZGFmMTlkMDY1YTE5ZjU1YTdhNThmMGJjZTQ2NTllNzVjZSw5YWRlOTg3Qw%3D%3D.

[489] Memorandum Opinion, [*Caption Redacted*], No. [Redacted], (FISA Ct. Aug. 26, 2014), http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

[490] Litt, *Privacy, Technology & Intelligence Collection*, *supra* note 362 ("The targeting procedures are designed to ensure that we target someone only if we have a valid foreign intelligence purpose.").

[491] Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 40.

[492] *See, e.g.*, NSA, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (July 22, 2009), http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.

These FISC-approved targeting procedures mandate the use of selectors or discriminants,[493] and the application of such procedures is carefully supervised.[494] A trained analyst, for instance, initially proposes a particular selector – an email address or telephone number, not a keyword or name – based on the targeting procedures' criteria.[495] Documentation must link the selector to a specified foreign-intelligence purpose.[496] Two different senior NSA analysts must review the proposed selector and the accompanying documentation to ensure it complies with the FISC-approved targeting procedures and then approve it before it is tasked and sent to a service provider.[497]

Tasked selectors are regularly reviewed by the NSA to ensure continued compliance with the targeting procedures. Analysts audit the collected materials every 30 days to determine whether the tasked selector is still associated with a valid "foreign intelligence target,"[498] and they must annually re-verify that the selector relates to a foreign intelligence purpose. The NSA additionally logs and demands justification for each query[499] run on collected data to detect abuse.[500]

---

[493] *See, e.g.*, 50 U.S.C. § 1881a(d), (g)(2).

[494] *See infra* Part 2.3.4.

[495] PCLOB, Section 702 Report, *supra* note 380, at 45–46; Rebecca J. Richards, Dir. of NSA Civil Liberties & Privacy Office, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333*, Part II(3)–(4) (Oct. 7, 2014). The NSA, to further safeguard this tool, requires supervisor approval for each analyst working on a particular mission and that each analyst complete required training. Richards, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333*, *supra* note 495, at Part III.

[496] PCLOB, Section 702 Report, *supra* note 380, at 45; Richards, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333*, *supra* note 495, at Part II(4).

[497] PCLOB, Section 702 Report, *supra* note 380, at 46; Richards, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333*, *supra* note495, at Part III(8) (The agency "perform[s] pre-targeting research and two-person review and approval before entering any [selector or discriminant] into NSA's collection systems, and conduct[s] checks throughout the targeting process to review and validate that the acquired collection is responsive to the documented foreign intelligence need.").

[498] PCLOB, Section 702 Report, *supra* note 380, at 48.

[499] In *Schrems v. Data Protection Commissioner*, [2014] IEHC 310, para. 12, the Irish High Court cited a *Guardian* newspaper article, disclosing the existence of "X Keyscore." According to the Guardian report, this programme permits NSA "analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing history of millions of individuals." *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet*, THE GUARDIAN (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. The NSA has denied the charges that XKeyscore is operated by unsupervised analysts and stated that analyst queries are subject to audit and compliance mechanisms. NSA Press Statement (July 30, 2013), http://icontherecord.tumblr.com/search/xkeyscore. The documents released concerning the programme show that it operates as a search tool used on already-collected data – not as a means of collection. Since the programme is not aimed at data stored in the US, data of EU citizens transferred to the US is unaffected. The NSA may collect data transmitted to and stored in the United States only through the use of selectors and discriminants as described. Illustrative Member States also deploy XKeyscore on data collected in Europe. *See, e.g.*, *Document Pertaining to the Agreement Between the NSA and Germany's Domestic Intelligence Agency BfV*,

This multi-step system limits the government's collection of communications from non-US persons significantly.[501] In 2014, for example, the Section 702 programme affected only 92,707 targets out of all the individuals whose data was available in the United States.[502] This number, while not trivial, falls far short of the initial reports on the PRISM programme in the *Washington Post* that "[t]he National Security Agency and the FBI are tapping directly into the central servers of … leading internet companies, extracting audio, video, photographs, e-mails, documents, and connection logs that enable analysts to track a person's movements and contacts over time."[503]

Furthermore, Section 702 authorizations are limited to one year and, to continue beyond that year, the Attorney General and the DNI must make another joint certification to the FISC and obtain a second approval.[504] And minimization procedures, discussed further below, ensure that legally-privileged attorney-client communications – to the extent feasible – are not collected.[505] "As soon as it becomes apparent that a communication is between a person who is known to be

---

ZEIT ONLINE (August 26, 2015) (reporting Germany's use of XKeyscore), http://www.zeit.de/digital/datenschutz/2015-08/xks-xkeystore-document.

[500] Richards, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333*, *supra* note 495, at Part III.

[501] Robertston, *Opinion*, *supra* note 398, at para. 31 (noting that use of selectors under Section 702 "is not 'bulk' or 'generalised' collection, and is more akin to the 'strategic monitoring' which was upheld by the European Union in *Weber and Saravia*.").

[502] *See* ODNI, *2014 Transparency Report*, http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

The NSA has stated publicly that NSA '"touches' about 1.6%, and analysts only look at 0.00004%, of the world's internet traffic.'" Joint Statement from the Office of the Director of National Intelligence and the National Security Agency (Aug. 21, 2013), https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_NSA.pdf

[503] Barton Gellman & Laura Poitras, *U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, available at http://www.sanders.senate.gov/newsroom/must-read/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program.

On June 7, 2013, the Washington Post updated this article to provide additional context, including the revelation that US *and British* intelligence agencies were conducting the programme and that these intelligence agencies were required to provide the service providers with legal process (a "directive") and discriminants. *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), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; *see also* Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 14–15 & n.41.

[504] 50 U.S.C. § 1881a(a).

[505] *See* Letter from Keith B. Alexander, Dir. of NSA, to James R. Silkenat, President, American Bar Ass'n (Mar. 10, 2014).

under a criminal indictment in the United States and an attorney who represents that individual," for example, "monitoring of that communication will cease."[506] Any such communications already collected are then segregated by the Department of Justice.[507]

Section 215 of the PATRIOT Act, as amended by the USA FREEDOM Act, also contains an important limit on Intelligence Community acquisition of data. As noted above, the government must submit "specific selection term[s]" (or "selectors" or "discriminants") to the telecommunications providers to prevent bulk and indiscriminate collection of metadata.[508] Metadata collected pursuant to these selectors is then reviewed, and any nonresponsive records are immediately destroyed.[509]

Together, these requirements restrain both law enforcement and the Intelligence Community collection of personal information. They require that the government specify in various degrees what particular communications or data it wishes to access, and they set a limit on how much the government may acquire.

Retention

The United States has instituted significant limitations on the government's ability to retain data automatically for indefinite periods of time.

Law Enforcement

The Wiretap Act requires that the contents "be recorded … in such a way as will protect the recording from editing or other alterations" and "made available to the judge issuing [the Title III warrant] and sealed under his [or her] directions."[510] The neutral magistrate may then order them destroyed; otherwise they are "kept for ten years."[511]

No particular statute limits the federal government's storage of information collected under ECPA. However, each federal law-enforcement agency, including the FBI, has promulgated a record-retention plan approved by the National Archives and Records Administration.[512] The government must retain the data under this plan and

---

[506] *Id.* at 3 (quoting NSA, *Section 702 Minimization Procedures* § 4).

[507] *Id.*

[508] 50 U.S.C. § 1861(b)(2).

[509] NSA, *Minimization Procedures Used By the National Security Agency in Connection with the Production of Call Detail Records Pursuant to Section 501 of the Foreign Surveillance Intelligence Act*, at 2 (Nov. 2015), https://www.nsa.gov/civil_liberties/_files/UFA_SMPs_Nov_2015.pdf.

[510] 18 U.S.C. § 2518(8)(a).

[511] *Id.* § 2518(8)(a).

[512] *See* US Dep't of Justice, *The Attorney General's Guidelines for Domestic FBI Operations* 35 (2008), http://www.justice.gov/archive/opa/docs/guidelines.pdf; *see also* 5 U.S.C. § 552a (Privacy Act, which limits dissemination of records); 36 C.F.R. §§ 1220.1–1227.14 (NARA regulations).

additional guidelines created by the Attorney General only so long as investigation remains open.[513]

The US surveillance authorities also do not impose any default retention requirement on private service providers with two exceptions. One, law enforcement may in individual cases request that service providers preserve specific stored contents of communications for 90 days pursuant to ECPA,[514] but such requests are limited to the identified communications. Two, the Federal Communication Commission – the independent federal agency charged with regulating telephone and internet service providers – requires that regulated service providers maintain records for 18 months for billing purposes.[515] That requirement, however, is wholly independent of the surveillance regime.

Finally, PPD-28 – along with other "Executive Orders, proclamations, Presidential directives, IC directives, and associated policies" – require that the information collected and retained be stored securely and limited to "authorized personnel."[516]

Intelligence Community

Various FISA provisions and Attorney General guidelines prohibit indiscriminate and indefinite storage of specific communications collected pursuant to a FISA Order. Foremost among them are the minimization procedures promulgated by the Attorney General and approved by the FISC.[517] These procedures require that the Intelligence Community determine whether unencrypted data should be permanently preserved as foreign intelligence or be destroyed within five years. To store the information beyond five years, the analysts must obtain express authorisation.[518]

Minimization procedures also apply to the communications and data collected under Section 702. The same five-year timeline applies to data collected under PRISM,[519] and a two-year maximum applies to unanalysed data obtained pursuant to Upstream.[520] Moreover, President Obama has stated that "long-term storage of personal information [is] unnecessary to protect [the United States's] national security [and] is inefficient, unnecessary, and raises legitimate privacy concerns."[521]

---

[513] US Dep't of Justice, *The Attorney General's Guidelines for Domestic FBI Operations*, *supra* note 512 at 36.

[514] 18 U.S.C. § 2703(f).

[515] 47 C.F.R. § 42.6.

[516] PPD-28, § 4(a)(ii).

[517] 50 U.S.C. §§ 1801(h), 1805(a)(3).

[518] *See* USSID SP0018 § 6.

[519] PPD-28, § 4(a).

[520] NSA, Dir. of Civil Liberties and Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, at 8 (2014), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.

[521] PPD-28 § 4(a)(i).

Furthermore, outside of FISA, PPD-28 directs that "[p]ersonal information [of foreign citizens] shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333."[522] Pursuant to this directive, the minimization procedures now direct that communications clearly unrelated to foreign intelligence be destroyed as soon feasible[523] and that "[n]onpublic communications that are acquired by the [US Intelligence Community] that contain personal information of non-U.S. persons may be retained in their original or transcribed form only … for up to 5 years unless the Director of National Intelligence … has expressly determined in writing that continued retention is in the national security interests of the United States."[524]

The Section 215 programme under the USA FREEDOM Act strikes a similar balance. The Act explicitly forbids the bulk collection of metadata stored in the United States,[525] and the service providers, who store the metadata, are not required to retain such information beyond the necessary 18-month period imposed by the FCC.[526] Metadata that is properly collected, in turn, must be destroyed within five years after the initial collection.[527] These limits balance the need for privacy and the recognition that "the significance to our national security of intelligence is not always apparent upon an initial review of information."[528]

Finally, as with information collected by law enforcement, the personal data stored by the government is kept secure from unauthorised access.[529]

Access And Dissemination

The US legal order further limits the scope of law enforcement's and the Intelligence Community's intrusions into the privacy of individuals by regulating who has access to collected and retained information and under what conditions that information may be released.

---

[522] *Id.* § 4(a)(i).

[523] Dep't of Justice, *Section 702 Minimization Procedures*, *supra* note 509, at § 3(c)(1)–(2); *see also* NSA, Dir. of Civil Liberties and Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, at 8 (2014), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.

[524] NSA *PPD-28 Section 4 Procedures* § 6.1(a) (Jan. 12, 2015). Department of Defense guidelines likewise call for the destruction of inadvertently intercepted communications "as soon as feasible." Dep't of Def., *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, No. DoD 5240 1-R, at C5.3.3.2.2 (1982).

[525] Pub. L. No. 114–23, § 103 (amending 50 U.S.C. § 1861(b)(2), (c)).

[526] *See* Savage, *Power Wars*, *supra* note 370, at 608.

[527] NSA, *2015 Minimization Procedures*, *supra* note 509, at 7.

[528] PPD-28 § 4(a).

[529] *See, e.g.*, Litt, *Privacy, Technology & National Security*, *supra* note 362 ("[W]e have secure databases to hold this data, to which only trained personnel have access.").

Law Enforcement

Law enforcement use of communications intercepted or collected under the Wiretap Act or ECPA must be consistent with the strictures imposed by 18 U.S.C. § 2517. These rules, in various ways, limit the dissemination of information to legitimate law-enforcement and counterterrorism purposes.

Furthermore, the recordings and other "evidence derived therefrom" may not be introduced in criminal proceedings against a defendant unless the government "furnish[es] a copy of the court order, and accompanying application, under which the interception was authorized or approved."[530] This disclosure permits a defendant to "move to suppress the contents" of the intercepted communications or evidence found due to the interception.[531] This right includes seeking to suppress the use of privileged communications, regardless of whether they are intercepted or otherwise collected.[532]

Intelligence Community

The US legal order imposes even stricter restrictions on the use and dissemination of information collected under the various sections of FISA. Section 1806 of FISA requires the government to "notify [an] aggrieved person and the court] that it intends to offer information collected via FISA "into evidence or otherwise use or disclose [it] in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against the aggrieved person." [533] Furthermore, Title I of FISA precludes "electronic surveillance" obtained via a FISA order from being "used or disclosed by Federal officers or employees except for lawful purposes,"[534] and information acquired as part of the Section 702 programme is governed by the same protections.[535]

In turn, regulations issued by the NSA define "lawful purposes" to include only those instances in which "personal information (i) is publicly available; (ii) is related to an authorized foreign intelligence requirement; (iii) is related to a crime that has been, is being, or is about to be committed; or (iv) indicates a possible threat to the safety of any person or organization."[536] Intercepted communications may be used for law-enforcement purposes only with the authorisation of the Attorney General,[537] and the Department of Justice regulations specifically preclude the dissemination of personal

---

[530] 18 U.S.C. § 2518(9).

[531] *Id.* § 2518(10)(a).

[532] *See id.* §§ 2517(4).

[533] 50 U.S.C. § 1806(c); *see also id.* § 1881e(a).

[534] *Id.* § 1806(e).

[535] *Id.* § 1881e

[536] NSA, *PPD-28 Section 4 Procedures* § 7.2 (Jan. 12, 2015).

[537] 50 U.S.C. § 1806(b).

information "about the routine activities of a non-U.S. person … without some indication that the personal information is related to an authorized foreign intelligence requirement."[538]

Privileged communications, in particular, receive protections. They may not, for instance, be used in criminal prosecutions.[539]

Section 215 likewise precludes government officials from using and disclosing the obtained information, except as authorized by law.[540]

2.2.4 Oversight

There should be some combination of executive, legislative, judicial and expert oversight for approval and review of surveillance measures.

The United States has instituted structural and statute-specific oversight mechanisms that operate on multiple levels. First, there is the judiciary. The Constitution and federal statutes mandate an essential role for judges – members of an independent branch of government, who hold their appointments for life, control when warrants issue, and supervise the execution of warrants. Second, there is the executive branch itself, which has appointed and empowered inspectors general and civil liberties officers to oversee and report on surveillance activities, established administrative controls, and releases public reports and other public information about surveillance. Third, there is Congress and its committees that control appropriations for government activities, hold hearings, and provide public reports. Finally, there are independent outside groups that have the power to request and release information and reports on the United States's surveillance activities. This report addresses each level of oversight in turn.

Judiciary

The US legal order places great emphasis on the independence of the judiciary, a branch co-equal with the executive and the legislature. As one member of the founding generation put it, "[t]he complete independence of the courts of justice is peculiarly essential in a limited Constitution."[541] The American Constitution protects the independence of federal judges by ensuring the concurrence of both of the other branches of the government through nomination by the President and confirmation by the Senate, and by conferring lifetime tenure without reduction in pay.[542]

In turn, the judiciary plays a key role in restraining and overseeing the surveillance activities of law enforcement and the Intelligence Community. Nearly all of the

[538] NSA, *PPD-28 Section 4 Procedures*, *supra* note 509 § 7.2.

[539] 50 U.S.C. § 1806(a).

[540] *See id.* § 1861(h) (governing use of information).

[541] THE FEDERALIST NO. 78 (Alexander Hamilton).

[542] U.S. Const. art. II, § 2; art. III, § 1.

government's surveillance tools require that the courts approve their deployment *ex ante*.

Wiretap Act

The Wiretap Act, as discussed above, requires the government to obtain a Title III warrant from a neutral magistrate before intercepting real-time communications. For such a warrant to issue, the judge must find on the basis of the required particularized showing[543] that probable cause exists to believe the intercepted communications will reveal evidence related to one or more enumerated felonies, that other means of acquiring the communications have been exhausted, and that the surveillance will be conducted in as limited a manner as possible.[544]

If the court approves the wiretap request, it continues to play a supervisory role. The government must reapply every 30 days – at a minimum – to maintain an authorized wiretap,[545] and the court may require status reports to justify continued authorisation before thirty days has run.[546]

To ensure that the courts are vigilant, the Wiretap Act also requires every judge who has issued a Title III warrant (or an extension) to report to the Administrative Office of the United States Courts, once the warrant has expired, the period for which surveillance was authorized, and the crime being investigated.[547] This information becomes the basis for a report by Administrative Office to Congress on the use of wiretaps each year.[548]

ECPA

The judiciary plays a similar role under ECPA. For the government to obtain a search warrant to collect stored contents of communications,[549] a judge must find that probable cause exists to believe the contents seized will be related to a crime.[550] The government may go ahead with the collection only once the court is satisfied that such a standard is met.

For a Section 2703(d) order to issue, permitting the government to acquire non-content information without providing notice to the target,[551] a neutral magistrate

---

[543] *See infra* part 2.2.2.

[544] 18 U.S.C. §§ 2516–18.

[545] *Id.* § 2518(5).

[546] *Id.* § 2518(6).

[547] *Id.* § 2519(1).

[548] *Id.* § 2519(3).

[549] *Id.* § 2703(a); *Warshak*, 631 F.3d at 288.

[550] Fed. R. Crim. P. 41.

[551] 18 U.S.C. § 2703(d).

must similarly find that "there are reasonable grounds" to believe that identified information is "relevant and material to an ongoing criminal investigation." And even when judicial approval is not necessary *ex ante*, *i.e.*, when the government uses a subpoena to acquire non-content information, the judiciary may decide whether to quash the government's request.[552]

FISA Title I

The FISC plays the dominant role in approving the Intelligence Community's conduct of electronic surveillance for foreign-intelligence purposes. The government may conduct such surveillance only by obtaining a FISA warrant,[553] which issues only if the FISC determines that probable cause exists to believe that the information the Intelligence Community proposes to intercept is foreign intelligence information.[554] FISA's probable-cause standard is identical to that used by courts under the Wiretap Act and ECPA. In recent years, the FISC has denied[555] and modified a number of FISA applications,[556] and the government has withdrawn others due to court scrutiny.[557] In multiple letters to Congress, the FISC has noted that "[i]n some cases," where the FISC judge "is inclined to deny [the government's application], the government may decide not to submit a final application, or to withdraw one that has been submitted, after learning that the judge does not intend to approve it."[558] These actions do not show up significantly in the statistics, even though "[d]uring the three month period from July 1, 2013 through September 30, 2013, [the court] observed that 24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action."[559]

Furthermore, the USA FREEDOM Act has authorized the FISC to appoint *amici curiae* charged with advancing "legal arguments that advance the protection of individual privacy and civil liberties."[560] The FISC, pursuant to this directive,

---

[552] Fed. R. Crim. P. 17(c)(2).

[553] 50 U.S.C. § 1803(a).

[554] *Id.* § 1805(a)–(b).

[555] *See, e.g.*, Report from Ronald Weich, Ass't Att'y Gen., to Sen. Joseph R. Biden, Jr., at 1 (Apr. 30, 2010) (noting that the FISC denied one FISA application), http://fas.org/irp/agency/doj/fisa/2009rept.pdf.

[556] *See, e.g.*, Report from Peter J. Kadzik, Principal Deputy Ass't Att'y Gen., to Sen. Harry Reid, at 1 (Apr. 30, 2014) (noting that the FISC modified 34 of 1,588 FISA applications for electronic surveillance), http://fas.org/irp/agency/doj/fisa/2013rept.pdf.

[557] Weich Report, *supra* note 555, at 1 (noting that the government withdrew 8 FISA applications).

[558] Letter from Hon. Reggie B. Walton, Presiding Judge, FISC, to Sen. Charles E. Grassley, at 3 (July 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Grassley-1.pdf; *see also* Letter from Hon. Reggie B. Walton, Presiding Judge, FISC, to Sen. Charles E. Grassley, at 1 (October 11, 2013) (providing additional statistics).

[559] October Letter from Hon. Reggie B. Walton to Sen. Charles E. Grassley, *supra* note 558, at 1.

[560] Pub. L. No. 114–23, § 401, 129 Stat. 279 (codified at 50 U.S.C. § 1803(i)(4)).

announced the appointment of five highly-qualified advocates on November 25, 2015.[561] The USA FREEDOM Act also requires the FISC to release publicly any FISC "decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act" within 45 days.[562] These provisions were designed to add balance to the FISC's largely *ex parte* proceedings.

Section 702

The FISC is heavily involved in the Intelligence Community's actions under Section 702. It reviews and approves the government's certification,[563] targeting procedures,[564] and minimization procedures.[565] This power is not merely theoretical: in 2011, the FISC held the government's Section 702 programme unconstitutional as applied, mandating changes (that were quickly implemented) to bring the programme into compliance with the Constitution and Section 702 itself.[566]

Section 702 also empowers the FISC to hear and investigate challenges from electronic-service providers to the Attorney General/Director of National Intelligence directives requiring the contents of communications.[567] If a directive fails to meet the statutory requirements or is otherwise unlawful, the FISC may set the directive aside.[568] If the FISC affirms the directive, Section 702 permits the service provider to appeal to the FISA Court of Review.[569]

FISC rules of procedure further require the government to report any instances of noncompliance with the FISC authorizations under Sections 702 and 215.[570] The

[561] *See* Poplin, *Amicus Curiae for FISC Announced*, *supra* note 371..

[562] Pub. L. No. 114–23, § 604, 129 Stat. 297 (codified at 50 U.S.C. § 1871(c)(1)).

[563] 50 U.S.C. § 1881a(i).

[564] 50 U.S.C. § 1881a(d).

[565] *Id.* § 1881a(e).

[566] Memorandum Opinion, [*Caption Redacted*], No. [Redacted], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011), http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf; *see also* Savage, *Power Wars*, *supra* note 370, at 564, 572 (detailing FISC criticism of government procedures).

[567] 50 U.S.C. § 1881a(h)(4); *see also* PCLOB, Section 702 Report, *supra* note 380, at 76 (noting FISC powers to investigate non-compliance).

[568] 50 U.S.C. § 1881a(h)(4); *see also In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, at *8–9 (FISA Ct. Rev. Aug. 28, 2008) ("Section 702(h) explicitly provides for the participation of parties other than the Government, in that electronic communication service providers can bring a challenge in the FISC to directives issued to them under the FAA.").

[569] 50 U.S.C. § 1881a(h)(6).

[570] FISC Rule of Procedure 13, http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

government, when issues have arisen, have made the required supplemental filings and confessions.[571] In fact, the temporary shuttering of Upstream by a federal district court in 2011 came about as a result of the government's self-reporting.[572]

Section 215

The FISC or another neutral magistrate must also approve a Section 215 order that requires service providers to release selected metadata.[573] The judiciary can accordingly monitor the executive's actions under this previously-controversial programme.[574] In the event that a service provider challenges the order, the FISC has the sole authority to hear that case.[575]

Executive Branch

The executive branch itself undertakes significant actions in the interest of compliance and transparency. Those actions take the form of procedures and controls to check surveillance and ensure compliance with the Constitution and federal statutes, independent oversight officers within the agencies, statutorily-mandated reports, and other voluntary disclosures.[576]

Internal Compliance Procedures And Controls

There are many procedures and controls mandated by statute or implemented voluntarily by the government. For example, the Wiretap Act, FISA Title I, and Section 702 all require high-level Department of Justice approval to apply for the relevant legal order.[577] The foreign-intelligence applications, in particular, must aver

---

[571] *See, e.g.*, Letter from Kevin J. O'Connor, Chief, Oversight Div., Nat'l Sec. Div., US Dep't of Justice, to Hon. Thomas F. Hogan, FISC, re: Update Regarding Compliance Incidents Reported in the December 2013, March 2014, and June 2014 Section 702 Quarterly Reports (July 30, 2014), http://www.dni.gov/files/documents/0928/Letter%20to%20Judge%20Hogan%2030%20July%202014.pdf; Letter from Kevin J. O'Connor, Chief, Oversight Div., Nat'l Sec. Div., US Dep't of Justice, to Hon. Reggie B. Walton, FISC, re: Notice of NSA's Assessment of Purge Practices and Discovery of Incomplete Purges (March 18, 2014), http://t.umblr.com/redirect?z=http%3A%2F%2Fwww.dni.gov%2Ffiles%2Fdocuments%2F0928%2FLetter+to+Judge+Walton+18+March+2014.pdf&t=OTkwMWE4MTU4YjQ5NDBiODVhZTU3YmI1NWYwMWU0MjUzYTNkODlmNyw5YWRlOTg3Qw%3D%3D; Savage, *Power Wars*, *supra* note 370, at 564, 572.

[572] Savage, *Power Wars*, *supra* note 370, at 572.

[573] 50 U.S.C. § 1861(c).

[574] *See, e.g.*, Kadzik Report, *supra* note 556, at 2 (noting that the FISC modified 141 of 178 applications for business records under 50 U.S.C. § 1862(c)(1)), http://fas.org/irp/agency/doj/fisa/2013rept.pdf.

[575] 50 U.S.C. § 1861(f).

[576] *See generally* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 657 (2016).

[577] *See, e.g.*, 18 U.S.C. § 2516(1) (Wiretap Act); 50 U.S.C. §§ 1804(a), (d) (FISA); 1881a(a) (Section 702).

that the government seeks "foreign intelligence"[578] and, for FISA Title I, that this intelligence cannot otherwise be obtained without the proposed surveillance.[579] These personal certifications ensure that the heads of the agencies are responsible for the conduct of American surveillance.

Next, the Department of Justice[580] and ODNI jointly assess compliance. Twice per year, the agencies release an unclassified report that details how, how often, and why noncompliance occurs.[581] In August 2013, that report revealed that the incidents of non-compliance were minimial and not systemic.[582]

Furthermore, the agencies have implemented various controls to ensure that the surveillance conducted remains in compliance with the Constitution and federal statutes after authorisation is obtained from the FISC. The NSA, for instance, has instituted significant controls surrounding the analysts' choice of selectors and audits on individual targeting decisions and minimization efforts.[583] These monitoring procedures have detected minor compliance issues, such as a failure to de-task all selectors and discriminants when a non-US person enters the United States,[584] but they have also detected a few systemic issues, such as a gap in the agency's procedures for purging irrelevant data[585] and inappropriate personal queries.[586] When issues have been detected, appropriate modifications have been made promptly.[587]

---

[578] FISA defines "foreign intelligence information" as "information that relates to … the ability of the United States to protect against actual or potential attack … of a foreign power …; sabotage, international terrorism, or the international proliferation of weapons of mass destruction …; or clandestine intelligence activities" or "information with respect to a foreign power or foreign territory that relates to … the national defense or security of the United States; or the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e).

[579] 50 U.S.C. § 1804(a)(7).

[580] The Department of Justice has a section of the National Security Division devoted to oversight of intelligence surveillance. US DOJ, *Sections & Offices* (September 9, 2015), http://www.justice.gov/nsd/sections-offices#oversight.

[581] US Dep't of Justice & ODNI, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence*, at 23–36 (August 2013), http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf

[582] *Id.* at 24.

[583] PCLOB, Section 702 Report, *supra* note 380, at 67–68; *see also supra* notes 495–503 and accompanying text.

[584] PCLOB, Section 702 Report, *supra* note 380, at 78.

[585] *Id.* at 79.

[586] *See Peterson*, *LOVEINT*, *supra* note 403.

[587] PCLOB, Section 702 Report, *supra* note 380, at 79.

Inspectors General

Congress has mandated that each agency within the executive branch has at least one inspector general. Inspectors general are independent, high-ranking appointees confirmed by the Senate for an indefinite term whose mission is to promote efficiency and ferret out fraud and abuse.[588] The Department of Justice Inspector General, for instance, is tasked with "detect[ing] and deter[ring] abuse, and misconduct in [Department of Justice] programs and personnel,"[589] and reporting to Congress semi-annually whether "Department programs and operations … are lawful, well-run, or otherwise in the public interest."[590]

Inspectors General routinely issue public reports when the government fails to meet those goals.[591] For example, a report by the Department of Justice Inspector General in 2007 identified excessive use by the FBI of "national security letters,"[592] and reports from the National Security Agency Inspector General have become available, detailing the number of phone and email accounts targeted by the NSA under a precursor to Section 702.[593] Inspectors General for the Department of Justice and Intelligence Community have access to classified information, so they are able to review sensitive law enforcement and intelligence surveillance programs, and report on these to Congress.

Civil Liberties Officers

Each agency also has a privacy and civil liberties officer, a senior official whose role in law enforcement and intelligence agencies includes to review, oversee, and audit day-to-day surveillance activities.[594] For example, the Department of Justice Chief Privacy and Civil Liberties Officer "review[s], overs[ees], and coordinat[es] the

---

[588] *See* 5 U.S.C. App. § 8H (requiring inspectors general for the Intelligence Community).

[589] US Dep't of Justice, *Inspector General Mission Statement*, (Jan. 2016), https://oig.justice.gov/; *see also* 5 U.S.C. app. 2.

[590] The Department of Justice Inspector General's Access to Information Protected by the Federal Wiretap Act, Rule 6(e) of the Federal Rules of Criminal Procedure, and Section 626 of the Fair Credit Reporting Act, at 5 (Op. O.L.C. July 20, 2015) (citing 28 C.F.R. § 0.29a(b)(2), (4)), *available at* http://www.justice.gov/sites/default/ files/olc/ opinions/attachments/2015/07/23/2015-07-20-doj-oig-access.pdf.

[591] *See, e.g.*, I. Charles McCullough, III, ODNI Inspector Gen., *Semiannual Report to the Director of National Intelligence: April 1–September 30, 2015* (Jan. 15, 2016); Letter from Dr. George Ellard, Inspector Gen., Nat'l Sec. Agency, to Sen. Charles E. Grassley (Sept. 11, 2013) (reporting "instances of intentional misuses of the signals intelligence authorities").

[592] US Dep't of Justice, Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (Mar. 2007), https://oig.justice.gov/special/s0703b/final.pdf.

[593] *See* Savage, *Power Wars*, supra note 370, at 211; *see also* NSA, Inspector General, *ST-09-0002 Working Draft* (Mar. 24, 2009), https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf.

[594] *See, e.g.*, 50 USC. § 403-3d(b)(1) (establishing position of Director of National Intelligence Civil Liberties Protection Officer); 42 USC. § 2000ee-1(a) (requiring privacy and civil liberties officers for the Central Intelligence Agency and National Security Agency).

Department's privacy operations" and "provides legal advice and guidance to Departmental components" to ensure that the government operates within its legal authority.[595] The ODNI Civil Liberties Protection Officer "ensur[es] that the protection of privacy and civil liberties is appropriately incorporated in Intelligence Community policies and procedures, oversee[s] compliance by the ODNI with privacy and civil liberties laws, review[s] complaints of possible abuses of privacy and civil liberties in programs and operations administered by the ODNI, and ensur[es] that the use of technology sustains, and does not erode, privacy.[596] As with the inspectors general, these officers release public reports evaluating the government's progress in melding a need for effective surveillance and for protecting privacy.[597]

Review Boards

The President's Foreign Intelligence Advisory Board and Intelligence Oversight Board, an element within the Executive Office of the President, have a standing obligation to "overse[e] the Intelligence Community's compliance with the Constitution and all applicable laws."[598]

Recently, President Obama also established the President's Review Group on Intelligence and Communications Technology after the Snowden disclosures.[599] This group reviewed United States surveillance policies and activities, and it then issued a public report with recommendations.[600] Many of those recommendations were subsequently included in PPD-28 or the USA FREEDOM Act of 2015.[601]

---

[595] US Dep't of Justice, *Office of Privacy & Civil Liberties*, http://www.justice.gov/opcl; *see also* 28 U.S.C. § 509 (note) (establishing Privacy and Civil Liberties Office).

[596] ODNI, *Civil Liberties Protection Officer*, http://www.dni.gov/index.php/about/leadership/civil-liberties-protection-officer.

[597] *See, e.g.*, NSA Civil Liberties & Privacy Office, *USA FREEDOM Transparency Report*, *supra* note 384; NSA Civil Liberties & Privacy Office, *Transparency Report: NSA's Implementation of FISA Section 702* (Apr. 16, 2014), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

[598] President's Intelligence Advisory Board & Intelligence Oversight Board, https://www.whitehouse.gov/administration/eop/piab/.

[599] President's Review Group on Intelligence and Communications Technology, *Liberty and Security in a Changing World*, *supra* note 428.

[600] It bears noting that, even though the review group recommended several changes to current United States policy, "nothing in [this report] indicated that [the United States] intelligence community ha[d] sought to violate the law or [wa]s cavalier about the civil liberties of their fellow citizens." Pres. Barack H. Obama, Remarks on Review of Signals Intelligence (Jan. 17, 2014).

[601] Peter Swire, *The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years* (Jan. 8, 2015), *https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years* (explaining adoption of Group's recommendations).

Public Reports And Disclosures

As noted before, FOIA exists to permit the press and private parties to obtain any unclassified documents from the government.[602]

The Director of National Intelligence, however, also publishes all declassified procedures, guidelines, speeches, and FISA opinions on the internet,[603] and the Office of Legal Counsel of the Department of Justice makes many of its opinions available for public consumption.[604]

The various agencies, moreover, have public reporting requirements. The Department of Justice must file a report with the Administrative Office of the United States Courts, which provides a general description of the intercepted communications, the number of arrests made pursuant to the information, and the number of convictions secured.[605] These reports are then released to the public for review.[606] Likewise, the Intelligence Community must submit yearly reports to the Administrative Office of the United States Courts and to Congress.[607] These reports must detail the number of applications approved by the Attorney General and the number of FISA orders granted or extended by the FISC.[608]

More specifically, law-enforcement agencies must notify the target of a wiretap application in short order after the Title III warrant expires or is denied.[609] Likewise, and, as noted earlier, law enforcement and the Intelligence Community must

---

[602] *See, e.g.*, *New York Times Co. v. U.S. Dep't of Justice*, No. 14-4432-cv (2d Cir. Oct. 22, 2015) (affirming district court order requiring disclosure of OLC opinions related to drone program), *available at* http://www.ca2.uscourts.gov/decisions/isysquery/27a87bdf-b5fd-4cb7-98f6-5bfe606ef80a/1/doc/14-4432_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/27a87bdf-b5fd-4cb7-98f6-5bfe606ef80a/1/hilite/.

[603] *See, e.g.*, ODNI, *IC On the Record*, http://icontherecord.tumblr.com/topics/section-702; *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 14-01 (FISC Mar. 20, 2014), *available at* http://apps.washingtonpost.com/g/documents/national/opinion-and-order-in-case/955/.

[604] *See* US Dep't of Justice, Office of Legal Counsel, http://www.justice.gov/olc/opinions; *see also* David J. Barron, Acting Asst. Att'y Gen., Off. of Legal Counsel, Dep't of Justice, Mem. re: Best Practices for OLC Legal Advice and Written Opinions 5 (July 16, 2010) (noting that "the Office operates from the presumption that it should make its significant opinions fully and promptly available to the public"), http://www.justice.gov/sites/default/files/pages/attachments/2014/07/11/olc-best-practices-2010.pdf.

[605] 18 U.S.C. § 2519(2).

[606] *See, e.g.*, US Dep't of Justice, *Wiretap Report 2014*, *supra* note 351.

[607] *See, e.g.*, Pub. L. No. 114–23, § 108; 50 U.S.C. §§ 1807; 1881a(l)(1); *see also* Off. of Dir. of Nat'l Intelligence, *Signals Intelligence Reform: 2015 Anniversary Report*, http://icontherecord.tumblr.com/ppd-28/2015.

[608] 50 U.S.C. § 1807(a).

[609] 18 U.S.C. § 2518(8)(d); *see also id.* §2703(d) (permitting delayed notification of access to stored communications).

disclose if surveillance was used to obtain evidence the government intends to introduce in a criminal proceeding.[610]

The end result is that these bodies provide oversight of the government's Wiretap Act activities, and the public remains informed of law enforcement's activities. If abuses are discovered, reforms can thus be instituted quickly and with dispatch.

Congress

Congress itself plays a significant role monitoring law enforcement's and the Intelligence Community's surveillance activities. As a non-parliamentary system, the US Congress is wholly independent of the executive branch and judiciary. Significantly, however, the legislature holds the power of the purse, meaning it can refuse to appropriate money to federal law enforcement or the Intelligence Community in response to unapproved surveillance.[611] The Judiciary and Intelligence Committees in both the House and Senate have jurisdiction over the Department of Justice and the Intelligence Community, and they frequently conduct hearings regarding surveillance.[612] They have secure facilities in which to receive classified briefings and large staffs with the necessary clearances to properly conduct intense and granular oversight proceedings. From these hearings, abuses can be identified and corrected, as they were with the original passage of the Wiretap Act and FISA and, more recently, the USA FREEDOM Act.

Independent Watchdogs

Independent oversight bodies provide a mechanism to ensure that law enforcement and intelligence surveillance comply with public law that, like the judiciary, is independent both of the prosecutorial or intelligence functions and of political decision-making.[613] The activity of such bodies can be supplemented by civil society.

---

[610] *Id.* § 2515; 50 U.S.C. § 1806(c)–(d).

[611] US Const. art. I, § 8, cl. 12.

[612] *See, e.g.*, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (July 8, 2015); Report of the Select Comm. on Intell., Covering the Period Jan. 3, 2013 to Jan. 5, 2015 (Mar. 31, 2015), http://www.intelligence.senate.gov/publications/report-select-committee-intelligence-covering-period-january-3-2013-january-5-2015; Comm. Study of the Central Intelligence Agency's Detention and Interrogation Program (Dec. 9, 2014); *Oversight of the U.S. Department of Justice: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (Jan. 29, 2014); *Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs: Hearing of the S. Judiciary Comm.*, 113th Cong. (July 31, 2013); *Video Laptop Surveillance: Does Title III Need to Be Updated: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (Mar. 29, 2010).

[613] *Cf.* ECtHR 4 December 2015, Application No. 4743/06, *Zakharov v. Russia*, ECLI:CE:ECHR:2015:1204JUD004714306, §§ 275 and 279 (approving of oversight bodies composed of legislators and members of the judiciary, but noting that political appointees and prosecutors charged with overseeing surveillance activities were not sufficiently independent).

Privacy And Civil Liberties Oversight Board

The foremost independent oversight body (within the Executive Branch) is the Privacy and Civil Liberties Oversight Board (PCLOB), a board of five experts with members from both parties nominated by the President and confirmed by the Senate. Mandated by statute following the attacks of 9/11,[614] the PCLOB has two main responsibilities:

> (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.[615]

The PCLOB, pursuant to this directive, has access to classified information and may elicit testimony and documents from the government.[616] The PCLOB is ultimately permitted to issue public reports, describing any abuses and offering recommendations for improvements.[617]

Two of these reports have particular significance for assessing the level of protection for personal data of EU citizens that is transmitted to the US. The first is the PCLOB's report on the government's metadata programme under Section 215.[618] The PCLOB found that the government's programme of bulk-collection domestic telephone metadata violated Section 215 itself as well as ECPA, and that it raised significant questions under both the First and Fourth Amendments to the US Constitution.[619] The report, moreover, found that "the Section 215 program has shown minimal value in safeguarding the nation from terrorism"[620] – in effect, that the programme was disproportionate. The report consequently recommended that "the government end the program"[621] and that Congress enact additional safeguards.[622]

---

[614] 42 U.S.C. § 2000ee; *see also supra* note 1.

[615] 42 U.S.C. § 2000ee(c).

[616] *See* 42 U.S.C. § 2000ee(d), (g).

[617] *See, e.g.*, 42 U.S.C. § 2000ee(e); PCLOB, Section 702 Report, *supra* note 380; PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance* (Jan. 23, 2014) (Section 215 Report), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[618] PCLOB, Section 215 Report *supra* note 617.

[619] *Id.* at 10–11.

[620] *Id.* at 11.

[621] *Id.* at 16.

[622] *Id.* at 17.

Those safeguards largely became the basis for the USA Freedom Act, which has become law.[623]

The second significant report is the PCLOB's report on the Section 702 programme, or "PRISM" programme.[624] This report found that "the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead the program consists entirely of targeting specific [non-United States] persons about whom an individualized determination has been made."[625] The PCLOB also noted that "[t]he Section 702 program has proven valuable to the government's efforts to combat terrorism," including by helping the Intelligence Community "understand the structure and hierarchy of internationals terrorist networks," "identify previously unknown individuals who are involved in international terrorism," and "discovering … connection[s] between [foreign] extremist[s] and [previously] unknown person[s] [in the United States]."[626] As a result, the PCLOB found, there have been at least "54 'success stories'" in which the Section 702 programme has played a role, and approximately 30 cases in which "Section 702 information was the initial catalyst that identified previously unknown terrorist operatives and/or plots."[627]

These reports – one critical of the proportionality of surveillance programs, one supportive – provide the public with the necessary insight into government surveillance programs. The thoroughness and candour of the PCLOB's reports demonstrate the independence of the board and effectiveness of its oversight.

Service Providers

The government permits telecommunications and internet-service providers to disclose "transparency reports," aggregate reports regarding government requests for information under Section 702.[628] These reports, for instance, show in six-month periods the number of data requests made by the government and the number of users affected.[629] Certain restrictions, however, apply: a company must wait two years to report "data relating to the first order that is served on [it] for a platform,

---

[623] Pub. L. No. 114–23, § 103 (amending 50 U.S.C. § 1861(b)(2), (c)).

[624] PCLOB, Section 702 Report, *supra* note 380.

[625] *Id.* at 111. *Cf.* Surveillance by intelligence services: fundamental rights safeguards and surveillance and remedies in the EU: http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services November 2015.

[626] *Id.* at 107–08.

[627] *Id.* at 109–10.

[628] *See, e.g.*, Letter from James M. Cole, Dep. Att'y Gen., to Colin Stretch et al. (Jan. 27, 2014), available at http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf; Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, 28 (Dec. 17, 2015), https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

[629] *See, e.g.*, Google, *Transparency Report*, https://www.google.com/transparencyreport/userdatarequests/; Facebook, *Government Requests Report*, https://govtrequests.facebook.com/country/United%20States/2015-H1/.

product, or service (whether developed or acquired) for which the company has not previously received such an order."[630]

Other Watchdog Groups

In addition, a robust civil society brings ad hoc oversight using various transparency statutes that permit individual citizens to petition the government for documents and other information. The Freedom of Information Act,[631] for example, creates a presumption that government information must be disclosed at the request of a private citizen or organisation. This statute provides a significant mechanism for obtaining information in the government's possession, such as government surveillance manuals, and is available to European citizens.[632]

Various outside groups have vigorously pursued FOIA requests and other transparency measures, which increase the public knowledge of the government's surveillance and disclosure policies and actions.

Civil litigation also presents opportunities to acquire previously unreleased information. Civil litigants have disclosure and discovery obligations[633] from which the government is not excused.[634] The public, as a result, can obtained access to pertinent documents regarding government surveillance.

The end result is that these bodies provide thorough oversight of the government's surveillance activities, and the public remains informed. If abuses are discovered, reforms can thus be instituted quickly and with dispatch.

---

[630] Letter from James M. Cole *supra* note 628, at 3.

[631] 5 U.S.C. § 552.

[632] *See, e.g.*, H. Marshall Jarrett, US Dep't of Justice, *Searching & Seizing Computers & Obtaining Electronic Evidence in Criminal Investigations* (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ssmanual2009.pdf.

[633] Fed. R. Civ. P. 26.

[634] *See, e.g.*, *Human Rights Watch v. Drug Enforcement Agency*, No. CV 15-2573 PSG (JPRx) (Aug. 14, 2015), *https://www.eff.org/document/order-holding-abeyance-ruling-motion-dismiss-and-granting-part-plaintiffs-request-discovery* (granting discovery regarding DEA surveillance program); *Campbell v. Eastland*, 307 F.2d 478, 485 (5th Cir. 1962) ("In a mine-run civil case the discovery provisions of the Federal Rules of Civil Procedure apply to claims against the government."); *cf. United States v. Nixon*, 418 U.S. 683 (1974) (establishing that high-government officials are not immune to legal process).

2.2.5 Legal Remedies And Redress

> *The public should be informed about surveillance laws and have some opportunity for access and rectification, and for judicial redress. If necessary for legitimate aims of surveillance, surveillance can be secret, in which event oversight or more general legal redress are necessary.*

Remedies and means of redress exist at law for individuals subject to illegal surveillance. They come largely in two forms: the right to exclude the collected information from the government's evidence in a criminal trial, and civil causes of action that allow for damages or injunctive relief. Both are generally open to US and EU citizens.

Exclusionary Rule

The Fourth Amendment usually precludes the government from introducing evidence obtained through unauthorised electronic surveillance or evidence derived from such illegal means.[635] This means that if the government fails to follow these strictures, any information or evidence obtained cannot be used to prosecute the individual. Under this doctrine, it matters not that "the surveillance was limited, both in scope and in duration, to [a] specific purpose" if the government's reasons for warrantless surveillance were not reasonable,[636] because the Constitution recognizes that "[t]he greatest dangers to liberty lurk in insidious encroachment by men [and women] of zeal, well-meaning but without understanding."[637] This mechanism protects the individual, but it also serves as a powerful deterrent to law enforcement by removing the main purpose for law enforcement collecting information – obtaining evidence on which to produce criminal convictions.

The Wiretap Act, ECPA, and FISA have codified this rule.[638] These statutes, in addition, require that targets of surveillance be informed that the government has collected their information and plans to use it against them in any adverse proceeding.[639] For instance, FISA demands that, if information is used for adverse purposes, the government must "notify the aggrieved person and the court … that the Government intends to so disclose or so use such information."[640] The

---

[635] *See, e.g.*, *Mapp v. Ohio*, 367 U.S. 643, 657 (1961).

[636] *Katz v. United States*, 389 U.S. at 354.

[637] *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting). The Supreme Court in *Mapp* largely adopted Justice Brandeis's dissent as the majority's position. 367 U.S. at 659 ("'Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. * * * If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy.'" (quoting *Olmstead*, 277 U.S. at 485 (Brandeis, J., dissenting)).

[638] 18 U.S.C. § 2515; 50 U.S.C. § 1806(e).

[639] *See* 18 U.S.C. § 2518(8).

[640] 50 U.S.C. § 1806(c).

aggrieved person then must be provided an opportunity to "move to suppress the evidence obtained or derived from [the government's] electronic surveillance."[641] As with the application of the exclusionary rule with respect to wiretaps,[642] section 1806(e) thus ensures that the government does not benefit from illegal surveillance and deters the deployment of further surveillance without appropriate approval.

Civil Causes Of Action

The surveillance statutes also provide civil causes of action that allow harmed individuals to sue for damages or, in certain instances, equitable relief. These apply against the individual officers, as well as the United States government.

The Wiretap Act creates a private cause of action against individual officers for "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the Act[643] and allows a court to order "appropriate relief," including "such preliminary and other equitable or declaratory relief as may be appropriate; damages … and punitive damages in appropriate cases; and a reasonable attorney's fee and other litigation costs reasonably incurred."[644] This right applies to foreign citizens as well as United States persons.[645]

ECPA similarly allows the target of surveillance conducted in willful violation of the statute to sued under for civil damages.[646] Relief against individuals can include money damages (no less than $1,000 per action), equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs.[647] Willful or intentional violations can also result in punitive damages, and employees of the United States may be subject to disciplinary action.[648]

Where US agents and officers willfully fail to comply with Title III provisions, ECPA authorizes suits against the United States under 18 U.S.C. § 2712. This section authorizes courts to award actual damages or $10,000, whichever is greater, and

---

[641] *Id.* § 1806(e).

[642] 18 U.S.C. § 2518(9)–(10).

[643] *Id.* § 2520(a).

[644] *Id.* § 2520(a), (b).

[645] *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 731 (9th Cir. 2011); *see also* PCLOB, Section 702 Report, *supra* note 380, at 99 n.444 (citing *Suzlon* for proposition that "any person" includes "non-U.S. persons").

[646] *See, e.g., Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121 (D. Conn. 2004) (granting summary judgment on liability under ECPA against police officers who served on AOL a purported search warrant that had not been signed by a judge). Government employees are subject to this provision, but United States itself is subject to liability under a separate provision. 18 U.S.C. § 2707(a).

[647] 18 U.S.C.§§ 2707(b), 2710(c)(2)(D), 2712(c).

[648] *See id.* § 2707(c), (d). Good faith reliance on a court order or warrant, grand jury subpoena, legislative authorisation, or statutory authorisation provides a complete defence to any civil or criminal action brought under ECPA. See *id.* § 2707(e). Qualified immunity may also be available.

reasonable litigation costs. Section 2712 also defines procedures for suits against the United States and a process for staying proceedings when civil litigation would interfere with a related investigation or criminal prosecution.[649]

Violations of ECPA may also give rise to a cause of action against the United States, and may result in disciplinary action against offending officials or employees.[650] As a result, suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of ECPA.[651] This section authorizes courts to award actual damages or $10,000, whichever is greater, and reasonable litigation costs. Section 2712 also defines procedures for suits against the United States and a process for staying proceedings when civil litigation would adversely affect a related investigation or criminal prosecution.[652]

Under FISA, "[a]ny aggrieved person" – including a European citizen (not an agent of a foreign power) – likewise has "a cause of action against any person" who conducted surveillance without statutory or Presidential authorisation or who misused or disclosed such information.[653] If successful, that person may obtain actual, statutory, or punitive damages and reasonable attorney's fees and litigation costs.[654]

2.3 The Authority And Limitations For Surveillance Under US Law Fall Well Within The Range Of Discretion Accorded To EU Member States

2.3.1 Introduction

This section compares current US laws and practices regarding government surveillance, as delineated in the preceding section, against the EU Benchmark. As noted above, Member States have considerable latitude in choosing the type of surveillance they consider appropriate.[655] Even though this latitude may be reduced when a strong consensus exists among Member States concerning the legality of specific practices, the breadth of government discretion under the EU Benchmark remains significant, as described in Parts 2.3.2.1 and 2.3.2.2 below.

This comparison uses the same four general criteria deployed above to survey the surveillance laws of the Illustrative Members States and of the US (specific legal

[649] *See id.* § 2712(b), (e).

[650] *Id.* § 2712.

[651] This section also applies to the Title III Wiretap Act, and specified sections of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c.

[652] *See* 18 U.S.C. § 2712 (b), (e).

[653] 50 U.S.C. § 1810.

[654] 50 U.S.C. § 1810.

[655] *See supra* Part 1.3.3. This is confirmed most recently in ECtHR (Grand Chamber) 4 December 2015, Application No. 47143/06, *Roman Zakharov v. Russia*, § 232; and in ECtHR 12 January 2016, Application No. 37138/14, *Szabó and Vissy v. Hungary*, § 57. Of course, each type of surveillance will require safeguards appropriate to prevent abuse of that type of surveillance.

authority, limited scope, appropriate oversight, and legal remedies and redress), which reflect the ECtHR guidance on ensuring proportionality discussed at length in Part 1.3.3 above. These criteria help establish the EU Benchmark against which to compare the US legal order for surveillance.

Any thorough comparison must establish facts fully and fairly. No adequacy decision can be based on allegations or rumours in press reports, such as Washington Post articles reporting on the Snowden revelations that were later retracted and corrected by the Post itself.[656] Nor can such a decision be based on allegations that have otherwise been proven to be inaccurate or unsubstantiated. For example, the PRISM programme was characterized as "mass and undifferentiated access" in the referral judgment of the High Court of Ireland,[657] and was assumed to be so by the Advocate-General.[658] Such allegations not only are inaccurate under binding US law, but also have been recognised as such by the FRA Report. That report, in fact, explains that the PRISM programme applies individualised search terms according to court-approved targeting procedures and, thus, is "targeted"surveillance – not "mass and undifferentiated."[659]

All previous European reports suffer from similar misconceptions or fail to account for recent changes in the US legal order. Since the start of the *Schrems* case in Ireland on 25 June 2013, there have been two independent reviews of surveillance activities, at least seven legislative actions, and 13 executive branch actions in the US,[660] many of which were not addressed in the European Parliament Resolution of 12 March 2014, or the LIBE Committee Report of 13 October 2015. Notable changes include the USA FREEDOM Act, which ended the telephone metadata bulk-collection programme previously conducted pursuant to Section 215 of the USA PATRIOT Act[661]; and the NSA's *Transparency Report: USA Freedom Act Business Record FISA Implementation* published on 16 January 2016, which clarifies that the

---

[656] *See* Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 11; European Union Agency for Fundamental Rights, FRA Report, *supra* note 127, at 17. The original erroneous article nevertheless was quoted in the referring judgment of the High Court of Ireland of 18 June 2014 in the *Schrems* case. See Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013, supra note 398*, at 14–15 & n.41; Robertson, *Opinion*, *supra* note 398, at para. 8 (noting that the CJEU "struck down [Safe Harbour] on the basis of an unexamined allegation by Edward Snowden that NSA had established PRISM in 2009 to obtain unrestricted access 'on a casual and generalised basis' to mass data stored on US servers" and that "[t]his is not factually correct, although it reflects many media misinterpretations of PRISM").

[657] *Schrems v. Data Protection Commissioner*, [2014] IEHC 310, § 52.

[658] Opinion of A-G Bot of 23 September 2015, Case C-362/14, ECLI:EU:C:2015:627, § 26. The CJEU also referred the "mass and undifferentiated accessing of personal data," *Schrems*, § 33, but in the context of describing the Irish High Court judgment.

[659] FRA Report, *supra* note 127, at 17.

[660] *See* Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013, supra* note 398*,* at 23–43.

[661] Pub. L. No. 114–23, § 103, 129 Stat. 268 (2015) (amending 50 U.S.C. § 1861). *See also supra* Part 2.2.1.

data previously gathered under that programme will "never be accessed."[662] Therefore, neither the Commission nor any supervising authority can refer uncritically to any of the reports published to date, as all are based in part on outdated and often incorrectly stated or merely presumed facts, and omit essential parts of the legal order in the US.

The overview of US surveillance in this report reflects the US legal order as it exists today and, thus, may serve as a cornerstone of the current, correct, complete, and substantiated backdrop from which an essentially equivalent comparison must be conducted. It is neither correct nor reasonable to base any decision concerning the level of data protection going forward on anything less.

The surveillance regimes in the Illustrative Member States and the US all structure laws and safeguards for surveillance by law enforcement agencies differently from that by intelligence services. This comparison therefore follows this differentiation, looking separately at the degree of consensus among the Illustrative Member States for each category, and then comparing US safeguards against the range of consensus and the variations among the Illustrative Member States. In the intelligence category, the analysis focuses in particular on untargeted surveillance, because it is this type of surveillance that has been the greatest cause of criticism of the US and the source of unsubstantiated allegations regarding the PRISM programme that were a concern in the *Schrems* case.

On the basis of these facts, as detailed further below, this report concludes that the level of data protection under the US legal order for surveillance as it exists today is essentially equivalent to the EU Benchmark, both with regard to law enforcement surveillance and to intelligence surveillance.

2.3.2 Measuring The US Legal Order Surveillance Against The EU Benchmark

2.3.2.1 Targeted Law Enforcement Surveillance: Broad Consensus Allowing Strong Surveillance Among Illustrative Member States, Condoned By ECtHR

The overview of EU surveillance laws shows broad consensus among the Illustrative Member States regarding law enforcement surveillance against targeted individuals. All Illustrative Member States employ secret law enforcement surveillance against individuals suspected of crimes of a certain degree of seriousness. The enumerations of such crimes vary widely among the Illustrative Member States and often are limited to general descriptions. For example, in France, certain forms of surveillance can be ordered for crimes and misdemeanours punishable by at least two years in prison.[663] In the UK, other than to justify the interception of communications or intrusive surveillance, there is no requirement for the crime even

[662] NSA Civil Liberties & Privacy Office, *Transparency Report: The USA FREEDOM Act Business Records FISA Implementation*, *supra* note 384, at 7.

[663] Criminal Procedure Code, Article 100.

to be "serious."[664] Thus, there is no specific consensus among Member States as to the types of crimes that can justify secret surveillance.

All but one of the Illustrative Member States require that a warrant for surveillance be issued by a judge, and all allow exceptions for emergencies or other special circumstances. The UK, the single outlier, permits a warrant to be issued by the Secretary of State.

In the Illustrative Member States, data subjects will not be informed of the surveillance when it is undertaken. The data subjects, however, will be informed before they are prosecuted, and they may defend themselves in standard criminal law proceedings. For example, in Germany, investigating authorities must inform certain individuals targeted by a surveillance measure as soon as such notification does not endanger the purpose of the investigation; the life, physical integrity, and personal liberty of another person; or significant assets.[665] This consensus among the Illustrative Member States is supported by case law from the ECtHR condoning secret surveillance for law enforcement purposes, provided the crimes are sufficiently serious to warrant its use and appropriate safeguards against abuse are in place.[666]

2.3.2.2 Intelligence Surveillance: Illustrative Member States Engage In Targeted And Non-Targeted Surveillance; Both Are Condoned by the ECtHR

Surveillance Of Targeted Individuals

All of the Illustrative Member States permit secret surveillance of targeted individuals for the purposes of protecting national security or state security and a number of the other purposes enumerated in Article 8 ECHR: "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Purposes specified by Illustrative Member States are broad enough to include, for example: "the scientific and economic potential of the State" (Belgium); "major economic, industrial, and scientific interests" (France); "the State's economic interests" (Poland); and "the economic well-being of the country" (UK).

In Poland, the Constitutional Tribunal found the term "the State's economic interests" to be insufficiently specific.[667] However, this solitary judgment does not establish any "broad consensus" that generally descriptive terms are insufficient to denote the purpose for which secret surveillance may be ordered. To the contrary, in *Szabó &*

[664] RIPA, §§ 22(2), 28 & 49.

[665] Code of Criminal Procedure, §§ 101(4) & (5).

[666] *Weber & Saravia*, § 4.

[667] Decision of the Polish Constitutional Tribunal, 30 July 2014, Case K23/11.

Vissy v. Hungary, the ECtHR noted that the term "terrorist threat" is sufficiently precise and permits sufficient "foreseeability" for citizens.[668]

With regard to the process of authorising surveillance against targeted individuals, in the majority of the Illustrative Member States, the warrants or authorisations are not granted by a court, but by a variety of non-judicial bodies, often a minister or other officer in the executive branch of government. For example, in France the implementation of surveillance measures by the intelligence services are subject to the prior authorisation of the Prime Minister and, in the UK, by the Secretary of State. Thus, there is no consensus among Illustrative Member States that such authorisations should be issued by a court. There is also no consensus among Illustrative Member States regarding the degree of suspicion required to authorise surveillance. Only two of the Illustrative Member States – Belgium and the Netherlands – specifically require a demonstration that there is no alternative, less intrusive method to obtain the information.

Surveillance Not Targeted At Specific Individuals

Five of the Illustrative Member States (France, Germany, Poland, the Netherlands, and the UK) carry out signals intelligence that is not targeted at specific individuals suspected of committing or preparing crimes or threatening national security. They generally do so by means of applying search terms (also referred to as "discriminants") for the purpose of filtering information from large data flows. In these Member States (other than Poland), the intelligence agencies have the technical ability to access data flows such as telephone or internet backbone cables directly, but they are permitted to use this access solely for the purpose of applying the search terms. In most cases, this is done using metadata without, in the first stage, accessing the content of the communications. However, in Germany the statutory restrictions in respect of the use of keywords for strategic telecommunications surveillance do not apply to telecommunications outside Germany – including in other EU Member States – provided such communications do not involve German nationals.

For the remaining Illustrative Member States, their laws do not explicitly authorise untargeted surveillance. Whether they nonetheless engage in similar signals intelligence, as the FRA Report has suggested some States do[669] – is currently unknown. In any event, it is not possible to state that there is a specific consensus among EU Member States regarding such signals intelligence.

Indeed, the number of countries engaged in signals surveillance is high enough that it is not possible to characterise any Member State engaging in untargeted signals

[668] *Szabó & Vissy*, § 64.

[669] *Supra* note 127, at 17; *see also id.* ("In 2015, the Council of Europe Commissioner for Human Rights stated that "in many Council of Europe member 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.")

intelligence of large data flows using search terms as an "outlier."[670] The ECtHR has repeatedly held that non-targeted signals intelligence does not infringe Article 8 ECHR, if accompanied by sufficient safeguards.[671]

As noted in the FRA Report and in Section 2.1, the Illustrative Member States have widely diverging systems of authorisation, oversight, and legal redress regarding secret intelligence surveillance. In Germany, for example, the PkGr is responsible for approving important aspects of the strategic telecommunications surveillance undertaken by the intelligence services. In the Netherlands, however, implementation of untargeted surveillance is permitted via the use of keywords without prior authorisation of the relevant minister. The diversity among Member States on all these points is broad, and the review of Illustrative Member State laws reveals little consensus on the precise measures that must be taken beyond the "minimum safeguards" noted in the ECtHR case law.

By contrast, there is broad consensus among the Illustrative Member States on one issue: direct legal redress by data subjects is available only to the extent information about the surveillance is communicated to the data subject, and this is often impossible without endangering the purpose for which the surveillance is justified. In some cases there are indirect processes like those in France, whereby at the request of the CNCTR the Council of State verifies whether surveillance measures have been implemented lawfully.

2.3.2.3 Law Enforcement Surveillance: The US Meets The "Essentially Equivalent" Test

With regard to secret surveillance for law-enforcement purposes, little or no criticism has been raised against the US criminal justice system. As shown in Section 2.2 above, there is a multitude of guarantees against abuse built into the US system, and comparison with the Illustrative Member States shows no doubt that the US system provides a level of protection that meets the EU Benchmark.

Specific Legal Authority

The US laws permitting secret surveillance for law enforcement purposes – the Wiretap Act and ECPA – contain clear obligations requiring law enforcement to demonstrate to a neutral magistrate that "probable cause" exists to believe the content of particular communications are relevant to a crime.[672] Furthermore, to intercept such communications in real-time, the crime being investigated must be among an enumerated list of serious felonies, such as espionage, kidnapping, murder, bribery, human trafficking and forced labour.[673] To access non-content

[670] For a decision finding an outlier, see *S. & Marper v. UK*, § 110, where the ECtHR noted that "England, Wales and Northern Ireland appear to be the only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material".

[671] The main case is *Weber & Saravia*, § 137.

[672] 18 U.S.C. §§ 2518(c), 2703(a).

[673] *See id.* §§ 2516, 2518.

information, or metadata, without notice to the data subject, law enforcement must show "reasonable suspicion" exists to believe the data is related to a crime.[674] There can be little doubt as to the clarity and quality of these two laws, and hundreds of court cases have shaped and further clarified their wording. Nor can there be doubt about the "foreseeability" of these laws: the list of crimes for which interception can be deployed is clearly spelled out, and the standards by which lesser forms of intrusion are precisely defined and publicly available.

The types of crimes for which secret law enforcement surveillance may be requested are at least as precise in the US as in the Illustrative Member States, and standards and methods for authorising all surveillance are at least as clearly established.

Limited Scope

US law establishes multiple safeguards to limit the scope of the data collected, used, and retained by US law enforcement authorities. For example, the factual basis for a warrant request must spell out "with particularity" the offence and the communications targeted, and this basis must establish the requisite "probable cause."[675] This requirement appears at least as strict as the corresponding tests set out in the Illustrative Member States, *e.g.*, "serious indication" (Belgium); "justifiable" (France); "initial suspicion" (Germany); "reasonable grounds for believing" (Ireland); "serious suspicion" (Netherlands); and "serious suspicion" combined with a justification requirement (Italy). Notably, there is no explicit threshold for suspicion in Poland and the UK.

In the US, a request for a wiretap warrant must also explain that other, less intrusive investigative procedures have failed or are unlikely to succeed.[676] A specific requirement to that effect has been included in the laws only of Belgium and the Netherlands, and in France, Germany, Poland, and the UK, a more general proportionality test may be applied. On this point, the US legal order appears to contain requirements at least as stringent as those in the Illustrative Member States.

Communications intercepted by US law enforcement are presented to a court and kept under seal for a period of ten years.[677] All of the Illustrative Member States generally provide similar retention limits and data-security standards. For example, in the UK, intercepted material and any related communications data must be destroyed as soon as there are no longer grounds for retaining it for an authorised purpose.[678]

US laws provide that surveillance information cannot be used against an individual in criminal proceedings without disclosure, and the defendant can move to suppress

---

[674] *See id.* § 2703(d).

[675] *See id.* § 2703(a); Fed. R. Crim. P. 41.

[676] *Id.* § 2518(1)(c).

[677] *Id.* § 2518(8)(a).

[678] RIPA, § 15(3).

the contents of any data obtained through improper surveillance.[679] On these points, the Illustrative Member States do not have laws that are stricter than those in the US.

Oversight

There is strong *ex ante* oversight by an independent judiciary in the US. Judges must find "probable cause" before any warrant is issued,[680] and the criminal justice system provides ample opportunity to challenge any evidence based on secret surveillance that is introduced against a defendant.[681] For the Wiretap Act, high-level Department of Justice approval is needed,[682] and the Act further requires that judicial supervision continue for every federal or state wiretap warrant and that each warrant be reported to the Administrative Office of the US Courts, which submits its findings to Congress in a public report.[683] Congressional committees regularly conduct hearings regarding surveillance.[684] The Freedom of Information Act (FOIA) permits the press and private parties to obtain any unclassified documents from the government, and is frequently used by watchdog groups.[685]

In the majority of Illustrative Member States, *ex ante* oversight is judicial. However, in Poland, prior authorisation for surveillance is granted by the Attorney General, and in the UK, a warrant for the interception of communications is granted by the Secretary of State. Both are members of the executive branch. The level of post-implementation review is different in each of the Illustrative Member States. Overall, the level of oversight in Illustrative Member States for law enforcement surveillance does not exceed the level of protection in the US.

Legal Remedies And Redress

The main protection against unlawful or abusive surveillance built into the US criminal justice system is the "exclusionary rule" that prevents individuals from being prosecuted on the basis of evidence that has not been legally obtained.[686] This rule applies fully to evidence obtained through surveillance.[687] Similar rules apply in the Illustrative Member States.

---

[679] 18 U.S.C. § 2515.

[680] *Id.* § 2518(3).

[681] *Id.* § 2515; *see also Mapp*, 367 U.S. at 354.

[682] 18 U.S.C. §2518(7).

[683] *Id.* § 2519.

[684] *See supra* note 353 (collecting representative hearings).

[685] *See* 5 U.S.C. § 552.

[686] *See, e.g.*, *Mapp*, 367 U.S. at 354.

[687] *See, e.g.*, *Katz v. United States*, 389 U.S. at 354 (excluding evidence obtained via unlawful wiretap).

The US justice system also permits civil causes of action that allow harmed individuals to sue for damages and equitable relief, including statutory damages (a remedy that permits a plaintiff to obtain an amount higher than the actual damages suffered).[688] In the EU, civil actions generally occur to a lesser extent than in the US, and the concept of "statutory damages" is not known.

Conclusion

There can be no doubt that the protection of data subjects with regard to secret surveillance by law enforcement agencies in the US is at least "essentially equivalent" to the protection available in the EU legal order. As a result, it is difficult to understand why the ECtHR, faced with such a system of safeguards, would consider that the laws of the US law enforcement system go beyond what is "necessary in a democratic society".

2.3.2.4 Intelligence Surveillance: The US Legal Order Passes the "Essentially" Equivalent Test

The US laws described in detail in Section 2.2 establish a broad set of safeguards that work together to prevent abuses and ensure that intelligence is conducted for the specific purposes provided in those laws. These safeguards apply quite specifically to surveillance in the US that could affect data of EU citizens transmitted to the US, and therefore operate to prevent abuse. Taken as a whole, these laws and safeguards meet the EU Benchmark.

Specific Legal Authority

The key US statute that authorises targeted surveillance that may affect EU citizens is the Foreign Intelligence Surveillance Act of 1978 (FISA). Section 702 of that statute also provides legal basis for the PRISM and Upstream programmes focused upon in *Schrems*. Additionally, Section 215 of the USA PATRIOT Act – as modified by the USA FREEDOM Act in 2015 – authorises a targeted telephone metadata collection programme.

Purposes Of Surveillance Defined

FISA, in all of its forms, permits electronic surveillance when a significant purpose is to collect "foreign intelligence information."[689] This term is defined as:

> "information that relates to .. the ability of the United States to protect against (A) actual or potential attack … of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction; or (C) clandestine intelligence activities by an intelligence service or network";

[688] 18 U.S.C. § 2712.

[689] 50 U.S.C. §§ 1804(a)(6)(B).

> "[as well as] information with respect to a foreign power or foreign territory that relates to … the national defense or the security of the United States; or … the conduct of the foreign affairs of the United States."[690]

The term has been further limited to mean "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons."[691] Moreover, the Director of National Intelligence has directed that "Intelligence Community elements should permanently retain or disseminate [a foreign person's] information only if [it] relates to an authorized intelligence requirement [and] not *solely* because of the person's non-U.S. person status."[692]

In terms of defining the purposes for which surveillance may be requested, these US terms are as precise as, if not more precise, than the general terms such as "terrorist threats" condoned by the ECtHR in its case law[693] and the purposes listed in Article 8 ECHR. In addition, US law prohibits surveillance for unlawful discrimination or suppression of dissent, or solely to benefit US corporations.[694] The only Illustrative Member State that has an explicit statutory provision comparable to this prohibition is Belgium, which broadly provides that the use of surveillance cannot hinder individual rights and freedoms.

The list of goals for which intelligence surveillance is permitted in the US is much narrower than the goals listed in Article 3(2)[695] and Article 13[696] of Directive 95/46 or

---

[690] 50 U.S.C. § 1801(e).

[691] Exec. Order *12,333* § 3.4.

[692] ODNI, *Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28*, at 5 (July 2014), http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

[693] *Szabó & Vissy v. Hungary*,§ 64 (and additional cases cited):

> "[T]he need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague …. It is satisfied that even in the field of secret surveillance, where foreseeability is of particular concern, the danger of terrorist acts and the needs of rescue operations are both notions sufficiently clear so as to meet the requirements of lawfulness. For the Court, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication."

[694] PPD-28 § 1(b)–(c).

[695] See Article 3(2) of Directive 95/46: "[P]rocessing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."

[696] See Article 13 of Directive 95/46:

> "(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official

in Article 8 ECHR.[697] It may also be recalled in this respect that several of the Illustrative Member States have used the list in Article 8 ECHR to a greater extent than the US. For example, Belgium, France, Poland, and the UK permit surveillance for the protection of national economic interests.

Therefore, in terms of the purposes that establish the necessity of surveillance, the scope for secret intelligence surveillance under FISA is specified significantly more narrowly and precisely than in the Illustrative Member States.

Scope Of Discretion And Foreseeability

FISA Title Isurveillance permits a neutral judge (namely, a member of the Foreign Intelligence Surveillance Court (FISC)) to issue an order only after determining that "probable cause" exists that the target is a foreign power (or its agent) and a significant purpose of the collection is to obtain foreign-intelligence information.[698] In addition, the government must show "a substantial factual nexus between the proffered target … and a foreign power, organisation, or person."[699]

Section 702 permits the intelligence services to engage in the PRISM and Upstream programmes only upon a detailed certification to the FISC that sets out the targeting and minimization procedures to be utilised. Those targeting procedures establish the specific parameters for creating "selectors" or discriminants (email addresses and telephone numbers only), which are then used to collect the contents of information (either stored or in real-time, depending on which programme).[700] Section 215 follows a similar process and requires that the FISC find "reasonable grounds to believe" that the specific selectors used by the government relate to foreign intelligence information.[701]

The procedures to be followed by intelligence agencies in FISA surveillance have been clarified further in documents such the NSA's *Transparency Report: USA Freedom Act Business Records FISA Implementation* of 16 January 2016.[702] The

---

authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others."

[697] See Article 8 ECHR, which lists the following public policy grounds on which interference can be justified: "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[698] 50 U.S.C. § 1805(a)

[699] *Id.* § 1804.

[700] *See supra* notes 390–398 and accompanying text.

[701] *Id.* § 1861(b)(2)(B).

[702] *See, e.g.*, United States Signals Intelligence Directive USSID SP0018 (Jan. 25, 2011); NSA, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (July 28, 2014), http://www.dni.gov/files/documents/0928/NSA%20Section%20702%20Targeting%20Procedures.pdf.

"foreseeability" of secret surveillance in the US is significant, both in terms of the conditions under which and the circumstances within which data subjects may be exposed to secret surveillance. For example, data subjects can estimate with a high degree of foreseeability that involvement with foreign terrorist organisations may expose them to PRISM or Upstream surveillance. Moreover, FISA directives issued under Section 702, including those in furtherance of PRISM and Upstream, remain in effect for one year – at which point the government must seek authorisation anew.[703]

In the Illustrative Member States, laws provide wide discretion to ministers or intelligence officials to authorise surveillance. The threshold level of suspicion for targeted surveillance required in each of the Illustrative Member States varies and in some instances is not provided for, as in Poland and the UK. In this regard, it may be recalled that the FRA report noted widespread bulk, untargeted surveillance in EU Member States, in many cases without a clear legal basis or oversight.[704]

In these circumstances, it appears difficult to argue that the level of protection in the US, in terms of specific legal authority and foreseeability, is lower than in the European Union.

Limitations On Scope

The Fourth Amendment to the US Constitution, part of the US Bill of Rights, protects the right of the American people to be free from unreasonable searches of their persons or their papers, and has been interpreted to protect "expectations of privacy."[705] FISA extends similar protections, in many ways, to all persons and protects these expectations by requiring the intelligence services to obtain a warrant before intercepting communications in real-time.[706] Section 702 provides that data collection must be conducted based on individualised suspicion and in a manner consistent with the Fourth Amendment, and Section 215 (as reformed by the USA FREEDOM Act) likewise requires judicial review and targeted collection. As a result, foreign citizens and their data maintain substantial and significant privacy protection – even when they live abroad.

In fact, under PRISM and Upstream, no data may be collected unless that data responds to "selectors" or "discriminants" that have been set pursuant to targeting procedures reviewed and approved by FISC,[707] and presented to an independent oversight body – the PCLOB – for pre-implementation review and comment.

With regard to the PRISM programme, which targets specific persons and groups using email addresses and telephone numbers as selectors, the number of targets

---

[703] 50 U.S.C. § 1881a(a).

[704] FRA Report, *supra note* 127, at 17.

[705] *See Katz*, 379 U.S. at 354.

[706] 50 U.S.C. § 1805(a).

[707] Robertson, *Opinion*, *supra* note 398, at para. 22 (noting that the PRISM programme "is not 'bulk' or 'generalised' collection, and is more akin to the 'strategic monitoring' which was upheld by the European Court in *Weber & Saravia*").

was limited to 92,707 targets out of the several billion people whose data was transmitted to the US in 2014. Access by the NSA in the aggregate was limited to 0.00004% of internet traffic. These numbers of targets may be put in perspective against the estimated 20,000 foreign fighters currently estimated to be in Syria, who make up only a part of ISIS fighters across the region and elsewhere, and to the numbers of fighters in other groups such as Al-Qaeda.

The Upstream programme, which is also authorised under Section 702 of FISA, is a more targeted version of the programme that collects contents of communications, using the same selectors, in real-time from entities controlling the internet backbone.[708] Reports estimate that information collected via Upstream constitutes only ten percent of that collected pursuant to Section 702.[709]

The US metadata-collection programmes are now similarly circumscribed. The intelligence services may collect metadata from services providers under the USA FREEDOM Act only by submitting FISC-approved selectors. The service providers then search their records, returning those metadata sufficiently related to the selectors. Furthermore, the USA FREEDOM Act makes bulk collection of metadata explicitly illegal.

The current state of the law in the US, therefore, is that untargeted surveillance and bulk collection of metadata by the government is unlawful. This process appears no less protective than the processes used in the Illustrative Member States that have laws authorising non-targeted surveillance. None of the Illustrative Member States provide for *ex ante* judicial review of individual search terms. Even in Germany, the country that has been held up by the ECtHR as the example to follow, has only delegated approval of selectors to the G10 commission, which is not a judicial body.

Multiple safeguards are in place in the US to limit the use of data captured in intelligence surveillance, notably under PRISM and Upstream. The procedures promulgated by the Attorney General and approved by the FISC provide that communications clearly unrelated to foreign intelligence must be destroyed as soon as feasible. Unexamined data obtained via Upstream may be retained for only two years. All data obtained pursuant to Sections 702 and 215 must be destroyed after five years unless the Director of National Intelligence certifies that continued storage of *specific records* is in the national interest. Data retained must not be used except as authorised by law. All these data retention limits apply also to non-US citizens.

In terms of data retention and access, the level of protection in the US is no less than in the Illustrative Member States. None of the Illustrative Member States provide in their surveillance laws for specific statutory safeguards relating to the actual security of the data obtained via authorized surveillance measures beyond, in cases like the UK, a general requirement to store such data securely. Indeed, the UK's Anderson Report stated that "safeguards must be more explicit and more stringent" and

[708] And not, as some have argued, a programme providing for direct access to servers of US internet companies.

[709] Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *supra* note 398, at 17.

recommended the implementation of "strict rules on data minimization […] similar to the controls imposed by the FISC in the United States."[710]

Only in France and Germany do the surveillance laws include prescriptive retention periods, which vary according to the type of data collected. However, these limits on retention only apply in certain cases or in respect of certain types of surveillance. Destruction of data following the requisite retention period is required in the surveillance laws of all Illustrative Member States (other than in Ireland); however, there is no explicit requirement that the destruction be irreversible.

In view of the above, it appears difficult to argue that the level of protection in the US, with regard to limiting the scope of surveillance, falls short of the level of protection required by the ECtHR.

Oversight

In the US, there is a combination of judicial, administrative, legislative, and independent expert oversight. First, the FISC, which is made up entirely of Senate-confirmed federal judges enjoying the unfettered independence assured by life tenure, must approve the government's applications under FISA to intercept and collect specific contents of information, and will do so only if the information proposed to be intercepted is believed to be foreign intelligence information. In fact, on numerous occasions the FISC has denied and modified FISA applications. The FISC also must approve all orders requiring telecommunications providers to release metadata under Section 215 as modified by the USA FREEDOM Act.

In contrast, the Illustrative Member States that permit government surveillance without targeting specific individuals do not require approval of a court; the approvals process involves committees of various types, often linked to the executive branch of government. Only Italy and Poland require any *ex ante* judicial approval of targeted intelligence surveillance.

Second, there are multiple compliance procedures and controls within the US agencies that request approvals for surveillance, and there are Inspectors General and Privacy and Civil Liberties Officers in all of the relevant agencies to provide internal oversight.

Third, the President's Foreign Intelligence Advisory Board also oversee the Intelligence Community's priorities for intelligence collection.

Fourth, the US Congress regularly holds oversight hearings, and the Privacy and Civil Liberties Oversight Board (PCLOB) is widely regarded as a highly influential independent oversight body. Indeed, the Section 215 metadata collection programme was shuttered and reformed in 2015 pursuant to the recommendations of a PCLOB report as well as the report of a specially-appointed Presidential Review Group.

---

[710] Anderson, *A Question of Trust – Report of the Investigatory Powers Review*, *supra* note 282, at 230.

Each of the Illustrative Member States has its own "mix" of oversight mechanisms. However, none of the Illustrative Member States has a combination as extensive as the US. The US uses the full menu of oversight mechanisms, where the Illustrative Member States are choosing à la carte.

Legal Remedies And Redress

The same two remedies and avenues of redress discussed above in connection with law enforcement surveillance are available for targets of unauthorised intelligence surveillance: the exclusionary rule and civil causes of action. Both are open to persons who are not US citizens and outside the US.

The Wiretap Act, ECPA, and FISA all build on the exclusionary rule, extending the rule to violations of statutory law and to non-criminal proceedings.[711] Under this rule, the government is prohibited from introducing evidence obtained directly or indirectly from unlawful surveillance.

In addition, the US legal order also has created three different civil causes of action that permit victims of unlawful surveillance to sue in court for an injunction stopping the surveillance, or for monetary relief.[712] These provisions, by their own terms, are available for US citizens and non-US persons alike.[713] Accordingly, significant and real legal remedies and redress are available under the US legal order.

As noted in Section 2.3.2.3, civil actions in the EU generally occur to a lesser extent than in the US, and the concept of 'statutory damages' is not known. The overview of Member States' redress systems shows that, in case of secret intelligence surveillance, the level of protection in the Illustrative Member States does not appear to be higher than in the US. For example, in the Netherlands, individuals directly affected by surveillance can bring court proceedings and also have the right to complain to the ombudsman. Whereas, in Poland affected individuals only have the right to complain to the Human Rights Defender (the ombudsman). In terms of an individual's right to access and rectify their data, this can often be limited to ensure the effectiveness of surveillance measures deemed necessary. Likewise, only four Illustrative Member States (Belgium, Germany, Italy, and the Netherlands) have explicit provisions in their surveillance laws that allow notification of surveillance to individuals after the fact and even then there are restrictions for national security purposes.

Conclusion

When the facts are carefully considered and unsubstantiated allegations are cast aside, it becomes clear that the American system and that of Europe – despite their stylistic differences – offer equal protections. In many ways it can be said that the United States has imposed even greater procedural safeguards than those of the Illustrative Members States.

---

[711] 18 U.S.C. §§ 2515, 2518(8)–(10); 50 U.S.C. § 1806(c)–(e).

[712] 18 U.S.C. § 2520(a), (b).

[713] *Id.* § 2520; *Suzlon*, 671 F.3d at 731.

This should be unsurprising. Both systems have a long history of valuing and guarding privacy. Both have judged that privacy rights and freedom of expression outweigh the value of mass surveillance in general and, while both systems recognise the need for law enforcement and intelligence services to engage in surveillance to detect, thwart, and punish crime and terrorist activities, their shared commitment to those rights of privacy, dignity, and personal autonomy ensure that any surveillance is carefully controlled and proportionate to the threat.

On the basis of these facts, this report submits that the US laws and regulations governing surveillance are essentially equivalent to those in the EU legal order.

PART THREE:

A STRONG BODY OF STATUTORY LAW, COMMON LAW, ENFORCEMENT AND LITIGATION, AND PRIVACY AND DATA PROTECTION PRACTICES ENSURE THAT EU CITIZENS WHOSE DATA IS TRANSFERRED TO THE US RECEIVE PROTECTION ESSENTIALLY EQUIVALENT TO WHAT THEY RECEIVE IN THE EU, ESPECIALLY WHEN COUPLED WITH A BINDING ADHERENCE TO EU DATA PROTECTION PRINCIPLES

3.1 Despite Differences Between The EU And US Legal Systems, Common Principles Underlie Privacy And Data Protection In The US And EU Directive 95/46

As the CJEU put it in the *Schrems* judgment, "when examining the level of [data] protection in a third country, the Commission is obliged to assess the content of the applicable rules in the country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules …."[714] In practice, this assessment involves a comparison of the third country's law and practices with basic provisions of Directive 95/46.[715]

Applied to the United States, this comparison is complicated by differences in legal systems. The US does not have an omnibus law as in EU Member States and as in most third countries judged adequate. Instead, it has a body of laws – a mosaic of federal and state statutes, common law jurisprudence, and public and private enforcement that obligate private entities to protect personal data and respect the rights of data subjects. Specific and detailed statutory frameworks enforced by various, sometimes overlapping, federal and state regulatory agencies (and through private rights of action) address the most sensitive categories of data – children's and students' data, medical records, financial information, and electronic communications. Privacy standards in these sectors are supplemented by broad and elastic state and federal laws that prohibit "unfair and deceptive" practices and acts, as well as by other state statutes and common law that protect expectations of privacy more generally. And these privacy and data protection interests are subject to the discipline and deterrence brought to bear by the over-arching rule of law, litigation and regulatory enforcement system in the US.[716]

---

[714] *Schrems*, para. 75.

[715] See, *e.g.*, Opinion 11/2011 of the Article 29 Working Party of 4 April 2011, on the level of protection of personal data in New Zealand , WP 182, at 3.

[716] *See generally,* Alan Charles Raul, Tasha D. Manoranjan & Vivek K. Mohan, *Chapter on United States,* in PRIVACY, DATA PROTECTION & CYBERSECURITY L. REV. 363 (2d Ed. 2015) ("[T]he US commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The US privacy system … rel[ies] more on *post hoc* government enforcement and private litigation, and on the corresponding deterrent value of such enforcement and litigation, than on detailed prohibitions and rules …. However, US federal law does impose affirmative prohibitions and restrictions in certain [sensitive] commercial sectors …"). The EU's Article 29 Working Party looked favourably on Israel's system based on the availability of certain data protections emanating from case law, notwithstanding the absence of directly corresponding provisions in written statutory law.

The specificity, diversity, and diffusion of the American system of privacy law can present some challenges in transatlantic translation (just as Americans can find the EU's omnibus approach unduly complicated). Indeed, when leading privacy experts on both sides of the Atlantic convened for the Privacy Bridges Project presented at the 2015 International Data Protection and Privacy Commissioners Conference, their first task was to write a brief paper describing their understanding of the system of privacy and data protection on the other side of the Atlantic; the results evidently showed wide divergence and misunderstanding. If differences in legal systems can challenge even experts in the field, then other Europeans less familiar with the American system and common-law legal process may find them so incomprehensible as to mis-perceive the US as a Wild West of data.

Such perceptions are ill-founded. Privacy is deeply embedded in American values, political culture, and law. Soon after the US established a postal system at the founding of the Republic, it adopted a law making it unlawful to invade the contents of mail.[717] Part 2.2.1 of this report explains the strong constitutional tradition of restraints on government access to information stemming from America's colonial experience and revolution. This Part describes the numerous laws, enforcement agencies, and remedies that shape how businesses, government agencies, and other institutions in the US treat personal data.

The development of these laws has been part of a dialogue across the Atlantic for more than 200 years, both informing and informed by European laws and principles. The US Constitution, adopted in 1788, shares philosophical roots with the contemporaneous Déclaration des droits de l'homme et du citoyen in France, as made plain by ratification of the Constitution's Bill of Rights in 1791.

The US Constitution does not contain an explicit right to data privacy, though it does recognise a "right of the people to be secure in their persons, houses, papers, and effects."[718] The US Supreme Court has recognized a right of privacy in a line of decisions[719] that, while involving protections against the State, protect expectations

---

See Opinion 6/2009 of the Article 29 Data Protection Working Party of 1 December 2009, on the level of protection of personal data in Israel, WP 165.

[717] Mail Fraud Act, 18 Stat. 283, 323 (1872) (codified, as amended, at 18 U.S.C. § 1341).

[718] US Const. amend. IV.

[719] These decisions began with *Griswold v. Connecticut*, 381 U.S. 479 (1965), which recognized the right to access contraception, and extended to prohibit warrantless wiretapping, *Katz v. United States*, 389 U.S. 347 (1967); to permit freedom to marry outside your race, *Loving v. Virginia*, 388 U.S. 1 (1967); to grant access to abortion, *Roe v. Wade*, 410 U.S. 113 (1973); to grant access to pornography within the home, *Stanley v. Georgia*, 394 U.S. 557 (1969); to recognise the right to sexual autonomy, *Lawrence v. Texas*, 539 U.S. 558 (2003); to recognise the privacy of location information tracked by vehicle GPS, *United States v. Jones*, 132 S. Ct. 945 (2012); to recognise the privacy of cell phone data, *Riley v. California,* 134 S. Ct. 2473 (2014); and to permit freedom to marry someone of the same sex, *Obergefell v. Hodges*, 576 U.S. __ (2015).

of privacy, interests in autonomy and freedom, and "personal dignity and autonomy" as "central to the liberty protected by [the Constitution]."[720] Although privacy is implied as a right in the Constitution, it is recognized explicitly in pivotal federal legislation, the Privacy Act of 1974. In the preamble to this legislation, Congress declared that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[721]

Analysis of privacy as a right unto itself begins in both the US and Europe in the late 19th Century. A fountainhead of privacy law in the US is the famous law review article by the great American lawyer (and later Supreme Court Justice) Louis Brandeis and his law partner Samuel Warren, "The Right to Privacy," published in 1890.[722] Warren and Brandeis discerned an existing right to privacy in US jurisprudence grounded in the dignity of the individual, also described as a "right to be let alone."[723] This right emanates from common law cases that implied relationships of trust based on disclosure of confidential information or that otherwise protected against intrusions into this right to be let alone.[724] Their article became a foundation for the evolution of the common law tort of invasion of privacy described more fully below and recognized in various state constitutions and laws.

This foundation overlaps with the development of a right to privacy in European law and represents an important cross-pollination between Europe and the US. French legal scholars trace the origins of privacy jurisprudence in their country to Warren and Brandeis.[725] Warren and Brandeis in turn cite a French law on publication of private information as the first explicit recognition of a right to privacy,[726] and they were influenced by the development of the German law of personality.[727]

This exchange of ideas continues to the present day. In response to the advent of widespread computing and large databases in the 1960s and 1970s, the US Department of Health, Education and Welfare appointed an influential advisory committee that developed the first iteration of the Fair Information Practice Principles

---

[720] *Planned Parenthood v. Casey*, 505 U.S. 833, 851 (1992).

[721] Privacy Act of 1974, Pub. L. 93-579 § 2(a), 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

[722] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4. HARV. L. REV. 193 (1890).

[723] *Id.* at 193.

[724] *Id.*

[725] J. Carbonnier, *Droit Civil*, Paris, Presses Universitaires de France, 8th ed., 1969, para.. 74, at 259; R. Badinter, 'Le droit au respect de la vie privée', *J.C.P.* 1968, No. 2136, para. 3.

[726] Warren & Brandeis, *supra* note 722, at 214 n.1 (citing *Loi Relative à la Presse*, *11* Mai 1868 ("Toute publication dans un écrit périodique à un fait de la vie privée constitue une contravention punie d'un amende de cinq cent francs.")).

[727] James Whitman, *Two Western Cultures of Privacy*, 113 YALE L. J. 1151, 1182–86 (2004).

(FIPPs).[728] Its recommendations articulated (albeit in different terminology) principles of transparency, consent, use limitations, access and correction, and data reliability that were reflected in the federal Privacy Act of 1974. In turn, these FIPPs became a basis for the Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD),[729] which both the US and various EU Member States helped to develop. The OECD guidelines then became a basis for the principles that underlie Directive 95/46.[730] Today, these principles are carried forward in the proposed EU General Data Protection Regulation and numerous US statutes and regulations, and they inform the practices of privacy professionals on both sides of the Atlantic.

Thus, the US legal order for privacy and data protection has common origins and common principles with the legal order in Europe. This is not to say that the two legal orders are identical. In addition to its different legal process, the US most saliently strikes a different balance between the rights of privacy and of free expression. Yet both systems both share a foundational commitment to protect fundamental rights and recognise privacy and free expression as fundamental. Both also recognise that these rights are not absolute and must be balanced with each other and with other fundamental rights.[731] And the *Schrems* judgment made clear that the legal order of a third country need not be identical to be deemed essentially equivalent to the EU data protection regime. What matters is the substance of the protections that results from the legal order, not the form. For two reasons, adequacy does not depend solely on the laws on the books.

First, the *Schrems* judgment states that assessment of a third country includes "the practice designed to ensure compliance" with domestic laws and international commitments.[732] Further, adequacy decisions concerning third countries must "take account of non-legal rules, application in practice, and the general administrative and

[728] Robert Gellman, *Fair Information Practices: A Basic History*, Version 2.15, at 2 (Dec. 4, 2015), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[729] *Id.* at 6.

[730] *Id.* at 10.

[731] The proposed Regulation expressly recognizes that "[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality." Sec. (3a) of proposed consolidated version of General Data Protection Regulation; *see also* Proposal for a Regulation of the European Parliament and of the Council of 25 January 2012, 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/2012/011 final, § 3.3 (summary of fundamental rights issues); CJEU 9 November 2010, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, ECLI:EU:C:2010:662.

[732] *Schrems*, para. 75.

corporate culture that exists in relation to privacy."[733] It is therefore necessary to look at how the legal order is put into practice.

An American propensity for litigation has made compliance not only with law but also with best practices essential to doing business in America and minimizing the risk of expensive litigation. Leading privacy scholars at the Berkeley Center for Law and Information conducted a multi-year empirical study of privacy practices and cultures among US and EU companies; they found that in spite of "sectoral, fragmented, and incomplete" laws on the books in the US, "corporate practices reflected a more integrated and robust approach to privacy management" in the US than among many EU peers.[734] Section 3.3 below explores this "privacy on the ground" in greater detail.

Second, where companies are legally bound to adhere to the principles of Directive 95/46, they may undertake obligations beyond those of applicable US laws. Such adherence can come about pursuant to a broad data transfer framework such as the 2000 Safe Harbour Framework. In *Schrems*, the CJEU stated that consideration of adequacy may take into account "a system of self-certification" provided the mechanisms for detection of violations and supervision of compliance are effective in identifying and punishing violations of fundamental rights.[735] It also can come about pursuant to "appropriate contractual clauses" or other rules of law applicable to a specific data transfer or set of transfers allowed under Articles 25(2) and 26(2) of Directive 95/46.[736] In either case, these Articles, read in light of the *Schrems* judgment, make clear that individual companies may qualify to transfer data to the US by binding themselves to rules that both reflect fundamental principles of the Directive and are subject to effective accountability and enforcement. The next section shows how companies' promises in this regard are enforceable in the US.

Taken together, the robust system of privacy and data protections laws and practices under the US legal order, coupled with enhanced adherence to a set of principles based on EU law through either a broad framework or specific commitments, provide protection for the personal data of EU citizens transferred to the US that is essentially equivalent to the level of protection within the EU. The legal order and the self-certification framework complement each other: the framework addresses differences between the US and EU legal order, and the US legal order reinforces commitments to the EU principles in the self-certification framework. The sections that follow show how these systems operate together.

---

[733] Opinion 11/2011 of the Article 29 Working Party of 4 April 2011, on the level of protection of personal data in New Zealand, WP 182, p. 2.

[734] Kenneth Bamberger & Deirdre Mulligan, *PRIVACY ON THE GROUND* 6 (2015).

[735] *Schrems*, para. 81.

[736] *Schrems*, para. 4.

3.2 Binding Adherence To Principles Of EU Data Protection Law Ensures That Data Transfers To The US Comply With Directive 95/46

Although the transatlantic data transfer framework approved in the Commission's Safe Harbour Decision has been invalidated in the *Schrems* judgment, the CJEU's judgment does not preclude another such broad framework that incorporates the principles of EU data protection law. Such a data transfer framework establishes a company-specific "adequacy" by requiring adherence to these principles. Adherence has two elements. First, it requires that companies publicly subscribe to the principles. Second, it calls for enforcement of these commitments by public bodies, principally the US Federal Trade Commission (FTC).

A company's commitment to adhere to the principles of such a framework is legally binding. The mechanism operates on a company-specific basis just as Model Clauses and Binding Corporate Rules do. The latter enables transfers to third countries regardless of whether these countries are found adequate because they directly require companies to act consistent with EU law and "compensate for the absence of a general level of adequate protection, by including the essential elements of protection which are missing …."[737] Under Article 25 (2) of Directive 95/46, such mechanisms permit data transfers "in light of all the circumstances surrounding a data transfer or a set of data transfers …," and Article 26(2) allows Member States to authorise transfers "where the controller adduces adequate safeguards," which "may in particular result from appropriate contractual clauses."[738] A transatlantic data transfer framework based on a binding commitment to principles of EU data protection law accomplishes the same safeguards.[739]

These commitments are legally binding because they are subject to enforcement by the FTC. As described more fully below, the FTC has broad authority to regulate unfair and deceptive practices or acts,[740] and it uses this authority to enforce promises that companies make to their customers. These include promises like commitments to the Safe Harbour Framework. Companies that certify falsely to a framework such as Safe Harbour also are subject to potential serious criminal liability.[741]

---

[737] Working document of the Article 29 Working Party of 24 July 1998, on transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP 12, p.16.

[738] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 1995 L281/31, as amended, Article 26(2).

[739] The question whether national security, public interest, and law enforcement requirements can override these binding commitments in ways that interfere with fundamental rights is addressed in Part 2.2 *supra*.

[740] 15 U.S.C. § 45(a).

[741] *See* False Statements Act, 18 U.S.C. § 1001; *see also Recertification: Annual Reaffirmation of an Organization's Commitment to the Safe Harbor Framework(s)*, EXPORT.GOV (May 2013) ("Safe Harbor certifying 'officer understands that misrepresentations in any information provided by the organization may be actionable under the False Statements Act, 18 U.S.C. [§] 1001.'").

In 2009, the FTC brought enforcement cases against six companies for their alleged failure to fulfill Safe Harbour commitments.[742] Since then, the FTC has brought more than 30 Safe Harbour enforcement cases. These actions involved allegations of the use of consumer data without consent, inadequate disclosures, data retention and sharing issues, and misrepresentations involving participation in the US-EU Safe Harbour framework.[743]

More than 4,000 companies bound themselves to the principles of the Safe Harbour Framework voluntarily. The incorporation of these principles has a substantial affect on US law by applying the rights of EU data subjects under Directive 95/46 regardless of whether these are explicitly reflected in US laws applying to companies that subscribe. FTC enforcement provides "effective detection and supervision mechanisms" to give force to these self-certifications.[744]

3.3 Rules And Practices In The US Correspond To The General Rules And Principles In Chapter II Of Directive 95/46

3.3.1 US Statutory Law, Common Law, Enforcement And Litigation, And Privacy Practices Establish A Framework Of Privacy And Data Protection

A review of adequacy begins with an examination of a country's legislation.[745] In the US since 1970, a continuously expanding array of federal and state privacy laws, regulations, and common law have established a comprehensive privacy regime that aligns with EU law. Privacy is addressed in approximately 350 separate statutes

---

[742] Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor 3–4 (Nov. 12, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf. *See also In re World Innovators, Inc.,* Compl., Docket No. C-4282 (FTC Oct. 6, 2009); *In re ExpatEdge Partners, LLC*, Compl., Docket No. C-4269 (FTC Oct. 6, 2009); *In re Matter of Onyx Graphics, Inc.*, Compl., Docket No. C-4270 (FTC Oct. 6, 2009); *In re Directors Desk LLC*, Compl., Docket No. C-4281 (FTC Oct. 6, 2009); *In re Progressive Gaitways LLC*, Docket No. C-4271 (FTC Oct. 6, 2009); *In re Collectify LLC*, Compl. Docket No. C-4272 (FTC Oct. 6, 2009).

[743] *See, e.g.*, *In re TRUSTe*, Docket No. C-4512 (FTC Mar. 12, 2015) (imposing a $200,000 fine, alleging that TRUSTe, Inc. failed to conduct over 1,000 annual recertification reviews for certified companies, despite representing that companies holding the TRUSTe Certified Privacy Seal are recertified annually and were in compliance with specific privacy standards, including COPPA and the US-EU Safe Harbor Framework); *see also* FTC, *Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed to Comply with International Safe Harbor Framework* (Aug. 17, 2015) (announcing settlement of charges with thirteen companies regarding allegations that they falsely claimed they were abiding by the Safe Harbour Privacy Framework even though they had allowed their certifications to lapse or never actually applied for membership in the program); FTC, *FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework* (Jan. 21, 2014) (announcing settlement of charges with 12 companies regarding charges that they falsely claimed they were abiding by the Safe Harbour Privacy Framework even though they had allowed their certifications to lapse).

[744] *Schrems* para. 81.

[745] *See* Part 3.1 *supra*.

within 33 of the 54 titles of the US Code (the authoritative compilation of US federal statutes). Most recently, the Cybersecurity Information Sharing Act adopted in December 2015 includes provisions requiring companies to delete personal information not needed for cybersecurity purposes from information before they share cyber threat indicators with the government or other companies.[746]

The most sensitive data – such as financial, medical, health, electronic communications, and children's information – are protected by nearly two dozen federal sector-specific laws and numerous state laws. These laws are backstopped by the broad reach of the Federal Trade Commission Act, which generally prohibits unfair and deceptive acts and practices and has been interpreted to prohibit a broad range of data processing that violates individuals' data protection interests.[747]

State laws apply additional privacy rights and data protections over and above the baseline of federal law and cover some areas not addressed by federal law.[748] States regulate information security, online privacy, cyber stalking, data disposal, data breach notification, medical information, financial information, employee privacy, consumer reports, unsolicited commercial communications, electronic solicitation of children, and children's online right to be forgotten, to name a few subjects.[749]

Certain states also require privacy policies for websites and impose security requirements for the handling of sensitive personal data. The State of California's protections are especially relevant for EU data subjects because numerous global technology companies are based in that state and tailor their privacy policies and practices to comply with its laws. Further, any company that does business with California residents (which includes most online companies) must comply with these laws. The California Constitution protects privacy as a fundamental right, a provision that is cited frequently in civil litigation against private parties.[750] California also

---

[746] Cybersecurity Act of 2015, Pub. L. No. 114–113, Division N, § 104(d).

[747] *See, e.g.*, *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 (3d Cir. 2015).

[748] For example, compare third party disclosure requirements in Title V, Subtitle A of the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act or GLBA), *see infra* note 757, that (among many detailed data protection provisions) permits affiliate sharing of certain information provided certain notice and other requirements are met, with the California Financial Information Privacy Act, Cal. Fin. Code §§ 4050–4060, which provides both notice requirements and a right to opt out of disclosures of certain information to affiliated third parties.

[749] *See, e.g.*, Cal. Bus. & Prof. Code §§ 22575–22579 (online privacy); Cal. Bus. & Prof. Code § 22580 *et seq*. (children's online right to be forgotten); Cal. Fin. Code §§ 4050–4060 (financial information); Conn. Gen. Stat. § 36a-701b (data breach notification); Fla. Stat. Ann. § 668.60 *et seq*. (unsolicited commercial communications); Mass. Gen. Laws ch. 151 § 4(9) (consumer reports and background checks); Md. Crim. Law § 3-805(cyber stalking and harassment); N.J. Pub. L. 2013, c.155 (C.34:6B-5 *et seq*.) (employer access to social media accounts); N.Y. Penal Law § 235.22 (electronic solicitation of children); S.C. Code Ann. §§ 37-20-190 (secure disposal); Tex. Health & Safety Code § 181.001 *et seq*. (health information); Utah Code Ann. § 13-44-201 (general information security).

[750] Cal. Const. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty … *and privacy*") (emphasis added).

leads the nation in detailed data protection laws and regulations, with over 100 such laws addressing privacy of personal data.[751]

Federal and state privacy laws are enforced by an expanding network of federal regulatory agencies, federal prosecutors, state Attorneys General and other state regulators, and private plaintiffs. Many states have created formal units charged with privacy oversight, and state Attorneys General often cooperate in joint enforcement actions against companies that experience data breaches or privacy violations.[752] In the US, coordinated and comprehensive privacy regulation combined with active enforcement and sizable fines establish a strong deterrent to motivate compliance with US privacy and security requirements – perhaps even stronger than in the EU.[753]

Regulation Of Sensitive Personal Data

The United States privacy regime at the federal and state levels includes special protections for information relating to personal finances, health and insurance, communications, children, and students.

Financial Data

The Fair Credit Reporting Act (FCRA)[754] was adopted in 1970, the same year that France first incorporated a right to privacy into its Civil Code.[755] FCRA protects consumers against the disclosure of personal information relating to consumers' creditworthiness, credit standing, credit capacity, character, general reputation, or

[751] Such laws relate to personal data collected by state agencies (birth, marriage, death, court, library, voter and driver's license records); Internet of Things (connected automobiles, RFID devices, smart meters); retail (credit card usage, personal data collection at point of sale, driver's license swiping, rental car surveillance, loyalty programs); telecommunications (calling patterns and financial data); employment (workplace surveillance, employee social media); healthcare (access, correction, disclosure, confidentiality, use of information for marketing); and insurance transactions.

[752] *See, e.g.*, David Streitfeld, *Google Concedes That Drive-By Prying Violated Privacy*, N.Y. TIMES (Mar. 12, 2013) (reporting joint privacy investigation by 38 states Attorneys General). http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?_r=1&.

[753] In its Communication introducing the General Data Protection Regulation in 2012, the Commission observed that "[i]n some cases, [Member States] are unable to perform their enforcement tasks satisfactorily." European Commission, Communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of Regions of 25 January 2012, on Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM(2012) 9 final, p. 7. *See also* Christopher Wolf, *Delusion of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. UNIV. J. LAW & POLITICS 227, 231 (2013) (noting that EU privacy law protections "are not matched by EU enforcement of those protections").

[754] 15 U.S.C. § 1681, *et seq.*

[755] Loi No. 70-643 du 17 juillet 1970; S. Kauder, Les lois "Informatique et liberté" en France, en Europe et dans le monde, available at: http://www.legalbiznext.com/droit/IMG/pdf/Informatiqueetliberte.pdf.

personal characteristics. The Fair and Accurate Credit Transactions Act (FACTA)[756] amended FCRA to protect against identity theft. The FTC, the Consumer Financial Protection Bureau (CFPB), and banking regulators share enforcement authority, and violators are subject to civil liability and enforcement actions.

The Gramm-Leach-Bliley Act (GLBA)[757] regulates all financial institutions.[758] Its privacy and safeguards rules require all financial institutions to safeguard consumer privacy. Under its Privacy Rule,[759] financial institutions must disclose their practices of collecting and sharing consumer personal information and are prohibited from sharing personal data with certain third parties without consent. Under its Safeguards Rule,[760] financial institutions must, among other things, implement a written information security programme to protect personal financial information. Several federal agencies – including the FTC, Securities and Exchange Commission (SEC), CFPB, and state insurance authorities – share enforcement authority under GLBA.

States also regulate financial data. Most state laws include restrictions on the ability to collect and use personal financial information.[761]

Health And Medical Data

Medical privacy is protected by several statutes, most significantly the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations.[762] HIPAA protects the privacy and security of individually identifiable health information and applies to healthcare providers, health plans and insurers, healthcare clearinghouses, and organisations that collect or process personal health information on behalf of covered entities (business associates), which include legal, accounting, administrative, and financial services, and claims and file management. The HIPAA Privacy Rule,[763] a regulation promulgated by the US Department of Health and Human Services (HHS), was adopted in 2000 and recently updated; it limits the collection, use, and disclosure of medical information. A complementary

[756] Pub. L. 108-159, 111 Stat. 1952 (amending FCRA, 15 U.S.C. § 1681, *et seq*).

[757] Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809.

[758] *Id.* § 6809. The term "financial institution" is defined broadly by reference to section 4(k) of the Bank Holding Company Act, 12 U.S.C. § 1843(k), and encompasses all entities providing financial services that are permissible for a financial services holding company to provide, such as banks, securities and insurance firms, thrifts and credit unions, as well as nontraditional financial institutions.

[759] 16 C.F.R. Part 313.

[760] 16 C.F.R. Part 314.

[761] *See, e.g.*, California's Security of Personal Information Act, Cal. Civ. Code § 1798.81.5; Consumer Credit Reporting Agencies Act, Cal. Civ. Code §§ 1785.1–1785.36; Financial Information Privacy Act, Cal. Fin. Code §§ 4050-4060.

[762] Pub. L. 104–19 §§ 262, 264; 42 U.S.C. §§ 1320d–1320d-9; 45 C.F.R. Parts 160 & 164.

[763] 45 C.F.R. Parts 160 & 164, Subparts A & E.

regulation, the HIPAA Security Rule,[764] sets forth minimum standards for the security of electronic personal health data.

The Health Information Technology for Economic and Clinical Health Act (HITECH)[765] requires notifications to individuals, covered entities, regulators, and the media in the event of a data security breach. The HHS Office for Civil Rights (HHS/OCR) investigates claims and assesses civil penalties for HIPAA and HITECH violations, and federal prosecutors may initiate criminal proceedings to enforce the requirements of this legislation. The FTC also has authority to enforce HITECH's standards against the providers of "electronic health records" that are not otherwise regulated by HHS/OCR.

Genetic information is separately protected under the Genetic Information Nondiscrimination Act (GINA),[766] which amended various statutes to limit the use and disclosure of genetic information.

Most states also have additional protections for the use, collection and disclosure of health information.[767] These state laws may apply to personally identifiable health information in a broader context than HIPAA, and indeed may provide broader penalty provisions than HIPAA (by, for example, authorising a private right of action).[768]

Electronic Communications Data

Rules relating to the privacy of electronic communications are of special importance to the level of protection for EU citizens whose data is transmitted or stored in the US, as much of that data comes within the scope of these rules.

The Electronic Communications Privacy Act (ECPA), discussed above in relation to government access to electronic communications data, also applies to private sector

[764] 45 C.F.R. Parts 160 & 164, Subparts A & C.

[765] 42 U.S.C. § 17932.

[766] Pub. L. 110–233, 122 Stat. 881 (2008) (codified at 42 U.S.C. § 2000ff (note)).

[767] California, for example, restricts access by unauthorised persons to birth and death records, psychiatric records, blood tests (particularly HIV tests), and medical records. Cal. Health & Safety Code §§ 102230–102232, 103525–103528, 120975–121020; Cal. Welf. & Inst. Code § 5328. It also limits the disclosure of patients' medical information and electronic medical information by healthcare and other businesses (including for marketing purposes) and guarantees the right of patients to see, copy, and correct their health records. Cal. Health & Safety Code §§ 1280.15, 123110; Cal. Civ. Code §§ 56–56.37, 1798.91.

[768] While state health privacy laws vary widely, most regulate the practices of health care plans and providers, or those that maintain medical information for patients or health care providers. *E.g.*, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56 *et seq*. A small minority of state laws, however, regulate medical records held by any entity in possession of such records as part of a comprehensive health privacy law. *E.g.*, Wis. Stat. Ann. §§ 146.81–146.84. Further, some state laws regulating health care plans and providers may also include strict limitations on re-disclosure of health information received from a health care plan or provider.

actors.[769] It protects the privacy and security of certain "electronic communications"[770] through two separate statutes that affect the private sector: the Wiretap Act[771] and the Stored Communications Act.[772] Outside of certain limited exceptions, ECPA prohibits the intentional interception or disclosure of electronic communications such as telephone calls, email, and text messages without the consent of the calling or receiving parties.[773] With certain exceptions, it also prohibits intentional, unauthorised access or disclosure of stored communications. ECPA also contains certain protections for "non-content" or transactional information, such as basic subscriber information, the recipient of a communication, or the date of a communication. Violators are subject to criminal and civil enforcement.

A majority of US states have also passed laws prohibiting wiretapping of communications or otherwise prohibiting eavesdropping. Some of these laws provide stronger protections than the federal law, and few are wholly preempted by federal law.[774] In particular, a number of states require consent from all parties to a communication – rather than just one party – to permit recording communications.[775]

The federal Communications Act authorizes the Federal Communications Commission (FCC) to regulate "unjust and unreasonable" practices by telecommunications providers.[776] The FCC has interpreted these provisions to require fair privacy practices by telecommunications and broadband providers. [777] In addition, Section 222 of the Communications Act regulates the collection and use of customer proprietary network information (CPNI) by telecommunications carriers, and prohibits carriers from using and disclosing customer information for certain purposes without the customer's consent. The FCC has declared that Section 222

---

[769] *See supra* Part 2.2.

[770] ECPA defines "electronic communications" as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted by a wire, radio, electromagnetic, photoelectronic or photooptical system, but does not include "(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device …; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds ...." 18 U.S.C. § 2510(12).

[771] *Id.* §§ 2510–2522.

[772] *Id.* §§ 2701–2712.

[773] *Id*. § 2510.

[774] *See, e.g.*, Ala. Code §§ 13A-11-30, 13A-11-31; Conn. Gen. Stat. §§ 53a-187–53a-189.

[775] *See, e.g.*, Cal. Penal Code §§ 631–637; Fla. Stat. Ann. §§ 934.03–934.43; 720 Ill. Comp. Stat. Ann. § 5/14-2; Mass. Gen. Laws Ann. ch. 272, § 99.

[776] 47 U.S.C. § 222.

[777] FCC, *TerraCom and YourTel to Pay $3.5 Million to Resolve Consumer Privacy & Lifeline Investigations* (July 9, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-334286A1.pdf.

and the Communications Act apply to Internet Service Providers (ISPs) and will be initiating rulemaking proceedings to apply the CPNI regulations to them.[778]

Other statutes regulate particular forms of communication and technology. The Cable Television Act protects consumer privacy by providing explicit requirements for notice, consent, use and disclosure, consumer access, destruction, and remedies for violations.[779] The Video Privacy Protection Act protects data on consumer video content preferences and bans disclosure of personally-identifiable information without written consent.[780] The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) protects individuals against unsolicited commercial electronic communications.[781] And the Telephone Consumer Protection Act (TCPA) protects individuals from unwanted or harassing telemarketing and other communications made by autodialers, pre-recorded messages, text messages, or faxes.[782]

Data Of Children And Students

The primary federal statute protecting children's information is the Children's Online Privacy Protection Act (COPPA),[783] which requires parental notification and verifiable express consent before collecting or using the personal information (including geolocation information and persistent identifiers) of children under age 13. The FTC has the authority to issue regulations under COPPA, and it substantially revised its regulations in 2012.[784] It actively enforces COPPA and has assessed penalties for violations of the Act that range up to $3 million.[785] State Attorneys General also may enforce COPPA.

The Family Educational Rights and Privacy Act (FERPA)[786] protects student data in education records and requires enhanced notice to students and parents, as well as consent before such records are released to third parties. The Protection of Pupil Rights Amendment (PPRA) expanded these protections to information regarding

[778] FCC, *In re Protecting and Promoting the Open Internet*, GN Doc. No. 14-28 (Mar. 12, 2015).

[779] 47 U.S.C. § 551

[780] Pub. L. No. 100–618, 102 Stat. 3195 (1988) (codified, as amended, at 18 U.S.C. § 2710).

[781] 15 U.S.C. §§ 7701–7713.

[782] 47 U.S.C. § 227 *et. seq*.

[783] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq*.; 16 C.F.R. Part 312.

[784] FTC, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule* (Dec. 19, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

[785] *See, e.g.*, FTC, *Operators of Online "Virtual Worlds" to Pay $3 Million to Settle FTC Charges That They Illegally Collected and Disclosed Children's Personal Information* (May 12, 2011), available at https://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-million-settle-ftc-charges.

[786] 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

underage students such as political affiliation, religion, income level (including participation in federally-funded assistance programs), mental and psychological conditions, sexual behaviour and attitudes, illegal or self-incriminating behaviour, and critical reviews of family members.[787]

State laws also protect children and student data. The most comprehensive state privacy regime is in California, which enacted the Student Online Personal Information Protection Act (SOPIPA), prohibiting online services from targeting advertisements to students or using student information to develop profiles of students.[788] Other states have enacted significant measures. In 2015 alone, 46 states introduced 182 bills focused on student privacy, and 15 states passed 28 new student privacy bills.[789] These laws establish requirements for data governance and privacy oversight, and promote transparency concerning the processing of student data.

General Regulation Of Privacy

In addition to the sector-specific regulation of privacy, US privacy is governed by several broad statutes that prohibit unfair and deceptive acts and practices, require data security for the protection of personal information, and require notification to consumers and regulatory agencies in the event of an information security incident that compromises the security or integrity of personal data. These general privacy protections and the state and federal agencies tasked with enforcing them are essential to the US privacy protection regime. Significantly, these general statutes apply to data that may not be covered by the sector-specific statutes that protect the most sensitive categories of personal information.

The Federal Trade Commission Act (FTC Act)[790] and its state analogues have the broadest impact on privacy and data protection in the US. These laws cover areas not addressed by sector-specific privacy laws by permitting government prosecutors to bring legal action to recover damages for (or to enjoin) privacy violations. The FTC, state Attorneys General, and private plaintiffs have enforced general principles of privacy to regulate and protect consumer privacy across all commercial sectors.

---

[787] *Id.* § 1232h.

[788] Cal. Stat., ch. 839 (2014) (codified at Cal. Bus. & Prof. Code § 22584 *et seq*.). California is the most active state in this area, with many of its provisions being adopted in other states. Most recently, California enacted the Privacy Rights for California Minors in the Digital World Act, which regulates online marketing directed to minors. The law prohibits online service companies from marketing products to children that they are not legally permitted to buy, and from collecting personal data from children for the purpose of sharing with third parties. It also requires that online service providers permit any California minor to request permanent deletion of collected and stored personal data, and that the provider disclose this right (including how to exercise it) to minors. *See* Cal. Stat. ch. 336 (2013) (codified at Cal. Bus. & Prof. Code § 22580 *et seq*.) (Privacy Rights for California Minors in the Digital World).

[789] *See* Data Quality Campaign, *Student Data Privacy Legislation* (2015).

[790] Federal Trade Commission Act (FTCA), 15 U.S.C. § 41 *et seq.*

The Federal Trade Commission

The FTC is the lead privacy enforcement agency in the US.[791] It has brought numerous enforcement actions totalling more than $1 billion in redress or disgorgement.[792] At the same time, the FTC has issued regulations on children's privacy,[793] financial privacy,[794] telecommunications privacy,[795] and other areas. Beginning with a workshop on the implications of the Internet in 1995,[796] the FTC also has elaborated privacy standards for industry in various reports and guidance on issues such as Internet advertising, the Internet of Things, big data, and other emerging issues. These reports and guidance carry significant weight through the threat of enforcement under the FTC's flexible authority detailed below.

The FTC is an independent administrative agency, led by five commissioners nominated by the President and confirmed by the Senate to serve seven-year terms, no more than three of whom may be from the same political party.[797] Although the President designates which commissioner shall act as Chairman, there is a limit on presidential influence and control. Unlike most other agencies in the executive branch, FTC commissioners do not serve at the pleasure of the President, and they have separate terms of office. Federal law limits the authority of the President to remove FTC commissioners from office and direct their actions, further strengthening their independence and authority.[798]

The FTC has authority to enforce privacy and security protections across a wide spectrum of US industries.[799] Its authority derives from Section 5 of the FTC Act,

---

[791] *See generally*, Edward R. McNicholas, Andrew J. Strenio, Jr. & Clayton G. Northouse, *FTC Enforcement* (BNA 2014).

[792] FTC, *Federal Trade Commission 2014 Privacy and Data Security Update*, available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[793] Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

[794] Privacy of Consumer Financial Information, 16 C.F.R. Part 313; Standards for Safeguarding Customer Information, 16 C.F.R. Part 314.

[795] Telemarketing Sales Rule, 16 C.F.R. Part 310.

[796] *See* Bamberger & Mulligan, *PRIVACY ON THE GROUND*, *supra* note 734, at 187.

[797] 15 U.S.C. § 41.

[798] *See Humphrey's Executor v. United States*, 295 U.S. 602, 626 (1935).

[799] Those industries excepted, in whole or in part, from the FTC's jurisdiction include banks, credit unions, telecommunications carriers, interstate transportation common carriers, air carriers, and packers and stockyard operators, all of which are regulated by other agencies under other laws. Financial institutions are regulated by a number of federal agencies, including the SEC, the Commodity Futures Trading Commission, and the CFPB, pursuant to the FCRA, the FACTA, the GLBA, and the Fair Debt Collection Practices Act, among others. Telecommunications common carriers are regulated by the FCC under the Communications Act of 1934 (47 U.S.C. § 151 *et seq.*). Interstate transportation common carriers are regulated by the Department of Transportation under 49 U.S.C. subtitle IV, and air common carriers are regulated by the Federal Aviation Act of 1958. The Secretary of Agriculture enforces the Packers and Stockyards Act of 1921 (7 U.S.C. § 181 *et seq.*),

which prohibits "unfair or deceptive" acts or practices.[800] The FTC interprets "unfair practices" to include unexpected information practices such as inadequate disclosures to consumers[801] and the failure to implement adequate protection measures for sensitive personal information,[802] and the FTC interprets "deceptive" to include misrepresentations, false promises, and failures to comply with representations made to consumers, such as statements in privacy policies and other publicly-disclosed privacy and security practices, as well as those regarding Safe Harbour certifications discussed above.[803] These sweeping definitions create a general privacy protection framework that broadly covers commercial activities throughout the US.

The FTC's enforcement authority includes the power to issue cease and desist orders, seek temporary restraining orders or permanent injunctions against proscribed conduct, and seek consent decrees to govern a company's conduct without a judicial finding of liability.[804] In the area of privacy and data protection, consent decrees typically require comprehensive privacy and security programs, robust notice and choice provisions, deletion of improperly-obtained consumer data, and independent third-party assessments, monetary compensation, or disgorgement of gains.[805] A company that fails to comply with an FTC order is subject to substantial civil penalties. An FTC enforcement action can result in 20 years of oversight and significant fines of up to $16,000 per violation per day. The pervasive publicity surrounding such enforcement actions serves as a strong incentive to other organizations to comply with fair privacy and security practices.

Through the process of bringing select enforcement actions and resolving them through consent decrees, with occasional actions going to litigation, the FTC has been able to signal a baseline set of privacy norms and principles regarding the collection and use of personal information. Professors Daniel J. Solove and Woodrow Hartzog have described this process as establishing a general "common law" of privacy.[806] Through the enforcement of its Section 5 authority, the FTC has attained the authority to provide "sprawling jurisdiction to enforce privacy in addition

---

although that Act arguably does not reach personal privacy concerns, which would then default to FTC enforcement.

[800] 15 U.S.C. § 45(a).

[801] *See, e.g.*, *Fed. Trade Comm'n v. Amazon.com, Inc.*, No. 2:14-cv-01038 (D. Wash., ongoing).

[802] Gina Stevens, *The Federal Trade Commission's Regulations of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, Cong. Research Service (2014) (collecting enforcement actions), https://www.fas.org/sgp/crs/misc/R43723.pdf.

[803] *See generally* McNicholas, Strenio & Northouse, *FTC Enforcement*, *supra* note 791, at chapter 2.

[804] *Id.* at 706–09.

[805] *See, e.g.*, *Fed. Trade Comm'n v. Wyndham*, Civ. No. 2:13-CV-01887-ES-JAD (D. N.J. Dec. 11, 2015), https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf.

[806] See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

to the pockets of statutory jurisdiction Congress has given to it in industry-specific privacy legislation. The FTC reigns over more territory than any other agency that deals with privacy."[807] Its enforcement actions and consent orders regularly operate to protect EU citizens and other global customers of companies under FTC jurisdiction

The FTC's authority to levy significant monetary fines and seek consumer redress or disgorgement of profits gives significant weight to this broad enforcement authority. For example, just this past December, the FTC secured a settlement from an identity theft protection provider for failure to secure personal information and deceptive statements related to its data protection services that included a settlement payment of $100 million.[808] By comparison, one of the largest settlements in the EU was an action by the UK Financial Services Authority in 2009 against HSBC related to alleged security failures for £3 million.[809] In 2013, the FTC reportedly initiated over 30 privacy-related enforcement actions and issued approximately $64 million in civil penalties[810]; that same year, the most active data protection authority in Europe was the Garante in Italy, which issued fines that totalled approximately $5.4 million.[811] In short, the US system imposes significant penalties and fines for the protection of privacy and security that are just as strong if not stronger than those imposed in the EU.

In addition to initiating enforcement actions, the FTC plays a leadership role in policy development, research, education, and stakeholder communications to protect consumers' personal information that resembles the thought-leadership role played by the Article 29 Working Party in the EU. The FTC has issued guidance or policy statements on the following:

[807] *Id.* at 586. In this light, Professors Solove and Hartzong observe, the common approach of classifying the US privacy legal regime as "fragmented" or "hollow" when compared with the EU is "outdated."

[808] FTC, *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges It Violated 2010 Order* (Dec. 17, 2015).

[809] Jill Treanor, *HSBC Fined £3m for 'Careless' Handling of Customer Details*, THE GUARDIAN (July 22, 2009).

[810] *See* FTC, *Federal Trade Commission 2014 Privacy and Data Security Update*, *supra* note 792.

[811] Ghostery, *Ignoring Privacy Enforcement Costing Businesses Millions Worldwide* (June 5, 2015), available at https://www.ghostery.com/intelligence/business-blog/business/ignoring-privacy-enforcement-costing-businesses-mi/.

- *Big Data* – addressing the effects of "big data" on consumer privacy, stressing the importance of de-identification, accountability, and "notice and consent" disclosures and highlighting areas of concern relating to discrimination, fraud, and exposure of sensitive data.[812] The FTC also has addressed the need for increased transparency and accountability of "data brokers."[813]

- *Internet of Things* – addressing the ability of ordinary objects to connect to the Internet and send and receive data – the "Internet of Things" – and the associated need for increased transparency, security, data minimization, and new forms of notice and choice.[814]

- *Mobile Privacy* – addressing the need for increased transparency, notice, and choices for mobile apps and online platforms,[815] and the privacy disclosure practices for mobile apps directed at children.[816]

- *Privacy-Protecting Technologies* – addressing emerging technologies and bridging the gap between the tech industry, the academy, and regulators. In recent weeks, the FTC convened "PrivacyCon" to, in the words of FTC Chairwoman Edith Ramirez, "deepen our ties to the academic and tech communities and ensure that the FTC and other policymakers have the benefit of work of leading thinkers in the privacy and data security arenas."[817]

The FTC conducts studies, issues reports, and testifies before Congress on legislative and regulatory proposals affecting consumer privacy and accountability.[818]

---

[812] FTC, *Big Data: A Tool for Inclusion or Exclusion?* (Jan. 2016), available at https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[813] FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014), available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[814] FTC, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[815] FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), available at https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[816] FTC, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

[817] Edith Ramirez, Chair, Fed. Trade Comm'n, Opening Remarks, PrivacyCon: An FTC Workshop (Jan. 14, 2016).

[818] FTC personnel have testified as experts before Congress on a number of privacy issues, including Do Not Track legislation (December 2010); Protecting Consumers' Privacy on Mobile Devices (May 2011); Protecting Consumers' Privacy (July 2011); Efforts to Protect Consumer Privacy (May 2012); Commercial Uses of Facial Recognition Technologies (July 2012); and Proposed Legislation Addressing Privacy and Security in Connected Automobiles (October 2015).

These studies, reports, and testimony are closely examined by industry and privacy professionals as policy statements that declare or shape the direction of FTC enforcement and, more generally, the protection of privacy in the US.

Most notably, the FTC's *Privacy Report* (2012) set out best practices for data controllers based on principles of privacy by design, enhanced consumer choice, and greater transparency.[819] Through such guidance and enforcement actions, the FTC has articulated and enforced a general right to privacy and data protection in the US.

State Privacy Enforcement And Common Law

US states enforce a broad range of laws designed to protect the right to privacy. They enforce unfair trade practice laws pursuant to state unfair and deceptive acts and practices laws patterned on the FTC Act. They also enforce data security requirements for sensitive personal information, and generally require data breach notification in the aftermath of data security incidents. In certain cases, states enable private plaintiffs to bring lawsuits and other actions to protect and enforce privacy rights. This combination of laws at the state level provides state Attorneys General, state officials, and private individuals with considerable ability to investigate complaints, initiate lawsuits or proceedings, enjoin the collection, processing or disclosures of personal information, extract monetary awards, and enter into settlements or consent decrees requiring data protection.

First, nearly every state has enacted what are referred to as "Little FTC Acts," statutes that prohibit unfair and deceptive acts or practices in terms identical or similar to the FTC Act.[820] Actions for alleged violations of these statutes rely on essentially the same theories as under the federal statute, namely, that prior statements regarding the processing of personal information (such as in a privacy policy) are deceptive, or that an act or practice is so egregious as to be unfair. These statutes empower state Attorneys General (and in some instances private plaintiffs) to bring independent enforcement actions, and they often do so by combining with other state Attorneys General in multi-state investigations.[821]

Second, almost every one of the 50 states has legislation that requires companies to implement information security measures. Data security laws generally require companies holding personal information about state residents to:

---

[819] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) (*2012 Privacy Report*), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[820] *See, e.g.*, Cal. Bus. & Prof. Code § 17200.

[821] The National Association of Attorneys General (NAAG) Consumer Protection Project, for instance, promotes information exchange between states regarding complaints, investigations, and enforcement actions, sometimes leading to multi-state actions. *See* NAAG, *Privacy in the Digital Age* (2013).

- implement and maintain reasonable security procedures and practices to protect the information from unauthorised access, destruction, use, modification, or disclosure;

- take reasonable steps to destroy personal information that is no longer to be retained or to make it otherwise unreadable or undecipherable; and

- contractually require third parties to whom the company discloses personal information to maintain reasonable security procedures.[822]

Some states impose more rigourous information security requirements. Massachusetts, for instance, requires entities to develop and implement a written comprehensive information security programme.[823] The regulation requires employee training, adoption of encryption standards, and regular monitoring and establishes requirements for securing computer systems.[824] These requirements are passed through to third-party vendors engaging in business with entities subject to the regulation.[825]

Third, data breach notification laws in 47 states require corporate and government entities to take particular actions in the event of a data security breach or suspected breach.[826] Once the notification threshold has been met, entities must notify state residents whose personal information was affected by a breach. Notice to law enforcement, consumer reporting agencies, and the state Attorney General or other regulators also may be required.

State privacy laws are enforced by a range of state and local entities. One state enforcement agency is the California Attorney General's Privacy Enforcement and Protection Unit. As part of the California Department of Justice, this unit enforces state and federal privacy laws, provides California residents with information on their rights and strategies for protecting their privacy, encourages businesses to follow best practices in privacy, and provides policy recommendations on related legislation.

---

[822] *See, e.g.*, Cal. Civ. Code § 1798.81.5 (2007); Md. Code Ann., Com. Law § 14-3503.

[823] Personal information is defined as the resident's name plus Social Security number, driver's license number or other state-issued identification number, or credit or debit card number, or other financial account number. This applies to electronic or paper data. *See* 201 Mass. Code Regs. § 17.02.

[824] *Id.* §§ 17.03–17.04.

[825] *Id.* § 17.03(2)(f). These requirements include (1) taking reasonable steps to select and retain third-party service providers capable of maintaining appropriate security measures; and (2) requiring that the third-party service providers by contract implement and maintain appropriate security measures for any personal information or data.

[826] *See, e.g.*, 815 Ill. Comp. Stat. 530/5, 530/10; N.Y. Gen. Bus. Law § 899-AA; Tenn. Code Ann. § 47-18-2107; Tex. Bus. & Com. Code § 521.053.

Finally, individuals are in some instances afforded private causes of action to protect their rights to privacy. Many state "Little FTC Acts" include private rights of action that can be used by deceived or unfairly injured individuals to redress privacy violations.

At the state levels, individuals also may seek to protect their privacy rights. State common-law systems recognise a web of privacy torts, including invasion of privacy,[827] public disclosure of private facts,[828] false light,[829] infringement of the right of publicity or likeness, appropriation,[830] and general negligence and misappropriation. These torts are widely recognised by state law, and individuals who have suffered legally recognised harm may assert such claims.[831] In some instances, damages for any of these torts can be expansive and include dignitary harms, mental distress, and special damages.[832]

Privacy On The Ground

The US privacy protection regime is also informed by practices on the ground. US companies and industry associations have developed privacy best practices, codes of conduct, and certification programs that build on recommendations and guidance from privacy regulators such as the FTC, but often exceed legal requirements.

These industry best practices often are memorialized in public-facing privacy policies. Even though there is no comprehensive law in the US that requires such policies, they have been so widely adopted that it would be a challenge to find a company website without one – and California law expressly requires such policies for companies that collect information online from that state's residents. Privacy policies have evolved as ways of competing on privacy, building customer goodwill, and protecting against litigation. In turn, these public commitments create an enforceable legal standard, as violations of privacy policies are litigated in breach-of-

[827] *See Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100–101 (E.D. Pa. 1996) (rejecting intrusion upon seclusion claim in the context of employer monitoring of employee e-mail).

[828] *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 852 (Cal. 1998).

[829] *Kolegas v. Heftel Broad. Corp.*, 607 N.E.2d 201, 209–210 (Ill. 1992).

[830] *Eastwood v. Superior Court*, 149 Cal. App. 3d 409, 417 (Cal. Ct. App. 1983).

[831] *See, e.g.*, J. Thomas McCarthy, *The Rights of Publicity and Privacy* §§ 3:1; 5:68; 5:123 (2d ed. 2015). Claims also may be asserted directly under a state constitution, such as in California, which recognizes a constitutional right to privacy. *See Sheehan v. S.F. 49ers, Ltd.*, 201 P.3d 472, 477 (Cal. 2009).

[832] Restatement of the Law (Second) of Torts § 652H (1977). Private plaintiffs in the US have pursued privacy violation claims in the state and federal court systems. For example, in March 2015 a federal judge gave preliminary approval to settle a class action litigation for $10 million brought by consumers against Target arising from the 2013 data breach in which up to 110 million consumers' personal data was potentially compromised, with payments up to $10,000 for each consumer. *See* Reuters, *Target WillPay $10 Million to Settle Lawsuit From Data Breach*, Fortune (Mar. 19, 2015). The wave of lawsuits a company can face after media reports of misuse of consumer data or a data security incident can serve as a strong deterrent.

contract claims and serve as a basis for deceptive practice cases brought by the FTC and state Attorneys General. The development of the regulatory "common law of privacy" through settlement or litigation outcomes in these cases then influence the terms of privacy policies as companies adjust their practices and disclosures in response.[833] The FTC also has influenced privacy practices by encouraging companies to honour "Do Not Track" browser signals and adopt other practices that promote privacy.[834]

The development of breach notification and data security laws also has had a profound impact on privacy and data protection practices. In the recent empirical study by the Berkeley Center for Law and Technology, US privacy managers unanimously described breach notification laws "as an important driver of privacy in corporations" that "called attention to the potential downstream effect of corporate treatment of consumers' information."[835] In addition to legislating issues of privacy and security, US legislators also influence corporate activities by conducting investigations, issuing letters of enquiry, conducting hearings, publishing reports, and introducing legislation. For instance, members of Congress issued detailed queries to data brokers[836] and car manufacturers[837] regarding cybersecurity protections and information collection practices.

Industry self-regulation of Internet advertising is a notable example of the interaction of public policy discussion and privacy practices. The Digital Advertising Alliance (DAA), National Advertising Initiative, and others have developed privacy principles for online advertising that encourage greater notice to consumers, promote consumer choice, and establish greater accountability. The DAA, for instance, promotes an "enhanced" form of notice.[838] It has developed an icon to provide a common means for its members to provide enhanced notice and a common means to opt out of behavioural advertising, the display of which indicates that the advertising company is engaged in interest-based advertising. By clicking on the icon, consumers can learn about interest-based advertising and the companies that may be engaged in interest-based advertising. The icon also links to a page where

---

[833] *See* Solove & Hartzog, *The FTC and the New Common Law of Privacy*, *supra* note 806, at 590–99.

[834] *See, e.g.*, FTC, *FTC Announces Agenda for Workshop Exploring Practices, Privacy Implications of Comprehensive Collection of Web Data* (Nov. 23, 2012), https://www.ftc.gov/news-events/press-releases/2012/11/ftc-announces-agenda-workshop-exploring-practices-privacy.

[835] Bamberger & Mulligan, *Privacy on the Ground*, *supra* note 734, at 71–72.

[836] Staff of S. Comm. on Commerce, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, 113th Cong. (2013).

[837] Sen. Edward J. Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (Feb. 2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[838] *See, e.g.*, DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

consumers can opt out of collection of personal information and delivery of targeted ads.

Industry associations also have taken steps to encourage consumer choice. Privacy principles state that companies may collect personal information for advertising purposes so long as an opt-out mechanism is provided.[839] Industry self-regulation can promote accountability even beyond hard legal obligations. DAA principles and practices require that at least one employee is responsible for ensuring compliance with privacy principles and that at least once per year, companies conduct an audit of compliance with industry standards.[840]

Other self-regulatory regimes can create a legally-binding effect on companies. The Payment Card Industry Data Security Standard (PCI DSS), for instance, is a set of technical, operational, and procedural requirements for secure processing of payment card data (debit and credit cards) promulgated by an organisation founded by major credit card companies.[841] The PCI DSS applies globally to all merchants and organisations that store, process, or transmit cardholder data. Compliance with these standards affect the various types of actions discussed thus far, such as FTC "unfairness" actions,[842] state data security enforcement actions,[843] and private plaintiff negligence claims.[844] These standards also are enforced contractually between merchants and their banks, and the contracts enable card brands to levy hefty fines for noncompliance.

Corporate practice and management has responded to the intricate web of state and federal privacy laws and regulations and the rise of self-regulatory programmes. A great many US companies have chief privacy officers even though no laws specifically require such a position,[845] and professional privacy associations such as

---

[839] *Id.*; DAA, *Application of Self-Regulatory Principles to the Mobile Environment* (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

[840] DAA*, Application of Self-Regulatory Principles to the Mobile Environment*, *supra* note 839.

[841] Payment Card Industry (PCI) Security Standards Council, *About Us*, https://www.pcisecuritystandards.org/organization_info/index.php.

[842] *See* Leslie Fair, *Wyndham's Settlement with the FTC: What It Means for Businesses – and Consumers* (Dec. 9, 2015) (noting that Wyndham's settlement with the FTC requires annual assessment of compliance with PCI DSS), https://www.ftc.gov/news-events/blogs/business-blog/2015/12/wyndhams-settlement-ftc-what-it-means-businesses-consumers.

[843] State Attorneys General may look to PCI DSS as a relevant industry standard that determines a "fair" business practice under state data security laws. Further, while generally a self-regulatory regime, the PCI standards are incorporated into statutory legal standards in at least one state law, in Nevada. Nev. Rev. Stat. § 603-1A.215.

[844] Private plaintiff suits may look to PCI DSS to establish a duty of care for negligence and other claims.

[845] The GLBA and HIPAA, however, require individuals to be responsible for the implementation of data security procedures.

the International Association of Privacy Professionals (IAPP) have emerged to train privacy professionals and inform industry practice. Since it was founded in the US in 2000, the IAPP has grown to over 25,000 members around the world, with the majority in the US. An IAPP membership survey found that US companies are "more likely" to mention the need to be a "good corporate citizen" than their European counterparts,[846] and "[p]rivacy practices in the U.S. are more likely to have certified decision-makers than their counterparts in the EU, with certification far more prevalent in large companies and mature privacy programs."[847]

IAPP also found that "U.S. firms are more likely than EU firms to be either in the Early or Mature stage of privacy" and devote a larger budget to privacy – US corporations devote more than twice as many resources than EU corporations.[848] Privacy-focused professionals occupy senior leadership positions in the majority of major US corporations. The recent empirical analysis by Berkeley scholars noted that "corporate structures frequently include direct privacy leadership, in many instances by C-level executives .... A community of corporate privacy managers has emerged. Ready evidence suggests that substantial effort is made to manage privacy."[849]

Article 25 (2) of Directive 95/46 provides that a decision about the adequacy of specific transfers can take into account "the professional rules and security measures which are complied with in that country." A comprehensive review of the US privacy legal regime, therefore, must extend beyond federal and state statutes and regulations to also include the prevailing practices that serve to further protect consumer privacy.

3.3.2 The Principles Of US Privacy Laws And Practices Correspond To The Basic Principles Under Directive 95/46

The Article 29 Working Party has articulated the essential elements of Directive 95/46 as purpose limitation, data quality and proportionality, transparency, security, access and rectification, and restrictions on onward transfer.[850] Mapping US privacy laws to these principles is complex because of the multiplicity of rules and jurisdictions involved. Nevertheless, consistent with the adoption of the Fair Information Practice Principles on both sides of the Atlantic, there are common themes in US and EU privacy laws and practices. In some aspects their application does not match up perfectly; in other aspects such as children's privacy, medical

[846] IAPP, *IAPP-EY Annual Privacy Governance Report 2015*, at 23 (2015), https://iapp.org/media/pdf/resource_center/IAPP-EY_Privacy_Governance_Report_2015.pdf.

[847] *See id.* at 6.

[848] *Id.* at 91–102.

[849] Bamberger & Mulligan, *Privacy on the Ground*, *supra* note 734.

[850] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand (Apr. 4, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp182_en.pdf.

privacy, financial privacy and data security, US laws go beyond those in the EU legal order. In addition, US rules for electronic communications and online marketing privacy may match or exceed those of the EU.

This section evaluates the US legal framework in light of principles identified by the Working Party. The examples of applicable laws are descriptive but not comprehensive as to the scope of each element within US privacy law. This comparison does not stand alone, because "any meaningful analysis" should take into account not only the content of laws but also "the system in place to ensure the effectiveness of such rules."[851] The US privacy regime and privacy practices on the ground together operate to ensure the fulfilment of EU data protection principles.

Purpose Limitation

> *The purpose limitation principle requires that data be processed for a specific purpose and subsequently used or disclosed only as not incompatible with the purpose of the transfer. The only exemptions are those necessary in a democratic society on one of the grounds listed in article 13 of the Directive (national security, defence, public safety, criminal proceedings, protection of the data subject, scientific research).*

US privacy laws restrict data processing to limit the collection and use of personal information. Sector-specific laws, such as HIPAA and GLBA, have often very strict secondary use restrictions. The FCRA requires recipients of consumer credit reports to specify and attest to the purpose for which they are requesting the data. And in a more general context, the FTC recommends that companies obtain express consent before collecting or using consumer information in ways that are inconsistent with the context in which such information is collected.[852] "For any data collection that is inconsistent with these contexts," the FTC states, "companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner—outside of a privacy policy or other legal document."[853]

The FTC also calls on companies to provide notice to consumers of material changes to their privacy policies.[854] Furthermore, any business that engages in commercial transactions with California residents online must post a privacy policy that states the purposes for which personal information is collected.[855] Any processing inconsistent with such purposes may be prosecuted as an unfair or deceptive practice.

---

[851] Article 29 Working Party, WP 12, Working Document on transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, p. 5 (adopted 24 July 1998).

[852] FTC, *2012 Privacy Report, supra* note 819, at ix.

[853] *Id.* at 27.

[854] *Id.* at 57–58; *In re Gateway Learning Corp.*, Docket No. C-4120 (FTC Sept. 10, 2004) (alleging, among other things, that Gateway Learning changed its privacy policy without providing notice or obtaining consent of consumers).

[855] Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579.

Financial Information

As noted above, the FCRA limits the use of information relating to creditworthiness, credit standing or capacity, character, general reputation, personal characteristics, and mode of living to a "permissible purpose." Such permissible purposes include those expressly authorized by the consumer, to facilitate a transaction initiated by the consumer, or as required by law. Under the GLBA, financial institutions may not share non-public personal financial information with third parties unless it previously offered the consumer an opportunity to opt out of such sharing and it has an agreement with the third party to keep shared information confidential. A financial institution may not disclose an account number or similar number for a consumer's credit card account, deposit account, or transaction account to any non-affiliated third party for marketing.

Health And Medical Information

HIPAA and HITECH authorise the collection and use of certain protected healthcare information for purposes that are essential to the provision of healthcare, including treatment, payment, and operations only. No data may be collected and used for any other purpose, including marketing, without the data subject's express written authorisation. HIPAA limits the disclosure of personal health information to the "minimum necessary" to accomplish the stated purpose of collection and use. Although a healthcare entity may disclose personal health information to a business associate (such as a billing company), it must ensure prior to disclosure that it has a valid contract with the business associate under which the associate is held to the same requirements as the healthcare entity. Ultrasensitive healthcare information is subject to even more stringent safeguards. Under separate legal requirements, employers and insurers are prohibited from requiring genetic testing or using genetic information as the basis for insurance premiums, employment decisions, or benefits coverage.

Electronic Communications Information

ECPA restricts the collection and use of communications information. It prohibits intentionally intercepting or divulging an "electronic communication," without consent or unless an exception applies. Section 222 of the Communications Act limits the use and disclosure of (and access to) information that relates to CPNI. Similarly, for example, consumer preferences evident from audiovisual media purchases and rentals are protected from disclosure under the VPPA absent informed written consent of the data subject. Laws in many states provide similar protections against interception or collection of personal electronic communications information.

Data Of Children And Students

COPPA sets limits on the collection and disclosure of children's personal information. For most purposes, website operators must obtain express, verifiable parental consent for use and disclosure of the personal information of children under age 13, and the purpose of the collection must be made clear to parents. State laws provide additional purpose limitations on data collection, use and disclosure. For

example, the Privacy Rights for California Minors in the Digital World Act restricts online companies from collecting personal data on, or marketing to, children who are not old enough to purchase the product. Other state laws limit the use of biometrics and student tracking devices, or provide for the protection and restricted disclosure of data collected through the use of such identification. SOPIPA restricts website operators and mobile application developers from developing profiles of students based on personal data and preferences, thereby establishing a strict purpose limitation on data collection. FERPA incorporates notice and consent provisions, and requires written consent for disclosure of such records with limited exceptions. PPRA similarly limits disclosure, and specifically incorporates sensitive data – such as political affiliation, religion, income level, mental health status, and sexual behaviour and attitudes, among others – into these limitations.

Data Quality And Proportionality

> *The data quality and proportionality principle requires that data should be accurate and, where necessary, kept up to date. The data should be appropriate, relevant, and not excessive in relation to the purpose for which it is transferred or subsequently processed.*

The FTC has developed and enforced the principles of data quality and proportionality. In its comprehensive statement of the right to privacy, the FTC declared that "[c]ompanies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy."[856] And the FTC has relied on this principle in bringing enforcement actions against companies that collect a disproportionate amount of information without demonstrating its relevance to the purpose and context of collection and adequately disclosing the collection practices.[857]

Principles of data quality and proportionality are also enforced through privacy policies. US privacy laws generally require data collectors to provide notice to consumers, usually through an online privacy policy, of the types of information collected by the entity, the purpose for the collection, and how the data is used and disclosed. Failure to disclose, or to limit collection in accordance with the disclosure, may be prosecuted as an unfair or deceptive act or practice, as well as direct violations of the law. These enforcement threats give data controllers an incentive to collect only appropriate and relevant information that is connected with the business purpose of the organisation and not excessive for the purpose for which it is collected. Data quality is also important in the US privacy regime. In addition to the notice requirements, a number of federal and state laws provide for access to and correction of personal information. It should be noted that a company's failure to comply with the terms of its online or published privacy policy could readily become

[856] FTC, *2012 Privacy Report*, *supra* note 819, at 30.

[857] *See, e.g.*, *In re Designerware, LLC*, Docket No. C-4390 (F.T.C. Apr. 11, 2013) (alleging that the collection of real-time location information, keystrokes, screenshots, and photographs from rented computers without notice or consent was an unfair business practice); *In re Sears Holding Mgmt. Corp.*, Docket No. C-4264 (FTC Aug. 31, 2009) (alleging that collection of all browsing information by an application was unfair because it was not sufficiently and prominently disclosed).

the subject of private litigation to the extent that individuals rely on and are injured by any such failure. Breach of contract claims could also discipline a company's failure to comply with promises or misleading statements communicated publicly or to the customers.

Financial Information

FCRA and FACTA protect consumers from disclosure of inaccurate and arbitrary personal information held by consumer reporting agencies, which is directly relevant to credit, employment or insurance decisions. FCRA requires any entity that ordinarily furnishes information to a consumer reporting agency to promptly notify the agency of any inaccuracies, corrections, or updates.[858]

Health And Medical Information

The HIPAA Security Rule requires covered entities and business associates to ensure the confidentiality, integrity, and availability of all electronic health information they collect and maintain. HIPAA and HITECH require implementation of administrative, physical, and technical measures to protect the integrity of health information. By imposing requirements to ensure data integrity, the HIPAA Security Rule is designed to ensure accuracy of data.

Electronic Communications Information

Section 222 of the Communications Act imposes limitations on the type of information telecommunications carriers may collect and requires telecommunications carriers to implement procedures to maintain the integrity of CPNI. The Cable Communications Act restricts the collection, use and disposal of data.

Data Of Children And Students

COPPA requires website and Internet operators that collect personal information of children under age 13 to maintain the accuracy and integrity of the personal information they collect. Such operators may only maintain personal information to fulfil the purpose for which it was collected, and operators must provide access to children's data for parents to ensure its accuracy.

[858] FCRA, 15 U.S.C. § 1681s-2(a)(1)–(2).

Transparency

> *The transparency principle requires that data subjects should be informed about the purpose for which data is processed and, when data is transferred onward, the identity of the processing controller in the third country, and any other aspect required to ensure fair treatment. The only exceptions are as stated in Articles 11(2) and 13 of the Directive.*[859]

US companies doing business online are generally expected to post data privacy policies publicly. In 1998, only two percent of websites had privacy policies; by 2000, "virtually all" of the most popular commercial websites had privacy policies.[860] Today, privacy practices of US businesses (and laws like California's statute requiring most businesses to post a privacy policy)[861] have spread the use of privacy policies throughout the marketplace. Commercial websites are expected to post plain, straightforward, and conspicuous online policies that explain the personal information collected, how it is processed and disclosed, and the choices consumers have regarding collection, use, and sharing. The FTC has recommended that privacy disclosures also be provided "just in time" and in the relevant context of the collection.[862] In many cases, federal and state enforcement actions are premised on the adequacy of disclosure and differences between a company's actual practices and the promises made regarding data collection, use, sharing, disclosure, and disposal practices.

Financial Information

In general, GLBA requires all financial institution to disclose and describe their privacy practices to consumers on an annual basis. The notice must state what information is collected, how it is used, to whom it is disclosed, and which disclosures may be controlled through consumer consent. FCRA requires consumer reporting agencies to provide detailed disclosures to consumers regarding the disclosure and use of personal data included in credit reports.

Health And Medical Information

HIPAA generally requires a detailed privacy notice describing the collection, use, and disclosure practices and enumerating individuals' rights regarding personal health

---

[859] Article 11(2) provides an exception for "processing for statistical purposes or for the purposes of historical or scientific research [where] the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law," requiring instead that member states provide "appropriate safeguards." Article 13 provides that member states may enact measures to restrict certain data subject rights for the purpose of national security, defense, public security, criminal investigations, "important economic or financial" interests of a member state, government enforcement of these activities, or the protection and rights of the data subject or other members of the public.

[860] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (May 2000).

[861] Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579.

[862] *See, e.g.*, FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* 15 (Feb. 2013).

information. Entities also must provide notice of any security breaches that reveal protected health information. Such disclosures are made publicly available on the HHS's website.

Electronic Communications Information

The Communications Act requires telecommunications carriers to provide annual CPNI compliance certifications and to disclose complaints of unauthorised disclosures. The Cable Communications Act requires cable operators to provide annual privacy notices personal data processing and consumers' rights to access, correct and delete their data.

Data Of Children And Students

COPPA generally requires website operators that collect children's personal information to post a children's privacy policy and provide direct notice to parents of personal data processing. Educational institutions must provide annual notice to students and their parents regarding their personal data processing under both FERPA and PPRA.

Security

> *The security principle requires adoption of appropriate technical and organizational measures against risks presented by processing and restrictions against processing except on instructions from the controller.*

Data security is an area where the US indisputably goes beyond measures in the EU. While the EU is finalizing adoption of a new General Data Protection Regulation that will apply data breach notification requirements, the US has had data breach notification laws in place for more than a decade.

California was the first state to enact such a statute in 2003. Such safeguards are now incorporated in the GLBA (financial data), HIPAA (healthcare data), the Communications Act (telecommunications data), and 47 state laws, plus the laws of numerous US territories and the District of Columbia (for broad categories of sensitive personal information). The laws generally require notification to individuals of incidents in which their personal information has been compromised, and often require direct notification to a regulator.

Generally state laws apply to "personal information" like the consumer's name, plus other identifying information (such as Social Security number, driver's license number, medical information). The state laws identify the data controllers (companies and governmental entities) covered by the law, as well as the notice requirements (to whom and when notice must be given) and any exemptions (such as for encrypted data). As discussed above, a significant effect of these widespread data breach laws is to promote a high degree of awareness of the governance and care of personal information. Many states, in response to highly-publicized data breaches, recently have amended their data breach laws to sweep in more personal data, establish minimum encryption standards, and require implementation of risk-

based information security programs.[863] Many states also permit private redress for data breaches under other laws, and many of these are brought as class action lawsuits.

Further, the federal Computer Fraud and Abuse Act,[864] the federal Identity Theft and Assumption Deterrence Act of 1988,[865] and multiple state laws criminalize unauthorised access of computer systems and identity theft.[866] These laws impose punishments of incarceration, forfeiture, restitution, and payment of attorneys' fees to the victim.

The US government also has focused attention on cybersecurity. Across the financial, critical infrastructure, communications, and other sectors, federal and state agencies have issued directives that require the implementation of comprehensive information security programs and compliance with detailed security requirements regarding the handling of sensitive personal information. At the encouragement of government, industry has gravitated towards implementation of a cybersecurity framework developed by the National Institute of Standards and Technology (NIST),[867] and US industries have deployed more robust and sophisticated practices to combat the threat of cyber attacks.

Financial Information

The GLBA Safeguards Rule requires financial institutions to protect the security and confidentiality of their customers' non-public personal information and implement a written information security plan. Each financial institution must designate an employee to coordinate its information security programme, conduct a risk assessment, and contractually obligate service providers to maintain safeguards. The FACTA Red Flags Rule requires financial institutions and other entities to develop programs that identity and respond to theft of personal information. Financial regulatory agencies – including the SEC, CFPB, Commodity Futures Trading Commission, the New York State Department of Financial Services, and state insurance regulators, just to name a few – have focused on cybersecurity regulatory enforcement.

Health And Medical Information

The HIPAA Breach Notification Rule imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of personal health

---

[863] *E.g.*, Cal. Civ. Code 1798.29 (SB-570); Conn. Pub. Act No. 15-142; Mont. H.B. 74; N.H. H.B. 322; Nev. A.B. 179; N.D. S.B. 2214; Or. S.B. 601; R.I. Identity Theft Protection Act of 2015 (SB134); Wash. H.B. 1078; Wyo. S.F. 35 & S.F. 36.

[864] 18 U.S.C. § 1030 *et seq*.

[865] *Id.* §§ 1028, 1028A.

[866] *E.g.*, Cal. Penal Code § 368 ("Crimes Against Elders, Dependent Adults and Persons With Disabilities").

[867] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

information. HIPAA also has a Safeguards Rule that requires entities to maintain administrative, physical, and technical safeguards to ensure the confidentiality, integrity and security of health information. It also requires that each entity identify a privacy official responsible for implementing privacy protections. The HITECH Act further promotes security by incentivizing covered entities to use encryption. In recent years, HHS has levied millions of dollars in fines (and in some cases referred criminal charges to the Department of Justice) against hospitals, health care providers, insurance companies, and pharmacies.

Electronic Communications Information

The Communications Act requires telecommunications carriers to implement data security protections for personal information. It requires notification of data breaches involving CPNI, and the FCC has interpreted the Communications Act to impose more general cybersecurity requirements regarding the handling of all sensitive personal information.[868] By regulation, the FCC extended these protections to personal information collected and maintained by Internet service providers.

Data Of Children And Students

COPPA imposes requirements on website operators to maintain confidentiality, integrity and security of child's personal information. SOPIPA requires data security measures and deletion upon request of the student.[869]

Access, Rectification And Opposition

> *The principle of rights of access, rectification and opposition state that an individual is entitled to a copy of all data relating to him or her, and the right to rectify any data that is inaccurate. In certain circumstances, the individual should be able to oppose having his or her data processed, subject only to the exceptions in Article 13 of the Directive.*

Although federal and state laws do not provide for the data subject's access to personal information held by companies in all circumstances, numerous statutes involving sensitive data provide for access as well as disclosures of what is collected and ways to correct errors or request deletions.

---

[868] *See, e.g.*, *In re TerraCom, Inc. & YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, FCC 14-173 (FCC Oct. 24, 2014).

[869] Data covered by SOPIPA includes but is not limited to information in the student's educational record or email, first and last name, home address, telephone number, email address or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliation, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information. Six states (Arkansas, Delaware, Georgia, Maryland, New Hampshire, and Oregon) passed similar laws in 2015.

Financial Information

FCRA requires that data collected by credit agencies be accurate and relevant, and provides mechanisms for data subjects to review and dispute the data collected. FACTA provides data subjects the right to obtain free copies of credit reports annually. Many state laws also cover consumer reporting information and require data subjects be provided rights of notice, access and correction.

Health And Medical Information

The HIPAA Privacy Rule provides data subjects the right to access their records, seek correction, and receive information regarding disclosures of their personal health information.[870] Although entities retain the right to deny a request for amendment in limited circumstances, HIPAA requires covered entities to include the individual's statement of disagreement or the individual's request for amendment with any subsequent disclosures of protected health information.[871] State laws relating to health records also permit access to and correction of records. California's law is typical of these in restricting access by unauthorised persons to birth and death records, sensitive testing records (such as HIV tests), psychiatric records, and medical records. It also guarantees patients' rights to see, copy, and correct health records pertaining to them.

Electronic Communications Information

The Cable Communications Act provides for data subjects' access to their personal information and the right to correct any such data. Consumers' personal content rental preferences, including audiovisual media and reading material, are protected against processing absent express consent. The VPPA provides strong protections against such disclosure, including a requirement that any consent be re-obtained every two years.

Data Of Children And Students

COPPA requires each website operator provide parents access to, and ability to delete, their children's personal information. The website operator must also give parents the opportunity to opt out of future data processing. FERPA ensures that students or the parents of underage students control access to their educational records and the right to correction.

[870] HIPAA 45 C.F.R. § 164.526(a)(1).

[871] *Id.* § 164.526(d)(5).

Restrictions On Onward Transfers

> *The onward transfers restriction principle states that successive transfers of personal data from the destination country to another country is permitted only if the third country ensures an adequate level of protection, subject only to the exceptions in Article 26 paragraph 1.*

Generally, federal and state law do not distinguish between data that is transferred within the US and data that is transferred outside the country, and thus do not separately address onward transfers to other countries. Nevertheless, the restrictions on data sharing and disclosures within each sector-specific laws, the need to adhere to use limitations and other commitments in privacy policies, and data security and breach laws discussed above operate to limit transfers to third parties. These restrictions also serve to limit onward transfers to foreign jurisdictions. In general, the transferring company or organisation retains legal responsibility for the personal data it transfers to third parties – whether they are in the US or otherwise.

Heavily regulated entities, like financial firms, are under particular obligations to scrutinise and monitor the suitability of third parties to which they transfer personal data. GLBA and Massachusetts law, for example, require onward transfer contracts for personal data provided to third parties.[872] While foreign transfers are not prohibited, banking agencies in particular have noted that extra due diligence may be appropriate where the transferee is located in a foreign jurisdiction. The FTC also has held companies responsible for the practices of third parties to which a company has transferred personal data.[873]

The US has further taken steps to provide compliance mechanisms for companies subject to onward data transfer restrictions imposed by other countries. In addition to the provisions within each law for general onward transfer of data, businesses in the US are also subject to compliance with the EU-US Safe Harbour Framework,[874] the US-Swiss Safe Harbour Framework, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system. The FTC's Office of International Affairs works with consumer protection agencies globally, including APEC and the Global Privacy Enforcement Network, to promote cooperation, combat cross-border fraud, and develop best practices. Organizations that operate under the 2000 Safe Harbour Framework must apply the notice and choice provisions of the framework before disclosing covered information to a third party which will be a controller of that information. The organisation must provide notice and obtain consent unless

---

[872] *See* Office of Comptroller of the Currency, US Dept. of the Treasury, *Third Party Relationships: Risk Management Guidance*, OCC Bulletin 2013-29 (Oct. 20, 2013); 201 C.M.R. § 17.03(f).

[873] *See, e.g.*, *In re GMR Transcription Services, Inc.*, Docket No. C-4482 (F.T.C. Jan. 31, 2014) (alleging that a company failed to "adequately verify that their service provider … implemented reasonable and appropriate security measures to protect personal information ... on [the service provider's] network and computers").

[874] Companies that certify to the US Department of Commerce their adherence to the Safe Harbour Framework are subject to FTC enforcement of their public commitments to their customers even though the CJEU has invalidated the Framework from the standpoint of EU law.

transferring data to an affiliate whose practices are deemed "adequate" or who contractually agrees to provide the same level of privacy as set out in the Framework.

3.3.3 An Effective System Of Enforcement And Compliance Ensures Effective Application Of These Principles

According to WP 12, the objectives of a data protection system are (1) to deliver a good level of compliance with the rules; (2) to provide support and help to individual data subjects in the exercise of their rights; and (3) to provide appropriate redress to the injured party where there is noncompliance.[875] The US privacy protection regime, which combines enforcement of broad privacy protections by the FTC and state Attorneys General together with sector-specific regulations, establishes a comprehensive privacy protection regime that fulfils these objectives.

Good Level Of Compliance With Rules

> *A good system is generally characterised by a high degree of awareness among data controllers of their obligations and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for the rules, as can systems of direct verification by authorities, auditors or independent data protection officials.*

Compliance with rules is motivated by the significant enforcement authority wielded by the FTC and other federal and state regulators. The FTC alone has levied more than 40 privacy lawsuits, 50 data security cases, 100 credit-reporting cases, 130 spam and spyware cases, 25 cases for violations of privacy notice and security requirements, 20 cases relating to collection of data from children, and 100 cases enforcing consumers' rights to be left alone from telemarketers.[876] As discussed above, the FTC also enforces voluntary promises made by participating organisations and has brought numerous cases relating to the US-EU Safe Harbour Framework. The FTC also acts as a privacy enforcement authority for the US in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system.[877] These enforcement actions have been against data controllers of all sizes, from tech giants to small start-up companies. Collectively, the FTC's cases have imposed nearly $200 million in civil penalties and more than $1 billion in redress or disgorgement.[878]

---

[875] *See* European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (Jul. 24, 1998).

[876] FTC, *2014 Privacy and Data Security Update*, *supra* note 810.

[877] *Supra* Part 3.3.1 ("The Federal Trade Commission").

[878] *Id*.

More recently, additional federal regulators have increased their profiles as regulators of privacy and data security, including the FCC and SEC. The SEC's authority over publicly-traded companies, and recent announcements about their examination priorities as well as statements about material disclosures regarding risks to data, have greatly expanded attention to privacy and cybersecurity compliance from management and corporate boards.[879]

Compliance with the rules is also motivated by businesses themselves through voluntary commitment to best practices and self-regulatory principles. Many businesses – mostly by choice rather than legal obligation – have privacy officers whose primary responsibility is to ensure compliance with state and federal data privacy and security laws as well as best practices.[880] Such individuals are generally responsible for the organisation's data privacy and security practices and procedures.[881] These individuals commonly look beyond the letter of the law to develop practices that anticipate best practices, government data management policy guidance, and requirements imposed in enforcement actions.[882] Such managers credit the deterrent threat and unpredictability of enforcement actions by the FTC and state consumer protection officials, as well as the expectations of consumers with the development of policies and practices that exceed the requirements of law.

As an additional layer of privacy protection, industry stakeholders have worked with government and privacy advocates to build a number of co-regulatory and self-regulatory initiatives that adopt domain-specific, robust privacy protections enforceable by the FTC and state Attorneys General. Examples of these accountability programs include the About Advertising icon by the DAA, the opt-out for cookies set forth by the Network Advertising Initiative, and the Children's Privacy Seal Program.[883] Some laws incorporate self-regulatory programs as part of the multi-faceted compliance scheme. For example, COPPA permits self-regulation by industry groups whose compliance programs have been approved by the FTC as providing equal or greater protection for children, with mandatory mechanisms for assessing compliance and incentives for complying.[884] Under these programmes, organisations will report violations that have not been corrected to the FTC.

The multi-level attention to consumer privacy – at the data controller level, through oversight by federal and state agencies, federal and state enforcement actions, consent decrees, and the imposition of punitive sanctions and decades-long

---

[879] *See, e.g.*, SEC Office of Compliance Inspections and Examinations, *OCIE's 2015 Cybersecurity Examination Initiative* (Sept. 15, 2015).

[880] *Supra* Part 3.3.1 ("Privacy On The Ground").

[881] *Id*.

[882] Bamberger & Mulligan, *PRIVACY ON THE GROUND*, *supra* note 734.

[883] *Supra* Part 3.3.1 ("Privacy On The Ground").

[884] *See, e.g.*, Children's Advertising Review Unit, *Self-Regulatory Program for Children's Advertising* (2009).

oversight, and private litigation, as well as the negative publicity effect of media reports – combine to create an environment of strong privacy protection in the US.

Support And Help For Data Subjects

> *The individual data subject must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost, including through institutional mechanisms allowing independent investigation of complaints.*

Consumers have numerous mechanisms to enforce their rights and seek assistance. As an initial matter, many federal and state laws require data controllers and processors to provide information regarding the information being collected, the process for seeking additional information and for filing any complaints.[885] For example, data subjects have the right under FACTA to receive an explanation of their credit scores and receive free annual credit reports. And under FCRA, data subjects have the right to dispute credit information and seek correction. The right to review and seek correction of personal information also exists under COPPA for children's information, HIPAA for health information, and other federal and state statutes and regulations.[886]

Many other federal and state agencies have similar mechanisms for collecting complaints about privacy concerns and providing mechanisms by which consumers may increase the protection rights. Telephone customers, for instance, may register their telephone numbers on the National Do Not Call Registry in order to restrict telemarketers from contacting them on that telephone number at home.[887] If a telemarketer contacts a consumer on a registered telephone number after an initial grace period, then the consumer may file a complaint on a website dedicated to this process.

In addition, federal and state enforcement agencies provide a process by which consumers may alert agencies of potential issues or violations. For instance, HHS's Office of Civil Rights has the authority to assess penalties for violations associated with HIPAA, and consumers may lodge complaints with OCR. Similarly, consumers may lodge complaints with the FTC regarding the data collection practices of a regulated company. The FTC has a complaint website that provides consumers with an easy mechanism for lodging complaints.[888] The FTC's website provides a mechanism to lodge a general complaint about how a company is handling personal information, as well as separate mechanisms for complaints regarding identity theft, scams and rip-offs, unwanted telemarketing, texts and spam, mobile devices and telephones, internet services, online shopping, computers, education, jobs, credit and debt, and other issues. The FTC provides notice that it does not resolve individual complaints but does provide information on the next steps that a consumer should take. State Attorneys General offices also have easy mechanisms for

---

[885] *Supra* Part 3.3.2 ("Transparency" and "Access, Rectification And Opposition").

[886] *See id*.

[887] FTC, *National Do Not Call Registry*, http://www.donotcall.gov.

[888] FTC, *FTC Complaint Assistant*, available at https://www.ftccomplaintassistant.gov/.

individuals to file privacy and other consumer-related complaints against companies.[889]

Redress And Compensation

> *The redress element must involve a system of independent adjudication or arbitration that allows compensation to be paid and sanctions imposed where appropriate.*

The US privacy regime provides mechanisms of redress to injured parties for violations. The system of privacy governance includes the enforcement muscle of the FTC, the FCC, the SEC, the CFPB, the HHS, the Office of the Comptroller of the Currency, the Commodity Futures Trading Commission, the Department of Education, state Attorneys General, and other federal and state entities. The Department of Justice also may bring criminal enforcement actions and seek imprisonment for violations of the Computer Fraud and Abuse Act, Privacy Act, HIPAA, ECPA, and other statutes. This system permits a variety of flexible enforcement alternatives.

The FTC is the most influential data protection agency in the US because it oversees such a wide range business conduct affecting consumers and imposes coercive corrective action as well as significant fines.[890] The case against Google for allegedly misrepresenting its privacy practices and circumventing the cookie settings of the Safari internet browser is a paradigm of tough enforcement by the FTC and state Attorneys General. In that case, the FTC obtained a settlement payment of $22.5 million from Google, and a consortium of nearly 40 state Attorneys General received an aggregate settlement payment of $17 million.[891] Through these enforcement mechanisms and the independent authority of US federal and state entities to investigate, levy fines, and seek redress, consumers are afforded privacy protections and, when appropriate, compensation.

The common law system recognizes a web of common law torts, including invasion of privacy, disclosure of public facts, showing the individual in a false light, appropriation or infringement of the right of publicity or personal likeness, and general misappropriation or negligence. Common law privacy torts include invasion of privacy,[892] public disclosure of private facts,[893] false light,[894] infringement of the

---

[889] *See, e.g.,* California, Complaint Submission Page, https://oag.ca.gov/contact/consumer-complaint-against-business-or-company; Massachusetts, Complaint Submission Page, http://www.mass.gov/ocabr/government/oca-agencies/dob-lp/file-a-complaint.html.

[890] *Supra* Part 3.3.1 ("The Federal Trade Commission").

[891] *See* FTC, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012); N.Y. Off. of Att'y Gen., *A.G. Schneiderman Announces $17 Million Multistate Settlement With Google Over Tracking Of Consumers* (Nov. 18, 2013).

[892] *See Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100–101 (E.D. Pa. 1996) (rejecting intrusion upon seclusion claim in the context of employer monitoring of employee e-mail).

[893] *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 852 (Cal. 1998).

right of publicity or likeness, appropriation,[895] and general negligence and misappropriation. These torts are widely recognized by state law.[896] Damages for any of these torts can be expansive and include dignitary harms, mental distress, and special damages.[897]

The plaintiffs' bar in the US vigilantly pursues privacy violation claims in the state and federal court system. For example, in March 2015 a federal judge gave preliminary approval to settle a class action litigation for $10 million brought by consumers against Target arising from the 2013 data breach in which up to 110 million consumers' personal data was potentially compromised, with payments up to $10,000 for each consumer.[898] The wave of lawsuits a company can face after media reports of misuse of consumer data or a data security incident is a strong deterrent.

These common law torts described above[899] help protect the collection, use, and potential abuse of personal data and can provide injured private parties with the right to bring actions against companies in the US. The common law from which Louis Brandeis and Samuel Warren derived a right to privacy in 1890 continues to evolve from covering the then-new technology of mobile photography to ever newer technologies that implicate personal data.

---

[894] *Kolegas v. Heftel Broad. Corp.*, 607 N.E.2d 201, 209–210 (Ill. 1992).

[895] *Eastwood v. Superior Court*, 149 Cal. App. 3d 409, 417 (Cal. Ct. App. 1983).

[896] *See, e.g.*, J. Thomas McCarthy, *The Rights of Publicity and Privacy* §§ 3:1; 5:68; 5:123 (2d ed. 2015). Claims also may be asserted directly under a state constitution, such as in California, which recognizes a constitutional right to privacy. *See Sheehan v. S.F. 49ers, Ltd.*, 201 P.3d 472, 477 (Cal. 2009).

[897] Restatement of the Law (Second) of Torts § 652H (1977).

[898] *See* Reuters, *Target WillPay $10 Million to Settle Lawsuit From Data Breach*, FORTUNE (Mar. 19, 2015).

[899] *Supra* Part 3.3.1 ("State Privacy Enforecement And Common Law").

CONCLUSION

This in-depth comparison of the legal orders for privacy and data protection in the European Union and the United States shows that the level of protection for data that is transferred from the EU to the US is essentially equivalent to the level of protection of personal data in the EU.

With respect to government surveillance, the judgments of the ECtHR make clear that the key to ensuring proportionality is to have safeguards against abuse. The US applies such safeguards to surveillance under the intelligence programs that affect the data of EU citizens stored in the US by the use of defined selection terms, and steps taken by both the President and Congress to extend the elaborate system of existing US safeguards to EU citizens. Under principles deeply embedded in the US legal order and political system, surveillance is constrained by a further array of safeguards including – specific limitations on purpose, on use and retention of data, *ex ante* and *ex post* review by neutral judges and other independent authorities, and available redress.

These safeguards ensure that this surveillance is proportionate and within the range permitted and necessary in a democratic society. Given the greater level of independent judicial involvement in approving surveillance orders, the range of transparency obligations imposed by law upon the intelligence agencies, and the extensive array of oversight mechanisms in place in the US, safeguards in the US legal order are in general more protective than those in effect in the EU – and, taken as a whole, they are certainly at least essentially equivalent to the legal order in the European Union.

With respect to privacy and data protection in the commercial sector, the layers of federal and state sectoral protections for sensitive data, active and broad enforcement of privacy and security obligations, common law remedies and litigation, the public commitments to industry self-regulation in the US, and the empirical comparison of the practices of privacy managers in US and EU companies provides concrete evidence that the US legal order is as effective *in practice* as the level of protection under Directive 95/46.

This report accordingly provides a substantive basis for the European Commission to make the findings required by the *Schrems* judgment in order to approve a new, strengthened transatlantic data transfer framework, especially where companies bind themselves to adhere to the basic principles of the Directive. In addition, because the EU and US legal orders are essentially equivalent, the European Commission should formally recognise under Article 25(6) that data subjects in the EU and US have comparable privacy rights. Such recognition would establish the most straightforward legal basis to comply with the EU's WTO trade obligations and facilitate transatlantic data flows and mitigate the disruption of global commerce and cooperation that continues in the wake of the *Schrems* decision. Such a recognition can readily be predicated upon a conscientious analysis of the law and practices in both the US and the EU.

The comparison for individualised adequacy determinations under Article 25(2), is specific to the laws and practices applicable in Member States rather than the EU

legal order as whole. However, no decision-makers may *assume* – without specific and verified evidence – that particular data flows from the EU to the US will effectively reduce the level of protection for data subjects in a Member State, nor could they conclude that a transfer to the US in a specific situation will lower the level of protection without evidence that the level of protection in the exporting Member State itself meets the EU Benchmark. This report furnishes evidence to the contrary and provides a basis on which in individual cases a supervisory authority or national court can find that the level of privacy and data protection in the US is equivalent to that in a particular Member State.

ABOUT THE AUTHORS

Sidley Austin LLP is a premier global law firm celebrating its 150th anniversary in 2016. With 1,900 lawyers and 19 offices worldwide, the firm provides a broad range of services to meet the needs of large and small businesses and other organizations across a multitude of industries, forums and governments. Sidley has a broad transactional practice and consistently ranks among the top global capital markets firms. Sidley also has an extensive litigation and arbitration practice, spanning nearly every area of substantive law. The firm also provides regulatory counseling and advocacy regarding communications, energy, environmental, food, drug and device, healthcare, insurance, Internet, life sciences, financial and securities law, and represents clients in virtually every major industry. Sidley is rated among the top law firms, recognized in the United States and globally for service and responsiveness, and widely recognized for its pro bono and diversity programs.

Sidley's Privacy, Data Security and Information Law practice group is a global and interdisciplinary team of lawyers focused on a broad range of emerging issues, including privacy and data protection; cybersecurity and data breach preparedness and response; Big Data; government surveillance; data localization; Internet law; cross-border data flows; and e-Commerce. The group handles litigation and investigations, cybersecurity compliance and regulatory counseling, data breach incident response, legislative and policy developments and sector-specific counseling internationally. Clients cover a broad range of industries. The practice and its lawyers consistently rank in the top tiers of *Chambers USA, Chambers Global*, and *The Legal 500*.

Jacques Bourgeois
Senior Advisor
Brussels
jbourgeois@sidley.com
+32 2 504 6490

Jacques Bourgeois is senior adviser in Sidley's Brussels office. He is a recognized authority on European Union (EU) law, with over four decades of experience in private practice and public service. Prior to joining Sidley, Jacques served for over 25 years as a senior official with the European Commission, where he was the principal legal adviser of the Commission in charge of foreign trade policy and, later, antitrust policy. Previously, he served for several years as head of the Trade Policy Instruments Division in the Directorate-General for External Relations. Since 2006, he has served as Chairman of the Competition Commission advising the Belgian government. He advises Sidley lawyers and clients around the globe on all aspects of EU law. He is also a professor at the College of Europe in Bruges and a guest professor at the University of Ghent.

Cameron F. Kerry
Senior Counsel
Boston
ckerry@sidley.com
+1 617 223 0305

Cameron F. Kerry is senior counsel in Sidley's Boston and Washington, D.C. offices. He is former General Counsel and Acting Secretary of the United States Department of Commerce, where he played a leadership role in consumer privacy issues and the flow of information and technology across international borders, including on the EU-U.S. Safe Harbour Framework. Cam is also a visiting scholar with the MIT Media Lab and a frequent speaker and writer on privacy and the digital economy. At Sidley, his broad practice operates at the intersection of law, technology and public policy, and is informed by his years of government service and more than three decades in private practice.

William Long
Partner
London
wlong@sidley.com
+44 20 7360 2061

William Long is a partner in Sidley's London office. He advises international clients on a wide variety of data protection, privacy, information security, social media, e-Commerce and other regulatory matters. William is on the DataGuidance panel of data protection lawyers and is a contributing author on a number of books, including leading legal text books published by BNA in the areas of privacy, cloud computing and the use of health data. He also co-authored a major global survey of Privacy, Data Protection and Cybersecurity law covering 62 international jurisdictions published by Law Business Research. William has been interviewed widely for his thought leadership and writes for a number of publications, including *Data Protection Law & Policy*, *Computer Weekly* and *CIO Today*.

Maarten Meulenbelt
Partner
Brussels
mmeulenbelt@sidley.com
+32 2 504 6467

Maarten Meulenbelt is a partner in Sidley's Brussels office. He has extensive litigation experience before the EU Courts, national courts and competition authorities, the European Commission and national regulatory authorities in several EU Member States with a specific focus on the life sciences sector. He is a member of Sidley's Privacy, Data Protection and Information Law, Global Life Sciences and Antitrust practices focusing on EU regulatory affairs, litigation and competition law issues affecting clients in Europe.

Alan Charles Raul
Partner
Washington, D.C.
araul@sidley.com
+1 202 736 8477

Alan Charles Raul is a partner in Sidley's Washington, D.C. office and the founder and leader of Sidley's Privacy, Data Security and Information Law practice. While practicing law at Sidley, Alan served as Vice Chairman of the Privacy and Civil Liberties Oversight Board and, prior to joining Sidley, he served as Associate Counsel to the President, General Counsel of the Office of Management and Budget and General Counsel of the U.S. Department of Agriculture. He represents a wide range of companies on federal, state and international privacy issues and litigation. He is a prolific writer and speaker on privacy, cybersecurity and related issues.

SIDLEY
150 YEARS

sidley.com

AMERICA • ASIA PACIFIC • EUROPE

MN-2984-01/16