STUDY

Requested by the LIBE committee

European Parliament

Exchanges of Personal Data After the Schrems II Judgment

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 694.678– July 2021

EN

Exchanges of Personal Data After the Schrems II Judgment

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, examines reforms to the legal framework for the exchange of personal and other data between the EU and the USA that would be necessary to ascertain that the requirements of EU law are satisfied and that the rights of EU citizens are respected, following the Schrems II judgment of the EU Court of Justice.

This document was requested by the European Parliament's Committee on Civil Liberties (LIBE).

AUTHORS
Ian BROWN, Visiting CyberBRICS professor at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro, Brazil
Douwe KORFF, Emeritus Professor of International Law, London Metropolitan University, UK

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Monika LAZARUK
Christina KATSARA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in July 2021

This document is available on the internet at:
http://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
BCRs	Binding Corporate Rules for data transfers
CDT	Center for Democracy and Technology
CFR	(EU) Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
CRS	(US) Congressional Research Service
DMA	Digital Markets Act
DSA	Digital Services Act
ECHR	European Convention on Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EEGs	European Essential Guarantees for surveillance
E.O. 12333	(US) Executive Order 12333
FISA	(US) Foreign Intelligence Surveillance Act
FISC	(US) Foreign Intelligence Surveillance Court
FTC	(US) Federal Trade Commission
GDPR	(EU) General Data Protection Regulation
ICCPR	(UN) International Covenant on Civil and Political Rights
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
OLC	(US Department of Justice) Office of Legal Counsel
OTI	(US) Open Technology Institute

PCLO	(US) Privacy and Civil Liberties Officer
PCLOB	(US) Privacy and Civil Liberties Oversight Board
PPD-28	(US) Presidential Policy Directive 28
SCCs	Standard Contractual Clauses for Data Transfers
TEU	Treaty on European Union
UDAP	Unfair and Deceptive Acts and Practices

LIST OF TABLES

ACKNOWLEDGEMENTS

The authors thank Professors Graham Greenleaf, Chris Hoofnagle, Andrea Matwyshyn and TJ McIntyre and Dr Thorsten Wetzling for their comments on earlier drafts, and also Ashley Gorski, Greg Nojeim and Prof. Peter Swire for advice on the recent *TransUnion* Supreme Court judgment.

EXECUTIVE SUMMARY

Introduction

On 16 July 2020 the Court of Justice of the European Union (CJEU) invalidated the Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US "Privacy Shield" agreement, concerned US government surveillance powers are not limited as required by EU law, and that EU persons do not have effective means of redress. The judgment upheld the validity of standard contractual clauses to allow data transfers under the General Data Protection Regulation (GDPR), but requires data controllers to assess the level of data protection in the recipient's country and to adopt "supplementary measures" if needed.

In this context the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) requested this study on reforms to the legal framework for the exchange of personal and other data between the EU and the USA to ensure EU law requirements are satisfied and EU citizens' rights are respected.

European data protection standards

In the EU, data protection is **a fundamental right**, enshrined in primary law. While activities of Member State authorities for national security purposes are outside EU competence, national constitutions and the European Convention on Human Rights apply. Moreover, the exemption does not apply to the imposition of legal obligations on private sector organisations, or to non-EU countries.

Under the GDPR, personal data can only be freely transferred to countries held by the European Commission to provide **"adequate"/"essentially equivalent" protection**. Otherwise, "appropriate safeguards" must be adopted by the EU data exporter. A third country's laws can only be said to provide such protection if they meet the standards set out in the European Data Protection Board (EDPB) Adequacy Referential. And in relation to access to personal data by a third country's intelligence agencies, its laws can only be said to provide this protection if they meet the standards set out in the EDPB's European Essential Guarantees for surveillance. Both documents fully reflect the CJEU's case law.

US privacy and surveillance laws

A US Congressional Research Service review found a "patchwork" of federal data protection laws which "primarily regulate certain industries and subcategories of data." The rather limited protections accorded to "US persons" by the Fourth Amendment are largely non-existent in relation to non-US individuals outside the USA, while "privacy torts" are too limited to even compare to EU data protection concepts.

The Federal Trade Commission (FTC) Act gives powers to the FTC to act against "unfair or deceptive acts or practices" by most commercial entities. Companies are bound by their data privacy and security promises, and certain privacy practices are held to be unfair. However, these broad principles cannot be relied on to read all of the many detailed requirements of EU data protection law into US law – in particular, a private right of action.

Several broad federal privacy bills have been introduced to Congress since 2019, and the House of Representatives Energy and Commerce Committee staff have produced a "bipartisan discussion draft." While such legislation would offer very significant improvements in protection of personal data, as currently drafted, none of them achieve "essential equivalence" to the GDPR.

Consumer privacy bills have been passed or introduced in dozens of the individual states. California's Privacy Rights Act (CPRA) (which will enter fully into force in 2023) is closest to the GDPR, but still falls

short of "essential equivalence" in scope and exceptions. Nor is it likely any other US state will adopt a law going beyond the CPRA.

The Foreign Intelligence Surveillance Act (FISA) regulates US national security and foreign intelligence-related electronic surveillance. Outside the US, electronic surveillance activities of the US intelligence community targeting non-US persons are generally governed by Executive Order 12333. Presidential Policy Directive 28 (PPD-28) contains limits on the use of signals intelligence collected in "bulk" by the intelligence community. **The CJEU invalidated the Privacy Shield adequacy decision because FISA s.702 and E.O. 12333, even as limited by PPD-28, are too permissive to meet the GDPR's standards of necessity and proportionality and do not provide EU data subjects with effective judicial redress.**

Analysis and recommendations

Our analysis shows that no US federal or state privacy law is likely to provide "essentially equivalent" protection compared to the EU GDPR in the foreseeable future. Indeed, there are serious and in practice insurmountable US constitutional and institutional as well as practical/political obstacles to the adoption of such laws.

The EU–US Safe Harbour and Privacy Shield agreements were attempts to overcome these US legal/constitutional constraints, by setting out detailed rules to reflect EU data protection law, with US companies self-certifying their compliance – which gave the FTC the right to sanction them if they did not. However, the way in which this was done was clearly defective: self-certification related to sets of watered-down principles rather than to the actual ones in the EU instruments, set out in impenetrable collections of different documents, and subject to limited enforcement by the FTC, which lacked the powers to effectively enforce the arrangements.

For the FTC to become an effective supervisory authority on the lines of the EU authorities, the FTC Act would likely have to be expanded or a new statute passed. Additionally, new or expanded Memoranda of Understanding should be signed among multiple US agencies, creating shared, coordinating enforcement teams. The FTC Act would need give the FTC the power to seek penalties for any violations of voluntarily accepted GDPR requirements; allow a broader range of entities to self-certify; allow the FTC to issue "trade regulation rules"; and instruct the FTC to formally cooperate with the EDPB.

It may not be possible to provide a right of action for individuals as broad as that envisaged in the GDPR. However, Congress could still significantly strengthen the right of action – and standing – of individuals, *including non-US persons*, who are significantly affected by privacy-related "unfair or deceptive acts or practices" committed by private entities.

If (i) the US and the EU were to take the legislative steps we outline relating to substance, enforcement and individuals' rights of action **and** (ii) the US were to reform its surveillance laws and practices, ***then*** **a new EU-US arrangement for self-certification by US entities could be achieved**, under which the EU could issue a new positive adequacy decision on the USA, limited to personal data transferred from the EU to entities that had self-certified their voluntary compliance with the EU GDPR substantive standards. Without these reforms, EU data protection authorities will be required to consider suspending transfers of personal data to the US even following an adequacy decision by the European Commission.

We reach this conclusion somewhat reluctantly, given the strong views on self-certification of the European Parliament. However, we believe it is the only workable solution, given the issues cannot be resolved by new federal or state privacy laws. We should stress that we are not talking about a revival

of the disastrous and untenable Safe Harbour/Privacy Shield arrangements, but about **a fundamentally different, enhanced system of self-certification**, with the self-certification itself **relating to the entire GDPR** and **much stronger enforcement** by the FTC.

In our view, it would be a positive *quid pro quo* if the EU were to offer the USA (and the rest of the world) the introduction of **a genuine "American-style" class action remedy** in relation to any violations of the GDPR, which anyone affected by such a violation (whatever their nationality, status, or place of residence) could join.

Legal academics and civil society groups are clear federal surveillance legislative reform will also be required to provide EU data subjects with "**an effective remedy before…an independent and impartial tribunal**". Such complaints could be initially investigated by US intelligence agency Privacy and Civil Liberties Officers, with their findings referred to the agency Inspector General or the Privacy and Civil Liberties Oversight Board (PCLOB). The complainant would be given standing to obtain judicial review from the Foreign Intelligence Surveillance Court.

Legislative reform will also be required to ensure the **necessity and proportionality of US surveillance** of data transferred under any adequacy finding. US civil society groups have recommended limiting bulk collection; narrowing the definition of foreign intelligence information and setting stronger standards to justify surveillance targets; reducing the default retention period for collected information from five years to three; and increasing transparency.

US academics and civil society groups have also called for much stricter limits on US "**secret law**". If the EU institutions are to be able to review the "essential equivalence" of a reformed US legal regime with GDPR protections, such authoritative legal interpretations or requirements affecting EU data subjects must be shared with them by the US authorities, along with any changes to the E.O. 12333 regime. Enough detail should be made public to be "adequately accessible".

The EU institutions should stand up for the rule of law and demand both the Member States and third countries bring their intelligence practices and domestic law frameworks fully in line with international human rights law. A pragmatic starting point would be the development and ratification of **a "minilateral" treaty covering intelligence activities of, in particular, the 30 EU/EEA states and the "Five Eyes" countries (USA, UK, Australia, Canada and New Zealand)**. This should include clear rules on the states concerned not surreptitiously spying on each other, with transparent arrangements for mutual assistance, subject to crucial rule of law and human rights safeguards and openness about practice.

Our recommendations effectively come down to four (we discuss their prioritisation after summarising them):

<u>Recommendation No. 1</u> (achieving general adequacy *pace* the issue of undue access):

The EU and the US should enter into discussions on the establishment of a much enhanced and strengthened self-certification scheme for US corporations.

Criteria/rationale:

We somewhat reluctantly concluded that, since no US federal or state privacy law is likely to provide "essentially equivalent" protection compared to the EU GDPR in the foreseeable future (or ever), general adequacy can only be achieved under a new self-certification scheme enforced through the FTC.

However, any such new self-certification scheme would have to apply to all substantive requirements of the EU GDPR; the FTC would need to be given wider and stronger powers; and EU data subjects should be accorded rights of standing in relation to breaches of the scheme.

Recommendation No. 2 (addressing the issue of undue access to data by US intelligence agencies):

The US should be urged to reform its federal surveillance legislation as a matter of urgency. This should involve limiting bulk collection; narrowing the definition of foreign intelligence information and setting stronger standards to justify surveillance targets; reducing the default retention period for collected information from five years to three; increasing transparency about surveillance activities; and providing EU data subjects with "an effective remedy before…an independent and impartial tribunal" – which can be achieved by granting EU complainants standing to obtain judicial review from the Foreign Intelligence Surveillance Court.

Criteria/rationale:

Given the strong and unambiguous stand taken by the CJEU in its *Schrems II* judgment, unless such reform is carried out, no new positive "adequacy" decision on the USA can be issued by the EU Commission. (If one were to be issued in defiance of the judgment, that would both seriously undermine the credibility of the Commission as a guardian of the Treaties and lead to yet another defeat – a "third strike" – in the Court. That should be beyond contemplation.)

Recommendation No. 3 (bringing surveillance generally under the rule of law):

The EU institutions and in particular the European Parliament should stand up for the rule of law and demand that both the Member States and third countries bring their intelligence practices and domestic law frameworks fully in line with international human rights law.

They should urge, as a pragmatic starting point, the urgent development and ratification of a "minilateral" treaty covering intelligence activities of, in particular, the 30 EU/EEA states and the "Five Eyes" countries (USA, UK, Australia, Canada and New Zealand).

As an interim measure, these 35 countries should agree not to spy on each other's citizens (and their data) without the notification and agreement of the citizen's home state.

Criteria/rationale:

The intelligence agencies of the constitutional democracies have operated for too long outside of a clear and acknowledged framework of (international, and often even constitutional) law. As the European Court of Human Rights Grand Chamber judgment in the *Big Brother Watch* case makes clear, the ECHR (as interpreted and applied by that Court) is insufficient for this purpose. While, regrettably in our view, the activities of the EU Member States in relation to national security are outside the scope of EU law, the EU (working with the Council of Europe) can be a midwife to a new international agreement in this area. However, this would take some years.

We therefore hope that an interim, less formal, "no spying on allies" agreement can be achieved in the meantime, within a relatively short timeframe.

Recommendation No. 4 (strengthening representative/class actions in the EU):

The EU should offer the USA (and the rest of the world) the introduction of a genuine US-style class action remedy in relation to any violations of the GDPR, which anyone who suffered material or non-material damage as a result of a violation (whatever their nationality, status, or place of residence) could join.

Criteria/rationale:

As the case of Max Schrems shows, EU data subjects' rights and interests are often not effectively enforced, or the individuals concerned supported, by the EU Member States' supervisory authorities, and court actions are costly and pose serious (financial) risks to them. In that regard, the EU can learn from the US (although the "Article III" jurisdictional issue imposes limits there too).

Overall, we concluded that if the above four recommendations were to be implemented, transfers of personal data from the EU to the USA could again be facilitated under the new self-certification scheme, with a new adequacy decision issued by the EU Commission that would not be invalidated by the Court.

Until this achieved, transfers of personal data from the EU to the USA must be based on "appropriate safeguards" including standard contractual clauses (SCCs) and Binding Corporate Rules (BCRs), or in due course approved codes of conduct or certifications issued by appropriate, accredited certification authorities – but in effectively all these cases, "supplementary measures" such as strong encryption will be required to protect transferred data against undue access by the US intelligence agencies. And no effective supplementary measures have yet been identified that could protect against such undue access if the data have to be accessible to the data importer in the USA in the clear. Some measures, such as audits, logs and reporting mechanisms could possibly be used in some such contexts (in particular, where the data are clearly not at all sensitive – in a broad sense – and unlikely to be of interest to the US intelligence agencies). But for sensitive data in the broad sense (sensitive data in the formal sense of the GDPR and other, more generally sensitive data such as communications data, financial data and travel data), these will generally not suffice.

The issues therefore need to be addressed **urgently**. This brings us to the final matter: prioritisation.

Prioritisation:
We believe the issues are best addressed in this order:

1. The EU should identify stop-gap measures such as audits, logs and reporting mechanisms that can possibly be used to allow some transfers of non-sensitive data – but also identify categories of data (and/or of controllers and processors or contexts) in relation to which these will not suffice. The European Parliament should ask the EDPB to address these matters in yet further guidance on EU–US data transfers, drawing on the work of the Commission in relation to the Digital Services Act and the Digital Markets Act.

   We believe this can be done in a matter of **a few months** at most.

2. The European Parliament should urge the EU Member States and the "Five Eyes" to adopt as a matter of urgency an interim, somewhat informal, "no spying on allies" agreement, while at the same time;

3. The EU Member States and the "Five Eyes" should commence a formal process towards the adoption of a formal "minilateral" agreement.

   We believe that (if the political will is there) an interim agreement could be possible within **a few months** – but ratification of a full treaty (which would also have to have internal effect in the USA – which not all US international agreements do) would take **several years**.

4. In parallel with the above, the EU should urge the USA to start the reforms of its surveillance laws and of the FTC Act that have been suggested by expert academics and civil society groups in the USA and the EU. It would be important to have a working group established on this issue that can exchange views on what is necessary (and possible) and report on progress; this working group should include representatives of the European Parliament.

We believe that significant reforms could be achieved in US law **this (executive order)/next (statutory) year** (again, if the political will is there, and the EU forcefully urges this).

- o – O – o -

1 INTRODUCTION

KEY FINDINGS

On 16 July 2020 the Court of Justice of the European Union (CJEU) invalidated the Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US "Privacy Shield" agreement, concerned US government surveillance powers are not limited as required by EU law, and that EU persons do not have effective means of redress.

1.1 Background

On 6 October 2015, the Court of Justice of the European Union (CJEU) declared invalid the European Commission's July 2000 decision on the legal adequacy of the EU-US Safe Harbour Framework (*Schrems I*).[1] On 12 July 2016, the European Commission issued an adequacy decision on the successor EU-US "Privacy Shield" Framework,[2] which provided a legal mechanism for companies to transfer personal data from the EU to the United States under the General Data Protection Regulation (GDPR). But on 16 July 2020 the CJEU delivered a judgment (known as *Schrems II*)[3] invalidating this adequacy decision, too.

The Court was concerned that the Fourth Amendment to the United States Constitution does not apply to EEA citizens; that the relevant legal regimes under the US Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (E.O. 12333) and Presidential Policy Directive 28 (PPD-28) were not limited as required by EU law; and that EU persons do not have effective means of redress against the US government in relation to unfair or unlawful processing under these US instruments. The CJEU also found out that the appointment of the Ombudsperson (as required under the Privacy Shield certification) did not meet the requirements of an official tribunal under European law, therefore EEA citizens did not have an adequate judicial remedy for complaints regarding processing of their personal data.

The Court upheld the validity of Decision 2010/87 on standard contractual clauses (SCCs), deeming them in principle an effective mechanism to ensure compliance with the level of protection provided in EU law. However, it indicated data controllers must assess the level of data protection in the recipient's country and must adopt "supplementary measures" if needed to protect transferred data against undue access by a third country's authorities – or suspend transfer if the data could not be adequately protected. The CJEU underlined an obligation on the part of each data protection authority in all EU Member States to suspend transfers of personal data if they deem that EU levels of protection are not met in the third country.

Two years before the *Schrems II* judgement, the European Parliament issued a resolution on Privacy Shield.[4] Given the revelations of misuse of personal data by companies certified, such as Facebook and

---

1 CJEU, Grand Chamber judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems I*"), ECLI:EU:C:2015:650

2 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p. 1–112.

3 CJEU Grand Chamber judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), ECLI:EU:C:2020:559.

4 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)), at: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html

Cambridge Analytica, it called on the US authorities to act without delay in full compliance with the assurances and commitments given and, if needed, to remove such companies from the Privacy Shield list. Parliament called also on the competent EU data protection authorities to investigate such revelations and, if appropriate, suspend or prohibit data transfers. Most importantly, Parliament considered the revelations clearly showed the mechanism did not provide adequate protection of the right to data protection. It noted concern at that time about the consequences of Executive Order 13768 on 'Enhancing Public Safety in the Interior of the United States' for judicial and administrative remedies available to individuals in the US, because the protections of the Privacy Act no longer applied to non-US citizens.

Overall, transfers of personal data from the EU to the USA were carried out for more than a decade (at least since 2000) without respecting European standards for data protection, resulting in irreversible harm to EU citizens and companies; yet the European Commission has ignored during this period numerous calls from the European Parliament and human and digital rights organisations. This underlines the gravity of the situation and the importance of taking remedial steps to guarantee protection for EU citizens and companies in the future.

More specifically, in the aftermath of the *Schrems II* judgement the LIBE Committee took up work on a resolution reaffirming the CJEU ruling has significant implications for adequacy decisions concerning all third countries and pointing at the need for legal clarity and certainty.

In this context the Committee requested this study in order to become acquainted with expert opinion on reforms to the legal framework for the exchange of personal and other data between the EU and the USA necessary to ensure the requirements of EU law are satisfied and the rights of EU citizens are respected.

1.2 Scope and objectives of the research and structure of the study

In chapter 2, we discuss the European view of data protection as a fundamental *sui generis* right, and the national security exemption in the EU Treaties, and the implications in particular in relation to transfers of personal data from the EU to non-EU countries or territories (so-called "third countries"). This is done with reference to the relevant case law of the CJEU, including notably the Court's *Schrems I* and *Schrems II* judgments, in relation to the flows of personal data that are subject to the GDPR from the EU to a third country, and the USA in particular; to the European Data Protection Board's (EDPB) updated Adequacy Referential; and to the Board's European Essential Guarantees (EEGs) for surveillance (in relation to the issue of access to EU data by authorities of third countries).

Chapter 3 summarises (a) US constitutional and common law on privacy, (b) US federal and state privacy laws and (c) US surveillance laws with reference to the main EU issues and standards identified in chapter 2.

Chapter 4 provides a deeper analysis of standards that must be met for the USA to provide for an adequate level of data protection, indicates the changes that would have to be made to US law in order for it to satisfy those EU requirements, and explores policy and legal options for the future, in relation to the exchange of personal and other data between the EU and "third countries" outside the European Economic Area.

- o – O – o -

2 EUROPEAN DATA PROTECTION STANDARDS

KEY FINDINGS

In the EU, data protection is **a fundamental right**, enshrined in primary law. Under the GDPR, personal data can only be freely transferred to countries held by the European Commission to provide **"adequate"/"essentially equivalent" protection**. Otherwise, "appropriate safeguards" must be adopted by the EU data exporter.

Furthermore, there must be one or more **independent public authorities** with responsibility for ensuring compliance with the relevant data protection instruments, which ensure "a good level of compliance" in practice, and provide "support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms".

A third country's laws can only be said to provide such protection if they meet the standards set out in the European Data Protection Board (EDPB) Adequacy Referential, on matters such as scope, purpose specification and limitation, and restrictions on onward transfers. And in relation to access to personal data by a third country's intelligence agencies, its laws can only be said to provide this protection if they meet the standards set out in the EDPB's European Essential Guarantees for surveillance.

While activities of Member State authorities for national security purposes are outside EU competence, national constitutions and the European Convention on Human Rights apply. Moreover, the exemption does not apply to the imposition of legal obligations on private sector organisations, or to non-EU countries.

Any persistent failure by an EU Member State to comply with the ECHR and with the judgments of the Strasbourg Court would be incompatible with membership in good standing of the Union.

2.1 Introduction

Under the GDPR,[5] personal data can only be freely transferred from the EU[6] to a non-EU country (a "third country") held by the European Commission (the executive branch of the EU), on the basis of an assessment under a set of prescribed standards, to provide "adequate" protection to such data. The CJEU has held this means the third country must provide "essentially equivalent" protection to that accorded in the EU by the GDPR. If a third country does not afford "adequate"/"essentially equivalent" protection to personal data, "appropriate safeguards" must be adopted by the EU data exporter and the third country data importer to ensure that the EU level of protection is not undermined.

[5] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ L 119, 4.5.2016, p. 1–88.

[6] The GDPR data transfer regime also applies to the three non-EU Member States of the European Economic Area (EEA), Iceland, Liechtenstein, and Norway. However, in this short study, we will generally just refer to the EU. This should be read as applying to the EU and those three other EEA Member States that are, for data protection purposes, not "third countries".

Whether the USA provides an "adequate" level of protection of personal data touches on two distinct but related matters: whether any US law generally provides such protection (or whether arrangements such as the Safe Harbour or Privacy Shield could ensure this); and whether US law allows its authorities to access personal data on EU persons only in circumstances and under conditions that meet EU standards. Under the GDPR, these two issues are linked, since a third country cannot be held to provide "adequate"/"essentially equivalent" protection to the GDPR if it grants its authorities powers to access personal data on EU persons that are excessively wide in EU terms, or if it does not provide remedies and remedial fora that meet the EU standards on procedural fundamental rights protection.

However, for the purpose of this study it is useful to first deal with these issues somewhat separately, before returning to the way they interrelate in the final chapter.

In section 2.2, below, we first discuss two matters that are crucial to understanding the "European" approach to these issues: the fact that in Europe data protection is seen as a fundamental, universal human right (section 2.2.1), and the somewhat contradictory exclusion of "national security" matters from EU law (section 2.2.2) – but we also note in the latter section: (a) that this "hole" in the EU legal order is limited by the case-law of the CJEU; (b) that it is "patched" by the application of the European Convention on Human Rights (ECHR) to matters that are outside the scope of EU law; and (c) that that "patch" can to some extent be made to stick also under EU law.

We then, in section 2.3, discuss the implications of these general matters for transfers of personal data from the EU to third countries, with a focus on the requirements that must be met by third countries if they are to be held to provide "adequate"/"essentially equivalent" protection compared to the EU (section 2.3.1).

In that respect, we note:

- the general (substantive and procedural/enforcement) standards laid down in EU data protection law (in particular the GDPR) which EU law requires to be "essentially and "equivalently" laid down in third countries' laws if those countries are to be held to provide "adequate" protection (sub-sections 2.3.1.1 and 2.3.1.2);
- the complex legal requirements for access to personal data by state authorities that are subject to EU data protection law, whereby we differentiate between different contexts and between access by EU and third country intelligence agencies (sub-section 2.3.1.3).

For completeness' sake, we also briefly discuss in this section the EU rules on regular and occasional transfers of personal data to third countries that are not held to provide "adequate"/"essentially equivalent" protection (in section 2.3.2).

In chapter 3, following an initial discussion of general matters, we first discuss, in section 3.1, US constitutional and common law principles on privacy and federal and state privacy laws (and some proposed and pending laws), and assess those against the general standards adduced at 2.3.1.1 and 2.3.1.2; and then, in section 3.2, we discuss the US federal laws regulating access by US authorities to personal data including data on EU persons (US surveillance laws), and assess those against the specific standards on that issue adduced at 2.3.1.3.

In chapter 4, we further analyse the situation and make specific recommendations.

2.2 Fundamental matters

2.2.1 In Europe, data protection is a fundamental right

In Europe, data protection is seen as **a fundamental, universal human right**. In the EU legal order, it is enshrined as a *sui generis* right in the EU treaties and in the EU Charter of Fundamental Rights (Article 8).[7] This has important implications, also in relation to data protection and more generally in relation to surveillance – including extraterritorial surveillance – by states.

It follows, first of all, that the privacy or data protection laws of any state should apply to all processing of all the personal data of all individuals whose rights (in particular data protection/privacy rights) are affected by actions of (private or public sector) entities under the jurisdiction of the relevant state, irrespective of the individuals' nationality or status or of where they are (i.e., even if they are not nationals or residents of the state or are physically outside of the territory of the state): the **principle of universality**.[8]

The principle of universality of human rights (and therefore of data protection):

The principle was most recently and forcefully expressed by the German Constitutional Court (based in Karlsruhe) in its May 2020 judgment on the Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst*), as amended in 2016.[9] In this, the Court held:

> According to Art. 1(3) [of the German Constitution, the Basic Law, *Grundgesetz*, GG], the fundamental rights of the Basic Law bind the legislature, the executive and the judiciary as directly applicable law. … [I]t cannot be inferred from the Basic Law's legislative history that fundamental rights protection was always meant to end at the national border. Rather, **the Basic Law's aim to provide comprehensive fundamental rights protection and to place the individual at its centre suggests that fundamental rights ought to provide protection whenever the German state acts and might thereby create a need for protection – irrespective of where and towards whom it does so.**
>
> (para. 89, emphasis added)

The German Constitutional Court rightly notes that this view was adopted partly "in response to the Nazi reign of violence and tyranny" (which of course extended far beyond the borders of the *Reich*) with the aim of:

> achiev[ing] [as early as 1949] a comprehensive binding effect of fundamental rights rooted in human dignity … in the conviction that the Federal Republic of Germany had to find its place in the international community as a partner that abides by the rule of law.
>
> (*Idem*)

---

7 See Douwe Korff and Marie Georges, *The Origins and Meaning of Data Protection*, January 2020, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518386

8 See the Council of Europe's Commissioner for Human Rights 2014 *Issue Paper* on *The Rule of Law on the Internet and in the wider digital environment* (written by Korff), section 3.3, *"Everyone", without discrimination*, and the Commissioner's first recommendation, *I. On the universality of human rights, and their equal application online and offline* (p. 21), at: https://rm.coe.int/the-rule-of-law-on-the-internet-and-in-the-wider-digital-world-issue-p/16806da51c

9 Judgment of German Constitutional Court of 19 May 2021 (BVerfGE 1 BvR 2835/17), at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html (German original)
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html (Court's own translation into English, which we use in quotes in this study).

However, that latter aim – *embedding states in an international community as partners that abide by the rule of law and that respect human rights* – is now also generally accepted by all European countries as the foundation for their international relations and is expressly reflected in Article 2 of the EU Treaty on European Union (TEU), quoted in sub-section 2.2.2.3, below.

As the Karlsruhe Court points out, this is also increasingly reflected in the case-law of the European Court of Human Rights, even if (as the Karlsruhe Court puts it):

> It has not yet been comprehensively determined to what extent [the ECHR's] guarantees apply to actions of the Contracting Parties outside of their own territory. The European Court of Human Rights is mainly guided by the criterion of whether a state exercises effective control over an area outside its own territory; on this basis, it has in many cases affirmed the applicability of Convention rights abroad … [and] there has been no final determination as to whether protection is afforded against surveillance measures carried out by Contracting Parties in other states.
>
> (para. 97, with reference to the summaries of the Strasbourg case-law in ECtHR [GC], *Al-Skeini and Others v. the United Kingdom*, Judgment of 7 July 2011, no. 55721/07, §§ 132 et seq. with further references, and to Aust, Archiv des Völkerrechts 52 <2014>, p. 375 <394 et seq. > with further references)

However, the German Constitutional Court noted that the latter matter – the question of whether extra-territorial surveillance was subject to the ECHR obligations of the State Parties to that Convention – was an issue in the European Court of Human Rights *Big Brother Watch* (*BBW*) and *Centrum för Rättvisa* judgments:

> In a decision that has not become final yet, the First Section of the European Court of Human Rights measured the implementation of surveillance measures targeting persons abroad against the standards of the Convention without any restrictions and found such measures to be in violation of the Convention. The complainants in this case included foreign nationals who were not present or resident in the state against which the applications were directed (…). Similarly, a Swedish foundation challenged strategic foreign surveillance powers under Swedish law that exclude domestic communications. The European Court of Human Rights reviewed these powers without calling into question the Convention's applicability abroad (…).
>
> (para. 98, with references to the Court's first instance judgments in *Big Brother Watch and Others v. the United Kingdom*, Judgment of 13 September 2018, no. 58170/13 and others, § 271, and in *Centrum för Rättvisa v. Sweden*, Judgment of 19 June 2018, no. 35252/08)

The Grand Chamber of the European Court of Human Rights issued the final rulings on the *BBW* and *Rättvisa* cases as this study was being finalised.[10] It is notable (as in the proceedings before the First Chamber) neither the United Kingdom nor Sweden even tried to argue the Convention should not be applied to surveillance activities that clearly extended (and still extend) to communications of and between individuals who are neither inside its territory (or territories) nor its nationals or residents. As the Court noted in relation to the UK:

> In respect of the [bulk interception of communications] regime, the Government raised no objection under Article 1 of the Convention [that stipulates that "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in [the main section of the ECHR"], nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. Moreover, during the hearing before the Grand Chamber the

[10] ECtHR, Grand Chamber judgment in the case of *Big Brother Watch and Others v. the United Kingdom*, 25 May 2021, at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}
ECtHR, Grand Chamber judgment in the case of *Centrum för Rättvisa v. Sweden*, 25 May 2021, at: http://hudoc.echr.coe.int/eng?i=001-210078

> Government expressly confirmed that they had raised no objection on this ground as at least some of the applicants were clearly within the State's territorial jurisdiction. Therefore, for the purposes of the present case, the Court will proceed on the assumption that, in so far as the applicants complain about the [bulk interception] regime, the matters complained of fell within the jurisdictional competence of the United Kingdom.
>
> (Para. 272; cf. the First Section judgment, para. 271)

The Swedish Government, too, did not raise any objection to the Court applying the Convention to its bulk surveillance activities, even though the Court noted in several contexts that Sweden's bulk data interception powers:

> may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State's territorial jurisdiction.
>
> (*Rättvisa* GC judgment para. 272)

Indeed, the Court noted that this was generally the case, also in relation to other countries:

> while the interception and even examination of communications of persons within the surveilling State might not be excluded, in many cases the stated purpose of bulk interception is to monitor the communications of persons outside the State's territorial jurisdiction, which could not be monitored by other forms of surveillance. For example, the German system aims only to monitor foreign telecommunications outside of German territory ...
>
> (*Idem*, para. 258)

It is therefore simply wrong to argue (as some still do) that surveillance activities undertaken by a state outside the territory of that state are not subject to the European Convention on Human Rights – and by implication that such activities should therefore also not be subject to European data protection instruments.[11] On the contrary, as the German Constitutional Court noted, just like the Karlsruhe Court applies the German constitutional standards to extraterritorial surveillance by German authorities, so **the European Court of Human Rights expressly applies the ECHR standards to European States' powers of bulk interception of extraterritorial communications – and the States concerned raised no objection to this approach by the Strasbourg Court** (as they could have done if they thought such an objection would have had any chance of success).[12]

In its intervention in the *BBW* case, the *International Commission of Jurists* also stressed that:

> the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction [does not] preclude that State's responsibility, since its control over the information [is] sufficient to establish jurisdiction.
>
> (ECtHR paraphrase of the ICJ submission in its *BBW* GC judgment, para. 299)

One of the dissenting judges in the *Big Brother Watch* Grand Chamber judgment, Judge Pinto De Albuquerque, put it eloquently:

---

[11] See Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations, Part 2, On Double Standards and the Way Forward*, 13 April 2021, at: https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/#comment-35772

[12] It is an important illustration of the close interactions between the European courts and between them and the constitutional courts of the European states that in its *BBW* GC judgment (discussed in some detail in section 2.3.1.3(iii), below), the Strasbourg Court devotes a significant section (section IV.B, paras. 247 – 252) to the Karlsruhe judgment discussed above, just as the Karslruhe Court looked closely at the Strasbourg case-law (as noted in the quotes in the text).

> The Convention places at its centre the individual, not the citizen of a State, which means that Convention rights as rights of the individual ought to provide protection whenever a Contracting Party acts and thus potentially creates a need for protection – irrespective of where, towards whom and in what manner it does so. Furthermore, the Convention rights should permeate the participation of Council of Europe member States in the international community, in so far as "the Council of Europe legal order can no longer be confused with the traditional international accord of juxtaposed egoisms. Sovereignty is no longer an absolute given, as in Westphalian times, but an integral part of a human rights-serving community".
>
> (Dissenting Opinion, para. 41)

(The Judge therefore rightly criticised the UK law under which the Investigatory Powers Tribunal does not accept complaints from applicants outside the UK, calling this a "*foreigner unfriendly* Weltanschauung *[that] could not be more alien to the spirit and letter of the Convention*". *Idem*)

The principle of universality is moreover expressly confirmed in relation to data protection in the explanatory note on Article 1 of the Modernised Council of Europe Data Protection Convention (Convention 108+) in the Explanatory Report on that convention:[13]

> The guarantees set out in the Convention are extended to every individual regardless of nationality or residence. No discrimination between citizens and third country nationals in the application of these guarantees is allowed.(6) Clauses restricting data protection to a State's own nationals or legally resident foreign nationals would be incompatible with the Convention.

We have dealt with the issue of universality and the application of international human rights- and data protection standards to extraterritorial (surveillance) activities of states in some detail because **the USA does not accept this principle of universal/extraterritorial application of international human rights law or of the international human rights treaties to which it is a party**. In chapter 4, below, we will note this in itself poses obstacles to any resolution of the EU – US personal data transfer issues.

<u>Other implications of viewing data protection as a fundamental right</u>:

It also follows from the view of data protection as a fundamental right that:

- the concepts and rights enshrined in such laws should be broadly interpreted and applied, and any limitations on those rights narrowly interpreted and applied (principles of legality, legitimate purpose, necessity, and proportionality);[14]
- there should be appropriate independent judicial avenues of redress for anyone whose data protection rights have been breached (principle of effective remedies);[15]
- the above should preferably be reflected in "omnibus" laws; and (as discussed in the next sub-section):

---

[13] *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Strasbourg, 10 October 2018, para. 15, which cross-refers to the Council of Europe *Issue Paper* on *The Rule of Law on the Internet and in the wider digital environment* (footnote 8).

[14] This approach was initially contested, with ECtHR Judge Fitzmaurice arguing that the ECHR should be narrowly interpreted, but his approach "*has now totally given away to an approach that focusses instead upon the Convention's law-making character and its role as a human rights guarantee that must be interpreted so as to permit its development with time*". As a result, the ECHR has come to represent "*the public order of Europe*". See David Harris, Michael O'Boyle, Edward Bates & Carla Buckley, *Law of the European Convention on Human Rights*, OUP, 2nd Ed., 2009, chapter 1, section 4.II, with reference to the ECtHR judgments in *Wemhoff* (1968) and *Golder* (1978). By contrasts, the US still holds to the Fitzmaurice view that human rights treaties (like "ordinary" treaties) should be interpreted and applied narrowly. On the implications of the "European" view of the principles of legality, legitimate purpose, necessity and proportionality for the issues addressed in this study, see in particular sub-section 2.3.1.1, below, under the heading "*General restrictions*".

[15] See Article 13 ECHR, Article 47 EU CFR.

- the protection accorded to personal data by should not be "undermined" if those data are transferred to another country.

In the next sections, we will discuss in more detail how the above principles are applied in practice, in particular in relation to data transfers. First, however, we must note the sweeping exemption from all EU law relating to the national security activities of the EU Member States and the limitations of this exemption.

2.2.2 The national security exemption in the EU Treaties

2.2.2.1 The "hole" in the EU Treaties

The EU Treaties – the founding documents of the Union – and in particular the Treaty on European Union (TEU) clarify the competences of the Union, and the limits of those competences. In particular, Article 4(1) stipulates:

> competences not conferred upon the Union in the Treaties remain with the Member States.

Article 4(2) adds more specifically:

> The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their 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**. (emphasis added)

In simple terms: No parts of EU law, including even the EU Charter of Fundamental Rights that guarantees, *inter alia*, protection of personal data, apply to the activities of the EU Member States in relation to the protection of their national security. Consequently, all EU data protection instruments that apply to processing of personal data by authorities of EU Member States (the GDPR, the e-Privacy Directive [2002/58/EC, ePD] and the Law Enforcement Directive [2016/680, LED]) stipulate that they "*do[ ] not apply to the processing of personal data … in the course of an activity which falls outside the scope of Union law*" – i.e., in particular, to processing of personal data by EU Member States agencies in relation to activities relating to national security.[16]

2.2.2.2 Limiting the size of the "hole" and "patching" the remainder

Limiting the size of the "hole"

In line with the fundamental rights approach outlined in section 2.1, the Court of Justice has restrictively interpreted the national security exemption in the Treaties. Most recently, in its Grand Chamber judgment in *La Quadrature du Net* (*LQDN*),[17] the Court confirmed its earlier case-law in which it held:

> although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national

[16] See GDPR, Article 2(2)(a); ePD, Article 1(3) (in slightly different terms); LED, Article 2(3)(a). The EU regulation setting out the data protection rules for the processing of personal data by the EU institutions and bodies themselves (Regulation 2018/1725) does not contain such a provision because by its very nature it does not apply to processing of personal data by intelligence agencies of the Member States.

[17] CJEU, GC judgment in Joined Cases C-511/18, C-512/18, *La Quadrature du Net v. France*, and C-520-18, *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL and others v. Belgium*, 6 October 2020, ECLI:EU:C:2020:791.

> measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.
>
> (*LQDN*, para. 99, with reference to earlier judgments)

The Court therefore held the rules on personal data processing operations by entities that are, in that processing, subject to EU data protection law (in that case, providers of electronic communication services, who are subject to the e-Privacy Directive), *including processing operations by such entities resulting from obligations imposed on them (under the law) by Member States' public authorities* (in that case, for national security purposes) can be assessed for their compatibility with the relevant EU data protection instrument and the Charter of Fundamental Rights[18] – and the Court held that laws that require "*as a preventive measure, … the general and indiscriminate retention of traffic and location data*" are incompatible with the Charter.[19]

The Court also for the first time[20] gave a definition of national security:

> That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.
>
> (*LQDN*, para. 135)

The "patch" over the remaining (limited) "hole"

However, this does not completely close the "hole":

> By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by [the e-Privacy Directive], but by national law only, subject to the application of [the Law Enforcement Directive], with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.
>
> (*LQDN*, para. 103)

In summary

- if a national law of an EU Member State imposes obligations on private sector entities or on EU Member States public sector entities other than law enforcement authorities that are subject to the GDPR and/or the e-Privacy Directive, the compatibility of those national legal rules with those EU instruments and with the Charter can be – and must be – assessed by the relevant national courts and (ultimately) the Court of Justice, even if those obligations are imposed for the purpose of protecting national security (typically, under special national security laws);
- if a national law of an EU Member State regulates the processing of personal data by "competent authorities" (in simple terms: law enforcement agencies) for the purposes of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security", the compatibility of the relevant legal rules with the Law Enforcement Directive and

[18] Para. 101 (see also para. 102).

[19] Para. 228. On the more specific requirements of the Charter in these regards, see section 2.3.1.3, below.

[20] Sarah Eskens, *EU power over intelligence gathering for national security purposes*, presented at TILTing 2021: Regulating in Times of Crisis, 19 May 2021.

with the Charter can be – and must be – assessed by the relevant national courts and (ultimately) the Court of Justice; and this includes any national legal rules of any EU Member State that gives law enforcement authorities the power to "directly implement" measures that impinge on data protection rights of individuals – such as the direct "hacking" into the systems or servers of providers of electronic communication services, or into the cables through which electronic communications flow – for law enforcement purposes;

- but if a national law of an EU Member State gives some of its authorities (typically, its intelligence agencies) the power to "directly implement" measures that impinge on data protection rights of individuals – such as (again) the direct "hacking" into the systems or servers of providers of electronic communication services, or into the cables through which electronic communications flow – for national security purposes, then the compatibility of the relevant legal rules with EU law including the Charter cannot – and may not – be assessed by the Court of Justice;
- however (as the Court expressly noted), such a national security law can – and must – still be assessed for its compatibility with any national constitutional requirements (such as there may, or may not be) and, more importantly for the present study, with the European Convention on Human Rights.

In other words, the ECHR provides a patch over the "hole" in the EU legal order, relating to national security.

2.2.2.3 Making the patch stick through EU law

The assessment of the compatibility of EU Member States' national security laws with the ECHR is in principle outside of the competence of the EU and the CJEU. However, it is a condition of membership of the EU that any Member must be a party to the Convention (and the EU is in the process of itself becoming a party to the ECHR, although that process is complicated and delayed). As it is put in the Treaty on European Union:

> The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

The TEU also sets out the conditions (Article 49) and principles (Article 6(1)) to which any country wishing to become an EU member must conform. The specific criteria that must be met for admission, known as the Copenhagen criteria, were established by the Copenhagen European Council in 1993 and strengthened by the Madrid European Council in 1995.[21] They too include stability of institutions guaranteeing democracy and respect for the rule of law and human rights – and the latter is in practice held to mean being a party to the ECHR, having laws in place that meet all ECHR standards, and complying with the judgments of the ECtHR.

Any serious and in particular systemic departure by any EU Member State from the principle of respect for the rule of law and human rights can be the basis for sanctions on that state under the so-called Rule of Law Framework – although the procedures are onerous (which is why improvements aimed at

[21] See: https://ec.europa.eu/neighbourhood-enlargement/policy/conditions-membership_en

strengthening them are being proposed, especially in the light of some threats to the rule of law in some Member States).[22]

Any persistent failure by an EU Member State to comply with the ECHR and with the judgments of the Strasbourg Court would be incompatible with membership in good standing of the Union – and this would also apply in relation to any persistent failure by an EU Member State to comply with the requirements of the ECHR in relation to surveillance, as interpreted by the Strasbourg Court.

At the very least, this provides some political glue to the patch over the "hole" in the EU legal order in relation to national security activities of the EU Member States (although the ambiguous situation in this respect is still criticised by the USA, as discussed at the end of section 2.3.1.3, below).

2.2.2.4 The national security exemption does not apply to third countries

Finally, the CJEU expressly held that the national security exemption in the EU Treaties only applies to national security-related activities of the EU Member States, and does not apply to national security-related activities of third countries:[23]

> [I]t should be made clear at the outset that the rule in Article 4(2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting [various articles] of the GDPR.

This has implications in relation to data transfers, more in particular in relation to the assessment of the "adequacy" of third countries, as also discussed in sub-section 2.3.1.3, below.

2.3 Implications for data transfers

Because, in Europe, data protection is seen as a fundamental human right, the protection of personal data should not be lost or undermined if the data are transferred to a non-EU country (so-called "third country").

From the European perspective, it therefore also follows that when personal data are transferred from the EU to any third country – or when data in the EU are directly accessed from a third country (which in Europe is held to also constitute a transfer)[24] – the continued protection of those data should be ensured. In this respect, it is important to distinguish between:

- transfers of personal data to third countries that are held by the EU to provide "adequate" protection ("adequate" third countries) (below, 2.3.1);
- regular transfers of personal data to third countries that have not been held to provide such protection ("non-adequate" third countries) (below, 2.3.2.1); and
- occasional transfers of personal data to "non-adequate" third countries under special derogations (below, 2.3.2.2).

---

[22] See: https://ec.europa.eu/info/sites/default/files/rule_of_law_factsheet_1.pdf
https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/initiative-strengthen-rule-law-eu_en
https://ec.europa.eu/info/sites/default/files/rule_of_law_mechanism_factsheet_en.pdf

[23] CJEU, *Schrems II* judgment (footnote 3), para. 81.

[24] See footnote 23 in EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, version 2.0, adopted on 18 June 2021 (reflected in a range of guidance including on direct access by authorities in third countries to data in the EU/EEA).

In line with the request for this study from the European Parliament, we focus on the first topic: transfers of personal data to "adequate" third countries, and the criteria for determining adequacy in that context, with special attention to the issue of access to data by third country authorities. The other two topics (regular and occasional transfers to "non-adequate" third countries) are more briefly discussed, for completeness' sake. We have also added a short section on "Stopping transfers" (below, 2.3.3).

2.3.1 Transfers to "adequate" third countries

Continued protection at EU level can be said to be ensured if a relevant third country has been assessed as providing **"adequate" protectio**n in EU terms (Article 45 GDPR). Article 45(2) GDPR stipulates that:

> When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Moreover, the Court of Justice has held in its *Schrems I* judgment that the "adequacy" requirement means that the third country must provide "**essentially equivalent**" protection to the EU rules, the GDPR in particular.[25]

This requires an in-depth "**adequacy assessment**" of the third country's laws and practices under the standards set by Article 45(2) as interpreted by the Court of Justice of the EU, as reflected in the 2017 EDPB-endorsed WP29 "Adequacy Referential":[26]

(a) in general, substantive terms;

---

[25] CJEU, *Schrems I* judgment (footnote 1), para. 73.

[26] Article 29 Working Party, *Adequacy Referential*, adopted on 28 November 2017, as last revised and adopted on 6 February 2018 (WP254rev01), at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108/
EDPB endorsement:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf
The 2017/2018 referential replaced very old previous guidance in the WP29 *Working Document – Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive* (WP12), adopted on 24 July 1998, at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

(b) in terms of procedural protection and remedies; and

(c) in relation to access to data by the third country's authorities.[27]

In 2021, the European Parliament "Welcome[d] the fact that the Commission follows the criteria set out in the Article 29 Working Party Adequacy Referential under the GDPR (as endorsed by the EDPB) and in EDPB Recommendation 01/2021 on the Adequacy Referential under the Law Enforcement Directive [and] considers that the Commission should not go below these criteria when evaluating whether a third country qualifies for an adequacy decision".[28]

The general substantive and procedural requirements for adequacy are discussed below, in sub-sections 2.3.1.1 and 2.3.1.2. The issues of access to data by third country authorities, and the specific issue of procedural protection and remedies in that context, are addressed in section 2.3.1.3, below, with specific reference to access to data by third country intelligence agencies. In that context, we also take into account the national security exemption in EU law – the "hole" in EU law, discussed at 2.2.2.

2.3.1.1 General substantive requirements for adequacy

In terms of substance, a third country's laws can only be said to provide "adequate"/"essentially equivalent" protection in terms of the GDPR if they meet the standards set out in the EDPB's Adequacy Referential on the following matters in particular:

- Scope;
- Purpose specification and limitation (and related matters);
- Grounds for lawful processing;
- Special categories of data ("sensitive data");
- Informing of data subjects;
- Data subject rights;
- General restrictions; and
- Restrictions on onward transfers.

[27] Strictly speaking, all aspects of a third country' adherence to the rule of law and "*respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law … as well as the implementation of such legislation*" should be considered (Article 45(2) GDPR), but to date, only the issue of "*access of public authorities to personal data*", more specifically access by a third country's law enforcement and intelligence agencies, has been examined (specifically, in the CJEU *Schrems I* and *Schrems II* judgments, the USA's rules in this respect).

[28] European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)) §33.

We briefly discuss the standards in each of these respects below.

Scope

Within its area of application,[29] the third country's law must protect personal information that is as widely defined as "personal data" is in the GDPR,[30] in respect of all of the activities defined as "processing" in the GDPR,[31] and must not unduly exempt significant kinds of personal information or significant activities that are covered by the GDPR.

Purpose specification and limitation (and related matters)

The third country's law must only allow processing or further processing of personal data for clearly spelled-out purposes (and not for vague reasons such as "any business purpose" or "to improve users' experience") and must prohibit processing of personal data for "illegitimate" (societally unacceptable) purposes (such as discrimination or social scoring). The law must lay down rules on the quality of personal data and limit retention of personal data with reference to the purpose(s) of the processing.

Moreover, any departure from the purpose limitation principles – such as allowing state authorities to demand access to data held by private entities for business purposes for law enforcement or national security purposes – must also be based on published, clear and precise rules that are foreseeable in their application; such exceptional access must be limited to what is necessary and proportionate in relation to the relevant legitimate purposes in question; and such access must be based on procedural safeguards to protect against abuse, and to effective remedies on the part of individuals. We will return to these matters under the heading *General restrictions*", below, and more in particular in section 2.3.1.3, below.

Grounds for lawful processing (selection)

Under the GDPR, all processing of personal data must be based on one of a series of specified legal grounds. The following are the most important legal bases for processing for the purpose of this study:

Re processing on the basis of consent: The third country's law must not allow for processing on the basis of "implied consent" or non-action on the part of a data subject (such as not "unticking" a pre-ticked box on a webpage), or on the basis of "consent" obtained in circumstances in which the individual was not fully informed about the details of the processing (see below, fifth indent), or was in a weak position *vis-à-vis* the entity collecting and further processing the data.

Re processing on the basis of a controller's "legitimate interests": To the extent allowed (see next sentence), the third country's law must stipulate (or ensure in practice) that processing based on this criterion is limited to what is "necessary" and "proportionate" to the relevant (clearly specified) legitimate interest of the entity concerned, and must also require that that interest be counter-

[29] An adequacy assessment, and a subsequent adequacy decision, may be limited to a law or legal regime applicable to a particular area or sector – e.g., the public sector – or to processing under a special EU – third country arrangement – such as the (since invalidated) EU – US Safe Harbour and Privacy Shield arrangements. However, within that area of application the relevant law must apply to all processing of all personal data (as defined in EU data protection law).

[30] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Article 4(1) GDPR)

[31] 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Article 4(2) GDPR)

balanced against the rights and interests of the individuals concerned. Moreover, the law should not allow for processing of any personal data on this basis by public authorities in the course of their public tasks, nor any processing of sensitive data on this basis by anyone (see the next indent).

Re processing on the basis of law: A third country's law that allows for processing (including disclosing) of personal data by anyone in order to comply with a "legal obligation", or to perform "a task carried out in the public interest or in the exercise of official authority" must lay down a clear legal framework that specifies the parameters of and the conditions for the processing/disclosure demand. If it does not – e.g., if it is too vague or grants excessive discretion to the entity demanding the data or carrying out the task – the law cannot be said to provide "essentially equivalent" protection to the GDPR.

Special categories of data ("sensitive data")

The third country's law must impose "essentially equivalent" strict conditions to the GDPR ones on the processing of the special kinds of personal data listed in Article 9(1) GDPR,[32] such as requiring "explicit" (as well as free, informed and express) consent for such processing. It must not allow processing of such data ("sensitive data") on the basis of a "balancing of interests", and it must impose such strict conditions on all of the categories listed in the GDPR (including trade union membership).

Informing of data subjects

The third country's law must require controllers to inform data subjects of (at least) the controller's identity, the purpose of the processing, the personal data involved and (where applicable) the right to withdraw consent, any intended automated decision making, and the risks involved in any intended data transfer.

Data subject rights

The third country's law must "essentially" provide for all the data subject rights provided for in the GDPR, i.e.:

- the right to information about the processing of their data;
- the right of access to the data subject's data, free of charge;
- the right of rectification of inaccurate data and to have incomplete data supplemented;
- the right to erasure of data if they are no longer needed;
- the right to restriction of processing (i.e., the blocking of data pending a dispute);
- the right to have third parties to whom the data were disclosed informed of any rectifications, erasures or restrictions (unless this is impossible or involves disproportionate effort);
- the right to data portability;
- the right to object to processing; and
- the right not to be subject to automated individual decision-making, including profiling unless conditions in the law are met that are "essentially equivalent" to those set out in these respects in the GDPR.

[32] I.e.: "personal data revealing **racial or ethnic origin**, **political opinions**, **religious or philosophical beliefs**, or **trade union membership**" as well as "**genetic data**, **biometric data** [when used] for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a natural person's **sex life or sexual orientation**" (emphases added).

General restrictions

Third country's laws may provide for restrictions on the above rights and obligations for important (legitimate) aims in a democratic society including national security, defence, public security, criminal legal investigations and prosecutions, other important public tasks and interests, or the protection of the data subject or the rights and freedoms of others. However, as explained in section 2.2.1, under EU fundamental rights law such restrictions must be set out in "law", respect the "essence" of the rights affected, and must be "necessary" and "proportionate" to the aim in question. These terms and concepts are used with minor variations in the core human rights guarantees in Articles 8 – 11 of the ECHR and more broadly (in relation to all rights) in Article 52(1) of the EU Charter of Fundamental Rights.

The concept of "law" is particularly important in the present context. In European law, in particular the ECHR, it is an "autonomous concept", meaning that a state cannot fulfil the condition that a rule (more specifically, a limitation of a right) is "law" or "based on law" by pointing to some existing legal rule in its domestic order, even if the rule in question is valid in domestic terms. Rather, under the Convention, the concept is linked to the "rule of law" and its opposite: arbitrariness. In order to qualify as "law" in the Convention sense, the legal rule in question must have certain qualities; it must have "the quality of law" in a state under the rule of law, and must not be capable of being arbitrarily applied. To this end:[33]

> Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.

And thirdly, domestic rules that are relied on to limit fundamental rights – e.g., rules that allow for access to personal data by state authorities – should not grant excessive discretion to those exercising power on the basis of those rules.

In the case of *Silver v. the UK*,[34] the respondent government accepted that unpublished orders and instructions on the screening of prisoners' correspondence could not as such be relied on – although overall the Court did not hold that the regime as a whole was not based on "law" because those orders and instructions operated within an accessible framework. Even so, the Court stressed in that case that:

> A law which confers a discretion must indicate the scope of that discretion.
>
> (para. 88)

The Court expanded on this in *Al-Nashif*, in which the applicant had been expelled from Bulgaria on national security grounds:[35]

> It would be contrary to the rule of law for the legal discretion granted to the executive in areas affecting fundamental rights to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the

[33] ECtHR, plenary judgment in the case of *The Sunday Times v. the United Kingdom*, 26 April 1979, para. 49, emphasis added, at: http://hudoc.echr.coe.int/eng?i=001-57584

[34] ECtHR, chamber judgment in the case of *Silver v. the United Kingdom*, 25 March 1983, at: http://hudoc.echr.coe.int/eng?i=001-57577

[35] ECtHR, section judgment in the case of *Al-Nashif v. Bulgaria*, 20 June 2002 (final since 20 September 2002), para. 119, at: http://hudoc.echr.coe.int/eng?i=001-60522

> manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

Moreover, the more severe an interference is that may be allowed under the rules, the clearer the rules must be. Thus, in the case of *Kruslin v. France*, the Court held that:[36]

> Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.

In sum: Secret or excessively vague rules, or rules that grant unfettered discretion, do not constitute "law" in the European human rights sense.

It follows that the absence of any of the data subject rights listed under the previous heading from any third-country laws being assessed on adequacy will raise serious doubts as to whether those laws provide for "essentially equivalent" protection to the GDPR. The laws of the third country should at the very least include the rights of information, access and rectification: without those, no third country law can be said to provide adequate data protection. There must also be clear limitations on profiling and automated individual decision-making.

Moreover, even if the main rights are recognised, they should not be subject to what would be seen in the EU as excessive carve-outs or exceptions: exceptions and derogations from data subject rights in third-party laws that are not limited to serving a major societal interest, or that are too vague or that grant excessive discretion cannot be said to provide "equivalent protection" to the GDPR. If limitations on those rights are imposed under secret rules (or secret interpretations of the rules), that also precludes a finding of "essential equivalence".

Restrictions on onward transfers

Under the third country's law, arrangements must be put in place to ensure that any onward transfers of EU personal data from the third country to another third country that has not been held to provide "adequate"/"essentially equivalent" protection compared to the GDPR (or, if an adequacy decision is limited to certain sectors or entities, from a covered entity in the third country to another entity in the third country that is not covered), do not undermine the protection of the data. This can generally be assured by contractual means (provided these are enforceable) – but not in relation to access to the data by the authorities of the third country in question (see below, at 2.3.2).

Laws in third countries that do not meet all of the above demanding tests, in all of the above respects – scope, purpose specification and limitation, grounds for lawful processing, sensitive data, informing of data subjects, data subject rights and restrictions – cannot be said to provide "adequate"/"essentially equivalent" protection to the EU GDPR.

2.3.1.2 General procedural/enforcement requirements for adequacy

It is a crucial element of European data protection law in general and the GDPR in particular, that in each country, there must be one or more independent public authorities with responsibility for ensuring compliance with the relevant data protection instruments. This requirement was first set out in Article 28(1) of the 1995 EC Data Protection Directive (Directive 95/46/EC) and then added to the

[36] ECtHR, chamber judgment in the case of *Kruslin v France*, 24 April 1990, para. 33, at: http://hudoc.echr.coe.int/eng?i=001-57626

Council of Europe regime (in order to bring it into line with the 1995 Directive) by means of the 2001 Additional Protocol to the 1981 Data Protection Convention (Article 1).[37] In the EU, this principle in fact derives from primary Union law including Article 8(3) of the Charter of Fundamental Rights and Article 16(2) of the Treaty on the Functioning of the European Union – which underlines its crucial importance.[38]

In 2010 and 2012, the CJEU, at the request of the Commission, assessed whether the German and Austrian data protection authorities, as then constituted, could exercise their functions "with complete independence" within the meaning of the second subparagraph of Article 28(1) of Directive 95/46. It held that , and held (with reference to the 2010 case of *Commission v. Germany*, Case C-518/07) that the words "with complete independence" must be given an autonomous interpretation; that they "*should be interpreted as meaning that the supervisory authorities for the protection of personal data must enjoy an independence which allows them to perform their duties free from external influence*"; and that "*those authorities must remain free from any external influence, direct or indirect, which is liable to have an effect on their decisions.*"[39]. Purely "functional" independence does not suffice; rather:[40]

> The independence required under the second subparagraph of Article 28(1) of Directive 95/46 is intended to preclude not only direct influence, in the form of instructions, but also … any indirect influence which is liable to have an effect on the supervisory authority's decisions.

In the light of these judgments, the GDPR greatly expanded on the requirements of the mandatory supervisory authorities: see Chapter VI, section 1, *Independent status*, in particular Article 52, *Independence*.

Without going into detail here,[41] it should be stressed that a third country can only be held to provide "adequate" protection to personal data if, in this "procedural/enforcement" respect, too, it provides "essentially equivalent" protection to that accorded by the GDPR (and the Charter and the Treaties). There is some flexibility in this respect – but the essence of independence and effectiveness must be in place. As the Article 29 Working Party put it in its Adequacy Referential, with reference to *Schrems I*:[42]

> [a]lthough the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union, a system consistent with the European one must be [in place].

Such a system, it said, is "characterized by the existence of the following elements":[43]

- there must be one or more "completely independent" and impartial supervisory authorities with effective supervisory and enforcement powers;
- the system should ensure "a good level of compliance" in practice, which can be ensured through sanctions, verifications and audits;

---

[37] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, CETS No. 181.

[38] CJEU Grand Chamber judgment of 16 October 2012 in Case C-614/10, *European Commission v. Republic of Austria*, ECLI:EU:C:2012:631, para. 36.

[39] *Idem*, paras. 40 – 41, with reference to the CJEU Grand Chamber judgment of 9 March 2010 in Case 518/07, *European Commission v. Federal Republic of Germany*, ECLI:EU:C2010:125, paras. 19, 25, 30 and 50.

[40] *Idem*, paras. 42 – 43.

[41] For a detailed discussion, see the commentary on Article 52, Independence, by Thomas Zerdick in Kuner *et al*., *The EU General Data Protection Regulation – A Commentary*, OUP, 2020.

[42] WP29 *Adequacy Referential (*footnote 26), section C.

[43] *Idem* (paraphrased).

- the system should ensure accountability, by "oblig[ing] data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority", e.g., through data protection impact assessments, the keeping of records or log files of data processing activities, the designation of data protection officers, or data protection by design and by default; and
- the system must provide "support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms".

We should mention that there have been serious questions about the effectiveness of enforcement by the supervisory authorities in the EU Member States. As the European Parliament put it:[44]

> there is a patchwork of national procedures and practices, which is a challenge for the cooperation mechanism set out in the GDPR for cross-border complaints; … there is a lack of clear deadlines, a generally slow pace of proceedings, a lack of sufficient resources for supervisory authorities, in certain cases a lack of willingness or of efficient use of already allocated resources; [and] there is a current concentration of complaints against alleged infringements by big tech companies in the hands of a single national authority, which has led to an enforcement bottleneck.

In practice and specifically as concerns the USA, the issue of procedural protection has arisen in particular in relation to access to personal data by third country (i.e., US) authorities. We will therefore return to that issue in section 3.

2.3.1.3 Requirements relating to access to personal data by state authorities

The EU requirements in relation to access to personal data by state authorities are complicated because they differentiate between access generally, access by law enforcement agencies and access by state intelligence agencies, and between what we will call "indirect access", i.e., access to data obtained under orders issued to companies such as electronic communication providers that are subject to EU data protection law and what we will call "direct access", i.e., access to data gained through surreptitious "hacking" into providers' systems (and in that regard there is a further distinction between direct access by law enforcement agencies – who are subject to EU data protection law [the Law Enforcement Directive] – and direct access by intelligence agencies, who are not subject to EU law at all, but who are subject to the ECHR). Moreover, access to personal data that are subject to EU data protection law by intelligence agencies of third countries is assessed differently from access to such data by EU Member States' intelligence agencies.

In this section we examine in turn:

- The issue of access generally;
- CJEU requirements relating to personal data retention obligations imposed on entities that are subject to EU data protection law, for the purpose of allowing access to the retained personal data by EU Member State intelligence agencies for national security purposes;
- CJEU requirements relating to indirect or direct access to personal data by third country intelligence agencies;
- ECtHR and national constitutional requirements relating to direct access to personal data by EU Member States' intelligence agencies; and

[44] European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II') (footnote 200, above), preliminary point G.

- Accusations of hypocrisy and "double standards" levelled against the EU and the EU Member States by the USA.

The issue of access generally

It follows from the general principles we set out at 2.2.1, that (a) EU Member States should impose substantive limits on access to (or disclosure of) personal data that are processed by private or public entities for their own purposes by (or to) other public entities for other purposes, and (b) that the rules governing such access must be subject to effective procedural/enforcement guarantees.

In terms of substance, such exceptional access (or disclosure), contrary to the purpose limitation principle, must be based on "law" (i.e., on published, clear, precise and in their application foreseeable legal rules), serve a legitimate purpose (that must be specified in specific, restrictive terms in the law), and be necessary and proportionate to that aim. The CJEU confirmed this, e.g., in relation to the disclosure of passenger name record (PNR) data to Canadian authorities when it held that the proposed Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record Data could not be concluded as proposed, *inter alia*, because it did not "*determine in a clear and precise manner the PNR data to be transferred from the European Union to Canada*", or the modalities of and limitations on the use of the data.[45]

It follows that, for a positive adequacy decision, a third country must also provide "essentially equivalent" protection to EU data protection law in that respect. In other words, the rules in a third country should quite generally limit access to (or disclosure of) personal data that are processed by private or public entities for their own purposes by (or to) other public entities of the third country for other purposes; the rules on such access in such third countries should be published, clear and precise and foreseeable in their application; and the exceptional public authorities access should be limited to what is necessary to achieve a legitimate aim, and be proportionate to that aim.

A third country that has laws that allow its authorities generally sweeping access to personal data (including data transferred from the EU) held by private entities or other authorities in that country, under laws that did not meet those basic rule of law requirements, cannot be held to provide "adequate"/"essentially equivalent" protection to such data compared to the GDPR.

The issue of procedural/enforcement guarantees is addressed by the CJEU in the light of Article 47 of the EU Charter of Fundamental Rights that reads as follows:

> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
>
> Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
>
> Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

[45] CJEU, Grand Chamber *Opinion on the proposed Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record Data* (Opinion 1/15), 26 July 2017, ECLI:EU:C:2017:592, para. 232, point 3.

The first paragraph is based on Article 13 of the ECHR that reads:

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

However, as the EU Fundamental Rights Agency (FRA) notes:[46]

> in [European] Union law the protection is more extensive since it guarantees the right to **an effective remedy** before a **court**. (emphases added)

Specifically, the Court has held that:[47]

> it is apparent from the Court's case-law that [Article 47 of the Charter] constitutes a reaffirmation of **the principle of effective judicial protection**, a general principle of European Union law stemming from the constitutional traditions common to the Member States (emphases added)

Or as the Court put it, even more forcefully, in *Schrems II*, with reference to both "settled case-law" and specifically *Schrems I*, para. 95:

> According to settled case-law, **the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.** Thus, **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 her, 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**.
>
> (para. 187, emphases added)

It follows that a third country that does not have in place judicial (or at least quasi-judicial) oversight over access to personal data by its agencies, cannot be held to provide "adequate"/"essentially equivalent" protection to such data compared to the GDPR.

These issues have special force in relation to **access to data by state intelligence agencies**, in particular under laws that allow for mass surveillance/bulk acquisition of data.

In that respect, however, it is important to recall the national security exemption in the EU Treaties, discussed at 2.2.2 – and that that exemption (a) is limited and (b) does not apply to third countries.

Consequently:

- there are CJEU standards in relation to laws that impose obligations on private entities to retain personal data (or even collect it), for the purpose of enabling access to those data by EU Member States intelligence agencies for national security purposes (what we will call "indirect/mandatorily facilitated access" to data by such agencies), typically, by requiring such entities to hand over data on demand ("push" access on demand), or more insidiously, by requiring such entities to build "back doors" into their systems through which the intelligence agencies can "pull" any data they wish themselves, without the entities even knowing or controlling what data are "pulled" (discretionary "pull" access);

---

[46] EU Fundamental Rights Agency, *EU Charter of Fundamental Rights, Article 47 commentary*, at: https://fra.europa.eu/en/eu-charter/article/47-right-effective-remedy-and-fair-trial

[47] CJEU, Third Chamber Judgment of 27 June 2013 in Case C-93/12, *ET Agrokonsulting-04-Velko Stoyanov v. Izpalnitelen direktor na Darzhaven fond 'Zemedelie' – Razplashtatelna agentsia*, para. 59, with references to, *inter alia*, Case 222/84 *Johnston* [1986] ECR 1651, paragraph 18; Case C-432/05 *Unibet* [2007] ECR I-2271, paragraph 37; and Case C-334/12 *RX-II Arango Jaramillo and Others v EIB* [2013] ECR, paragraph 40. Emphasis added.

- there are also CJEU standards in relation to both "indirect/mandatorily facilitated access" and "direct" access to personal data by the intelligence agencies of third countries – and these relate specifically to that issue in relation to the US intelligence agencies;
- but there are no CJEU standards in relation to direct access to personal data by EU Member States' intelligence agencies, typically, by "hacking" into providers' systems or into communication infrastructure such as undersea Internet cables. Rather, as noted below under the heading "*ECtHR and national constitutional requirements relating to direct access to personal data by EU Member States' intelligence agencies*", in that regard only the ECHR standards and national constitutional standards apply (although non-compliance with those standards can have implications in EU law, too – as discussed in section 2.2.2.3);

Below, we first discuss these standards separately, in the above order (distinguishing where relevant between the substantive and the procedural/enforcement requirements), before discussing whether there are major differences between them (taking into account criticism of EU "double standards" from the USA).

CJEU requirements relating to personal data retention obligations imposed on entities that are subject to EU data protection law, for the purpose of allowing access to the retained personal data by EU Member State intelligence agencies for national security purposes

In *Digital Rights Ireland*, the CJEU assessed the compatibility with the EU Charter of Fundamental Rights of Directive 2006/24, the so-called Data Retention Directive.[48] This directive had as its main objective:

> to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism.
>
> (*Digital Rights Ireland*, para. 24)

The Court held (i) that the the duty of mandatory data retention imposed on providers in itself constitutes a "*particularly serious*" interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter (paras. 34, 36 and 37); (ii) that in this respect "*it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way*" (para. 33); and (iii) that accessing the retained data by the competent national authorities constitutes a *further* interference with that fundamental right (para. 35).

The question was whether the Directive adhered to the rule of law requirements already noted ("law", legitimate aim, necessity and proportionality: cf. para. 38). The Court held that the interference, though particularly serious, was not "*such as to adversely affect the essence of those rights given that … the directive does not permit the acquisition of knowledge of the content of the electronic communications as such*" (para. 39). (This relates to the fact that under the Charter any interference with the "essence" of a fundamental right is *ipso facto* incompatible with the Charter, without any need to assess the legitimacy of the aim of the interference or its necessity or proportionality: cf. Article 52(1), first sentence, CFR.)

[48] CJEU, Grand Chamber judgment in Joined Cases C 293/12 and C 594/12, *Digital Rights Ireland* and *Kärntner Landesregierung*, ECLI:EU:C:2014:238. In the quotes and paraphrases in the text, the extensive cross-references to earlier case-law have been omitted for the sake of brevity.

The fight against international terrorism in order to maintain international peace and security and the fight against serious crime in order to ensure public security were, of course, legitimate aims in a democratic society (paras. 42-44). The issue therefore was whether mandatory retention of communication data (other than content data) was proportionate to those aims (para. 45).

In that regard, the Court held that (to limit ourselves to the core paragraphs):

> in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict. (para. 48)
>
> [D]erogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. (para. 52)
>
> Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. (para. 54)

However, by contrast, the Court found that the Directive:

> Covered, in a generalised manner, all persons and all means of electronic communication 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;
>
> Affected, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions';
>
> Applied even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime;
>
> Did not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, [was] not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences;
>
> Failed to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use but rather simply referred in a general manner to serious crime, as defined by each Member State in its national law;
>
> Did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use;
>
> Did not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained was limited to what is strictly necessary in the light of the objective pursued;
>
> Required that the data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned;
>
> Did not state that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.
>
> (paras. 57 – 64, paraphrased)

The Directive therefore violated Articles 7 and 8 of the Charter (para. 65).

The Court reaffirmed the above position and expanded on it in its subsequent judgment in *Tele-2/Watson*.[49] In particular, the Court expressly said that:

> **Article 15(1) of [the e-Privacy Directive], read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime**, *provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*
>
> (para. 108, emphases added)

It therefore reiterated the conditions already indicated in *Digital Rights Ireland* as to the need for the national legislation (itself) to:

> lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary.
>
> (para. 109, cross-references omitted)

Data retention for the purpose of fighting serious crime or countering a serious risk to public security must meet "**objective criteria**, that establish a connection between the data to be retained and the objective pursued" (para. 110, emphasis added); and must be based on:

> **objective evidence** which makes it possible to identify a public whose data is likely to reveal **a link, at least an indirect one, with serious criminal offences**, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.
>
> (para. 111, emphasis added)

The Court somewhat **qualified** this in its Grand Chamber judgment in *La Quadrature du Net* (*LQDN*), already mentioned in section 2.2,[50] in relation to **certain particularly grave threats**, i.e.:

> [threats to] the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of **activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.**
>
> [The objective of protecting the state and its population from such special threats] goes beyond … inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in the preceding paragraph can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements

[49] CJEU GC judgment of 21 December 2016 in *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* ("*Tele-2/Watson*"), ECLI:EU:C:2016:970.

[50] See footnote 17, above.

> laid down in Article 52(1) of the Charter [i.e., legality, necessity and proportionality – DK/IB], **the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives**.
>
> Thus, **Article 15(1) of [the e-Privacy Directive], read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, as referred to in [the two previous paragraphs], to national security which is shown to be genuine and present or foreseeable. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection … with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.**
>
> (paras. 135 – 137)

The threats mentioned in the first of the above paragraphs (para. 135) appear to us to correspond to the kinds of threats mentioned in the "derogation clause" in the European Convention on Human Rights, Article 15:

> (1) In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.
>
> …

Such situations are strictly circumscribed,[51] and any European state wishing to rely on this clause must declare it to the Secretary General of the Council of Europe (Article 15(3)). Suffice it to note here that while the precise limitations of the data retention obligations that EU states can impose (in particular in relation to national security) remain somewhat unclear, it is clear from the above that EU law imposes exacting, detailed demands on any EU rules or any rules of any EU Member State that wants to introduce mandatory retention of communications data (or other sensitive data, or indeed non-sensitive data) that are processed subject to EU data protection law.

However, the EU and the Member States have been reluctant to come up with laws that actually meet those standards – something that is rightly criticised by the European Parliament and civil society.[52]

Indeed, very recently, the French *Conseil d'État* (the country's highest administrative court) issued a ruling on the French data retention law that upheld that law on the basis of the above paragraphs from

---

[51] For details, see *Law of the European Convention on Human Rights* (footnote 14), chapter 16.

[52] See Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe*, September 2017, at:
https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf
("*[The] basic standard [of legality, necessity and proportionality] laid down by the CJEU [in DRI and Tele-2/Watson] is not adhered to by most EU member states, despite their legal obligation to comply with the Court's jurisprudence.*" p. 4). Regrettably, this is still the case. See EDRi/ILP Lab, *Data Retention Revisited*, October 2020, at:
https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

LQDN[53] – even though France has not declared a state of emergency or invoked Article 15 under the ECHR.

Specifically, the *Conseil* stretched the exceptional permissibility of targeted, preventive data retention to counter real and immediate threats to the very fabric and life of the nation, linked to specific (geographical or other) targets (*LQDN* judgment, paras. 108 – 111, quoted above) to allow for such preventive data retention of communication metadata to counter pervasive threats from terrorism that, in the present political climate, could take place anywhere in France, at any time. Indeed, the *Conseil* applied the rules relating to the highly exceptional threats noted in *LQDN* to a much wider range of threats to French national interests, including industrial and economic espionage and the rise of radical and extremist groups (see para. 44 of the ruling).

In effect, the *Conseil d' État* turned the (high) exception suggested in the above paragraphs in the *LQDN* judgment into the rule – it would appear to us, in direct contradiction of the CJEU when it ruled, in its *Tele-2/Watson* judgment, that:

> in so far as **Article 15(1) of [the e-Privacy Directive]** enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court's settled case-law, be interpreted strictly. That provision **cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of [the e-Privacy Directive], to become the rule, if the latter provision is not to be rendered largely meaningless**.
>
> (*Tele-2/Watson*, para. 89, emphasis added)

The authors agree with Arthur Messaud of *La Quadrature du Net* (which brought the case to the *Conseil d' État*), that the *Conseil* "*disingenuously misinterpret[ed] the La Quadrature du Net (LQDN) CJEU ruling*".[54] The case cannot be further appealed (in particular, not to the *Conseil Constitutionnel*). However, the French Government is still changing the "Intelligence Law" and the rules on data retention. At the time of writing (June 2021), the bill is under discussion in the *Assemblée Nationale*, and it is quite possible that the *Conseil Constitutionnel* will be asked to issue a decision on its compatibility with the French Constitution and with EU law.

But that aside, **a third country cannot be held to provide "adequate"/"essentially equivalent" protection to personal data compared to the EU if it has laws which (like the invalidated EU Data Retention Directive) imposes excessive duties on providers of communication services to retain such data and make it accessible to the third countries law enforcement (or intelligence) agencies, and/or which do not provide appropriate procedural safeguards in this regard. Third countries that impose such duties under laws that do not contain the kinds of limitations and safeguards indicated by the CJEU cannot be held to provide "adequate" protection to the relevant personal (communications) data.**

(NB: We discuss the suggestion that the EU and the EU Member States are hypocritical in this respect, because they do not actually themselves adhere to the Charter as interpreted by the Court of Justice, and other allegations of "double standards", below.)

---

[53] *Conseil d'État*, ruling of 21 April 2021 in case No. 393099, ECLI:FR:CEASS:2021:393099.20210421, at: https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043411127

[54] Arthur Messaud and Noémie Levain, *CJEU rulings v. French intelligence legislation*, about:intel, 14 May 2021, at: https://aboutintel.eu/cjeu-french-intelligence-legislation/

CJEU requirements relating to indirect or direct access to personal data by third country intelligence agencies

As already noted, Article 45(2) GDPR expressly requires that the Commission, when assessing the adequacy of the level of protection in a third country, must "*in particular, take account of*" (*inter alia*) "*relevant legislation … including concerning … national security … and the access of public authorities to personal data*" (under such laws), as well as "*the existence and effective functioning of one or more independent supervisory authorities in the third country … with responsibility for ensuring and enforcing compliance with the data protection rules.*"

The first point to be made in this regard is that, as already noted, direct remote access by an entity from a third country to data located in the EU is also considered a transfer.[55] Moreover, in a recent decision of the *French Conseil d'État*, it was held that the use by an EU company of a server in the EU that was managed by an EU-based subsidiary of a US parent company (in casu, Amazon Web Services Luxembourg SARL, a subsidiary of Amazon Web Services Inc. in the USA) also exposed the data on the server to access by the authorities in the USA, because the parent company was subject to US surveillance laws and could be ordered to order its subsidiary to allow access. [56] The use of a cloud-based server in a third country will also often raise issues over possible access to the data in the server by authorities of the third country. Dutch and German authorities have therefore raised serious doubts as to whether Microsoft's cloud-based Office 365 suite could be used (in particular, by public bodies and educational establishments) in a GDPR-compatible way.[57]

On the more general issues, the Court noted in its 2016 *Schrems I* judgment,[58] that (contrary to the above stipulations in the GDPR) the decision in which the EU Commission held that the Safe Harbour agreement provided adequate protection (Decision 2000/520) wrongly did:

> not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.
>
> [And neither] does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind.
>
> (paras. 88 – 89)

Those were the main reasons for invalidating the Safe Harbour agreement (which was then replaced by the Privacy Shield Agreement until that too was invalidated by the Court).

---

55 See footnote 24.

56 *Conseil d'État* order of 12 March 2021 in urgency proceedings (acting as *juge des référés*) N° 450163, *Association Interhop et autres*, at:
https://www.dalloz.fr/documentation/Document?id=CE_LIEUVIDE_2021-03-12_450163#texte-integral

57 *DPIA of Diagnostic Data in Microsoft Office ProPlus*, commissioned by the Netherlands' Ministry of Justice and Security, 5 November 2018, p. 8, emphasis added, at:
https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/
"*Microsoft Office 365: Bewertung Der Datenschutz-Konferenz zu undifferenziert – Nachbesserungen gleichwohl geboten*" – press statement by the DPAs of Stuttgart, Munich, Ansbach, Wiesbaden and Saarbrücken, 2 October 2020, at: https://www.datenschutz.saarland.de/ueber-uns/oeffentlichkeitsarbeit/detail/pressemitteilung-vom-02102020-stuttgart-muenchen-ansbach-wiesbaden-saarbruecken/

58 See footnote 1.

On the first point (substantive limitations), the Court reiterated in *Schrems II*,[59] first of all, that:

> the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter [right to private and family life, home and communications, and right to protection of personal data], whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.
>
> (para. 171, case references omitted)

Access by authorities of a third country to personal data of EU persons that are transferred to the third country (or that are accessed directly by such authorities while in the EU) therefore *ipso facto* also constitutes an interference with – and a limitation on – the rights of the EU persons concerned. This means that the principles discussed above, at 2.3.1.1 (in particular under the sub-heading "*processing on the basis of law*"), must be applied to such access. In the words of the Court:

> in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be **provided for by law** and **respect the essence of those rights and freedoms**. Under the second sentence of Article 52(1) of the Charter, subject to the principle of **proportionality**, limitations may be made to those rights and freedoms only if they are **necessary** and **genuinely meet objectives of general interest recognised by the Union** or the need to protect **the rights and freedoms of others**.
>
> Following from the previous point, it should be added that **the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned** (…).
>
> Lastly, in order to satisfy the requirement of proportionality according to which **derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary**, the legislation in question which entails the interference must lay down **clear and precise rules** governing the scope and application of the measure in question and imposing **minimum safeguards**, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. **[The legislation] must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.** The need for such safeguards is all the greater where personal data is subject to automated processing (…).
>
> (*Schrems II*, paras. 174 – 176, emphases added, with reference to CJEU Opinion 1/15, discussed at the beginning of the present sub-section)

The Court then applied these principles to the legal regimes under which US law enforcement and intelligence authorities could demand or gain access to data including personal data on individuals in the EU. The Court examined in detail in particular the US President-issued Executive Order 12333 (EO 12333) and Presidential Policy Directive 28 (PPD-28), as well as Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the United States Foreign Intelligence Surveillance Court (FISC), established under it. The Court assessed these regimes and in particular the limitations and guarantees inherent in them by reference to their descriptions in the Privacy Shield adequacy decision (quoted in the section

[59] See footnote 3.

in the judgment headed "*The Privacy Shield Decision*", at paras. 42 – 49 of the judgment). Without going into details here,[60] the Court held as follows:

> It is thus apparent that **Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances … that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter**…
>
> It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection' … That possibility, which allows, in the context of the surveillance programmes based on **EO 12333**, access to data in transit to the United States without that access being subject to any judicial review, **does not**, in any event, **delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data**.
>
> **It follows therefore that neither Section 702 of the FISA, nor EO 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.**
>
> (paras. 180 and 183 – 184, emphases added)

The EDPB has since clarified the kinds of limitations and guarantees that should be in place in order to ensure that access to personal data by intelligence agencies meets the European – and in particular the EU Treaties and Charter – requirements, in its recommendations 02/2020 on the European Essential Guarantees for surveillance measures (EEGs).[61] Here, it must suffice to note that, in line with our discussion of data protection as a fundamental right in sub-section 1.2.1, the EEGs note the following:[62]

> Following the analysis of the jurisprudence, the EDPB considers that the applicable legal requirements to make the limitations to the data protection and privacy rights recognised by the Charter [for the purposes of national security] justifiable can be summarised in four European Essential Guarantees:
>
> A. Processing should be based on clear, precise and accessible rules [that are foreseeable in their application];
>
> B. [Strict] necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated [which must relate to a serious threat to national security that is shown to be genuine and present or foreseeable];
>
> C. An independent oversight mechanism should exist; and
>
> D. Effective remedies need to be available to the individual.
>
> The Guarantees are based on the fundamental rights to privacy and data protection that apply to everyone, irrespective of their nationality.

---

[60] For those details, see the Commission *Privacy Shield decision* and the parts of it quoted in these paragraphs in the *Schrems II* judgment and section 3.5, below.

[61] EDPB, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, adopted on 10 November 2020, at:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

[62] *Idem*, para. 24.

> (Words in square brackets that reflect the elaborations on each of the "essential guarantees" provided for in the EEGs added. We refer to the full document for important further detail.)

Laws in third countries that do not meet the above-mentioned CJEU standards as reflected in the European Essential Guarantees for surveillance measures (EEGs) tests cannot be said to provide "essentially equivalent" protection to the GDPR.

On the issue of procedural/enforcement guarantees (the second point in *Schrems I*, paras. 88 – 89, quoted earlier) the Article 29 Working Party pointed out, with reference to that judgment, that, in relation to the issue of access to data by this country intelligence agencies:[63]

> [a]lthough the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union, a system consistent with the European one must be [in place].

Such a system, it said, is "*characterized by the existence of the following elements*":[64]

- there must be one or more "completely independent" and impartial supervisory authorities with effective supervisory and enforcement powers;
- the system should ensure "a good level of compliance" in practice, which can be ensured through sanctions, verifications and audits;
- the system should ensure accountability, by "oblig[ing] data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority", e.g., through data protection impact assessments, the keeping of records or log files of data processing activities, the designation of data protection officers, or data protection by design and by default; and
- the system must provide "support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms".

The existence and quality of procedural guarantees in the USA against undue surveillance, and their availability to EU persons, was one of the two main issues in *Schrems II* (the other was the substantive question of access to transferred data by US authorities itself, discussed above).

The CJEU assessed the issue in the light of Article 47 of the EU Charter (quoted in paragraph (i)) and its ruling (also quoted there) 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 her, 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*" (*Schrems I*, para. 187).

In *Schrems II*, the Court went on to discuss both the absence of proper judicial redress for EU individuals under the relevant US laws in relation to the collecting of personal data on them by the US intelligence authorities, and the question of whether this was compensated for by the introduction of an Ombudsman Mechanism in 2016. [65] In the first respect, the Court ruled in relation to the main applicable legal US instruments, PPD-28 and E.O. 12333:

> **[T]he US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities.**

---

63 WP29 *Adequacy Referential* (footnote 26), section C.

64 *Idem* (paraphrased).

65 The Ombudsperson Mechanism is described in a letter from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to the Privacy Shield decision.

> **Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter**…
>
> **As regards the monitoring programmes based on EO 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either.**
>
> (paras. 181 – 182, emphases added)

And as concerns the Ombudsman Mechanism, the Court held this:

> **does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.**
>
> (para. 197, emphases added, cross-references to earlier case-law and the Advocate General's opinion omitted)

Under EU law, third countries that do not provide effective judicial remedies to EU persons in relation to the processing of those persons' personal data in those countries, including in respect of access to those data by the third country's intelligence agencies, cannot be held to provide "essentially equivalent" protection to the GDPR.[66]

ECtHR and national constitutional requirements relating to direct access to personal data by EU Member States' intelligence agencies

As noted above, at 2.2.2.3, EU law does not apply to direct access to personal data by EU Member States' intelligence agencies (i.e., the Member States' agencies responsible for safeguarding national security),[67] i.e., by the agencies "hacking" into providers' systems or into communication infrastructure such as undersea Internet cables. However, as also noted there, the EU Member States, all being party to the ECHR, are required to ensure that such access does meet the requirements of that Convention – and any systemic failure by an EU Member State to comply with the Convention in that regard would be incompatible with being a Member in good standing of the EU, too.

There is extensive case-law of the European Court of Human Rights relating to state surveillance.[68] Here, it will suffice to focus on the very recent Grand Chamber judgment in *Big Brother Watch and others v. the United Kingdom*,[69] which dealt with the bulk interception, by the UK intelligence agencies, of data flowing through the international submarine fibre-optic cables operated by communication service

---

[66] The USA criticised the application of the EEGs to third countries, given that the Court of Justice of the EU cannot apply those guarantees to surveillance activities by EU Member States in relation to their national security (because actions by EU Member States in that area are completely outside the scope of EU law including the Charter and the GDPR). We discuss this below.

[67] When EU Member States' intelligence agencies act in relation to "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" – as they increasingly do – they are subject to EU law, more specifically to the Law Enforcement Directive. Regrettably, the distinctions between intelligence/national security activities and law enforcement activities, and between the agencies involved in these supposedly separate matters, are increasingly blurred. See the Council of Europe's Commissioner for Human Rights 2014 *Issue Paper* on *The Rule of Law on the Internet and in the wider digital environment* (footnote 8), section 1.2, *Cybercrime, cybersecurity, terrorism and national security*, and footnote 6 on p. 29 of that paper.

[68] For an overview of the standards set by the case-law prior to the *BBW* GC judgment, see Douwe Korff & Ian Brown, *The inadequacy of UK data protection law*, Part Two, *UK Surveillance*, submission to EU bodies, November 2020, section 3.1, *Issues and applicable standards*, at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf

[69] See footnote 10.

providers;[70] with the sharing of the data by the UK with the US and other states;[71] with "acquisition of communications data", i.e., the obtaining of such data by the agencies from such service providers under legal orders;[72] and related procedural/enforcement issues and safeguards. As Farrell and Newman noted, "The internet and other global telecommunications networks made it easy to gather information in bulk, while new data techniques allowed analysts to sift through the huge amounts of data collected in search of valuable intelligence. Intelligence officials [are] now worried less about how to get data, and more about avoiding paralysis in the face of the enormous piles of material that accumulated every day on their servers."[73]

The *BBW* GC judgment summarised its earlier case-law in interception of communications (including the Chamber judgment in the case),[74] and then built on and further clarified that earlier case-law (and in the process appears to have weakened its position, as noted below).

As already mentioned in section 2.2.1, it is notable that (as in the proceedings before the First Chamber) in the *BBW* case, as in *Centrum för Rättvisa*, neither the United Kingdom nor Sweden even tried to argue that the Convention should not be applied to its surveillance activities that clearly extended (and still extend) to communications of and between individuals who are neither inside its territory (or territories) nor its nationals or residents.

Here, it must suffice to note that the Court held the following (in paraphrase):

- The Court "proceed[ed] on the assumption" that, in relation to bulk data collection that is mainly directed at the communications of individuals outside of the territory of the state (cf. para. 344, quoted below), "the matters complained of fell within the jurisdictional competence" of the state (para. 272). In fact, as already noted in section 2.2.1, the UK (and in *Rättvisa*, Sweden) did not even try to argue otherwise. In other words, the ECHR applies to extra-territorial surveillance by Contracting Parties.
- Under the ECHR, surveillance and bulk data collection inherently constitute "interferences" with the right to privacy and confidentiality of communications and Article 8 ECHR (which guarantees these rights) applies to all stages of such surveillance including the interception and initial retention of communication data (para. 330). All such measures, at all stages, must therefore be based on "law" and "necessary" and "proportionate" to a legitimate aim (which national security of course as such is) (para. 332).
- States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security (para. 338, confirming earlier case-law, in particular Weber and Saravia).
- The decision to operate a bulk interception regime falls within this wide margin of appreciation, i.e., the decision of a State to establish such a regime – to allow bulk data collection for national

---

[70] See the section in the GC judgment on "I. Relevant Domestic Law", sub-section A *The interception of communications*, paras. 61 – 102. For an overview of the relevant activities by the UK agencies (in particular, the UK's Government Communications Headquarters, GCHQ) and of the uses of the intercepted data, see Douwe Korff & Ian Brown, *The inadequacy of UK data protection law*, Part Two, *UK Surveillance* (footnote 68), sections 2.2 and 2.3.

[71] See sub-section B, *Intelligence sharing*, paras. 103 – 116. This is discussed in Korff & Brown (previous footnote), section 2.4.

[72] See sub-section C, *Acquisition of communications data*, paras. 117 – 121.

[73] Henry Farrell and Abraham Newman, *Schrems II Offers an Opportunity—If the U.S. Wants to Take It*, Lawfare, 28 July 2020, at: https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it

[74] ECtHR, First Section judgment of 13 September 2018, summarised in the GC judgment, paras. 274 – 276.

security purposes – is not in itself necessarily in breach of the Convention (para. 340, again confirming earlier case-law, in particular Weber and Saravia and Liberty).

- The acquisition of related communications data (metadata) through bulk interception is not necessarily less intrusive than the acquisition of content. The Court therefore considered that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content (para. 363, with reference to para. 342), although "the legal provisions governing [the treatment of related/metadata] may not necessarily have to be identical in every respect to those governing the treatment of content" (para. 364).

Beyond this, the Court felt it necessary to "further develop" the case-law, first of all, because bulk interception is different from targeted interception, with which the earlier case-law was mainly concerned (para. 343):

> [B]ulk interception is generally directed at international communications (that is, communications physically travelling across State borders) … [and] Council of Europe member States operating a bulk interception regime appear to use it for the purposes of foreign intelligence gathering, the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism [rather than to investigate certain serious crimes].
>
> (paras. 344 – 345)

Secondly, "*in the intervening years technological developments have significantly changed the way in which people communicate*":

> Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago (see paragraph 322 above). The scope of the surveillance activity considered in those cases would therefore have been much narrower.
>
> (para. 341)

The Court therefore agreed with the Chamber that the six "minimum safeguards" that it had developed in relation to targeted interception mainly for law enforcement purposes should be reviewed. In relation to bulk interception for national security/intelligence purposes, it therefore dropped the first two of those safeguards: that the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted should be spelled out in the law, and it held that:

> [T]he requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence.
>
> (para. 348)

In the end, the Court applied the following (partially new, partially more specific, and partially revised) tests to ascertain whether the domestic legal framework (*in casu*, the UK framework) met the requirements of the Convention:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;

5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and
8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

(para. 361, reflecting the Court's considerations in paras. 274 – 275)

Here, it will suffice to note two matters in these respects (beyond the issues of extraterritorial application and the margin of appreciation and its application to bulk data interception, noted earlier). These are, first, that it is clear from the judgment that **the relevant matters should be spelt out in the law itself (or at the least in published rules issues under the law)**: this is not a matter that can be left to, e.g., internal ministerial instructions – and certainly not to unpublished, secret instructions. The same applies to interpretations of the law that affect its application in these respects: at least at the normative level, the rules – and their interpretation should be accessible and sufficiently clear to be foreseeable in their application.

Second, that the system (or systems) of **oversight** is (are) crucial:

> [I]n order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to **"end-to-end safeguards"**, meaning that, at the domestic level:
>
> - that an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken;
> - that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and
> - that the operation should be subject to supervision and independent ex post facto review.
>
> In the Court's view, **these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime** (see also the report of the Venice Commission …, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).[75]
>
> (paras. 349 – 350)

On the first of these, authorisation, the Grand Chamber "agreed with the Chamber that while **judicial authorisation** is an 'important safeguard against arbitrariness' it **is not a 'necessary requirement'**" (para. 351, emphasis added). However, bulk interception should be authorised by **an independent body**; that is, a body which is independent of the executive (para. 351, see further para. 352). In addition, "an **effective remedy** should be available to anyone who suspects that his or her

[75] This is a reference to the 2015 *Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies*, at:
https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e
We note that the Court did not expressly take up other recommendations made by the Venice Commission, such as the recommendation that, in relation to surveillance for intelligence (rather than law enforcement) purposes, "*The power to contact chain (that is, identify people in contact with each other) should be framed narrowly: contact chaining of metadata should normally only be possible for people suspected of actual involvement in particularly seriously offences, such as terrorism.*" (para. 16). However, such more specific requirements can now reasonably be read into the Convention requirements.

communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime" (para. 357, emphasis added). (However, the court acknowledged that if the person concerned is not informed of the surveillance, the nominal availability of a remedy becomes meaningless: see para. 358 – which is why it suggested "*a remedy which does not depend on notification to the interception subject … may even offer better guarantees of a proper procedure than a system based on notification*" (*idem*). But it did not spell out what such an alternative remedy would look like in practice.)

Applying the above criteria, the Court held that the UK regime for bulk data interception did not meet the (essentially procedural) requirements it had spelled out – and that that regime therefore violated both Article 8 (right to private life, home and correspondence) and Article 10 (freedom of expression and the right to seek, receive and impart information) of the Convention (paras. 522 and 528, respectively).

The Court also addressed the issue of **sharing of intelligence between states**:

> it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Consequently, the Court considers that **the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself:**
>
> - First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law.
> - Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer.
> - Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred.
> - Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control.
>
> (para. 362, colon and indents added)

However, its examination on this issue was limited. Specifically, the Court agreed with the Chamber that:

> the interception of communications by foreign intelligence services [read, in the specific context of the case: the USA's intelligence services] could not engage the responsibility of a receiving State {read: the UK], or fall within that State [the UK]'s jurisdiction within the meaning of Article 1 of the Convention, even if the interception was carried out at that State [the UK]'s request.
>
> (para. 495)

The Court held, with reference to the International Law Commission's Article on State Responsibility[76] and the *International Commission of Jurists*' submission on these (para. 493 of the judgment) that is

[76] International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001, at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

would only be different if the receiving State were to be effectively responsible for the other State's surveillance, i.e.:

> if the foreign intelligence services were placed at the disposal of the receiving State and were acting in exercise of elements of the governmental authority of that State (Article 6 [of the ILC Articles]); if the receiving State aided or assisted the foreign intelligence services in intercepting the communications where that amounted to an internationally wrongful act for the State responsible for the services, the receiving State was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the receiving State (Article 16); or if the receiving State exercised direction or control over the foreign Government (Article 17).
>
> (para. 495)

However, "[*t]he Grand Chamber agrees with the Chamber that none of these elements were present in the situation under consideration*" (para. 496). Even so, the Court did consider the issues of **access to information collected by the UK intelligence agencies by other "Five Eyes" intelligence agencies** and the **requesting of intelligence by the UK from other countries**. In respect of the former, the Court noted that:

> In the United Kingdom it would appear that Five Eyes partners could access elements of the product of GCHQ's interception warrants on their own systems.
>
> (para. 396, with reference to further detail in para. 180)

In that respect it held that:

> where material has been intercepted in accordance with domestic law, the Court considers that the transfer of that material to a foreign intelligence partner or international organisation would only give rise to an issue under Article 8 of the Convention if the intercepting State did not first ensure that its intelligence partner, in handling the material, had in place **safeguards capable of preventing abuse and disproportionate interference**, and in particular, could **guarantee the secure storage** of the material and **restrict its onward disclosure**.
>
> …
>
> [W]here intercept material was disclosed to the authorities of a country or territory outside the United Kingdom, the intelligence services had to take **reasonable steps to ensure** that the [foreign] authorities in question had and would maintain **the necessary procedures to safeguard the intercept material**, and to ensure that it was disclosed, copied, distributed and retained only to the minimum extent necessary. The intercept material could not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency and it had to be returned to the issuing agency or securely destroyed when no longer needed. …
>
> (paras. 395 – 396, emphases added)

And it found that:

> **There were therefore safeguards in place to ensure that intelligence partners would guarantee the secure storage of transferred material and restrict its onward disclosure.** A final safeguard, to which the Court attaches particular weight, is the oversight provided by the IC Commissioner and the IPT.
>
> In light of the foregoing, the Court considers that **the precautions to be taken when communicating intercept material to other parties were sufficiently clear and afforded sufficiently robust guarantees against abuse**.
>
> (paras. 398 – 399, emphases added, cross-reference omitted)

In other words, this data sharing – this effectively direct access by US and other intelligence agencies to data collected in bulk by the UK agencies – does not violate the ECHR.

This of course falls far short of the EU GDPR requirement that when personal data are transferred to a third country, that third country must provide "essentially equivalent" protection to that accorded to such data under EU law. Indeed, it also falls short of the similar requirement under the Additional Protocol to the Council of Europe Data Protection Convention (Convention 108) – which the Court did not mention, presumably because the UK has not acceded to that protocol (although the UK is a signatory).

In relation to the UK requesting information from other countries (again, especially the other "Five Eyes" and more especially the USA), the Court held that:

> The protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States; or even, although not directly in issue in the cases at hand, by obtaining such communications through direct access to those States' databases. Therefore, in the Court's view, where a request is made to a non-contracting State for intercept material the request must have a basis in domestic law, and that law must be accessible to the person concerned and foreseeable as to its effects. It will also be necessary to have clear detailed rules which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention.
>
> Upon receipt of the intercept material, the Court considers that the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards, first developed by the Court in its case-law on the interception of communications by Contracting States, are equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If, as the Government contend, States do not always know whether material received from foreign intelligence services is the product of interception, then the Court considers that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept.
>
> Finally, the Court considers that any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent ex post facto review.
>
> (paras. 497 – 499, emphases added, cross-references to earlier case-law omitted)

The Court then found that, in this specific respect, too, there had been no violation of the Convention because:

> the [UK] regime for requesting and receiving intelligence from non-Contracting States [read: in particular the USA] had a clear basis in domestic law and, following the amendment to the [Interceptions of Communications] Code, that law was adequately accessible.
>
> (para. 501)

In the light of these findings, the Grand Chamber held that:

> [T]he [UK] regime for **requesting and receiving intercept material** [read: in particular from the USA] was compatible with Article 8 of the Convention.
>
> (para. 513, emphasis added)

The *BBW* Grand Chamber judgment therefore effectively upholds the sweeping UK – USA/"Five Eyes" data sharing agreements and practices as being in accordance with the Convention. In our opinion, this is the most dangerous aspect of the judgment – and clearly incompatible with the EU standards discussed earlier.

In particular, in our opinion the Court failed to really understand the nature of the interstate surveillance arrangements under which these activities are carried out jointly rather than on the basis of case-by-case requests for information – and indeed apparently often carried out "hand in glove", with the hand being the USA and the agencies in the "glove" the US "partners".[77],[78] It follows that **the *BBW* Grand Chamber judgment in fact does not (as some have suggested) hold that the UK–USA data sharing agreements (let alone the "Five Eyes" agreement more generally) are (is) in accordance with the Convention**. Rather, in our opinion, the Court was enticed to follow the "red herring" of states (more specifically, the UK and the USA between them, and the "Five Eyes") making specific "requests" for specific intelligence from other states, when the real issue is that for states in multilateral intelligence arrangements these activities are carried out jointly rather than on the basis of case-by-case "requests" (and indeed some cases, carried out "hand in glove", with the hand being the USA and the agencies in the "glove" the US "partners").[79] **These wider multinational intelligence cooperation agreements and arrangements still need to be properly assessed under European and international human rights and data protection law** (and then brought into line with the relevant standards: see chapter 4.).

In this study, we are less concerned with the specific defects of UK law (or in *Rättvisa*, of Swedish law). Rather, our aim was simply to tease out from the lengthy judgments the criteria that the Strasbourg Court applies to bulk data interception. These are set out above. Overall, three main matters should be noted: (i) the European Court of Human Rights holds that, because it has to grant Contracting States a wide margin of appreciation in relation to national security issues, it cannot interpret the Convention as prohibiting bulk interception for national security/intelligence purposes *per se*, although it claims to be aware of the major risks to fundamental rights inherent in any such activities; (ii) that claim is rather undermined by the Court's excessively lax approach to international intelligence data sharing; and (iii), rather than prohibiting bulk surveillance and sweeping sharing of intelligence data, the Court focussed only on oversight and procedural protection matters.

There were strong separate opinions by individual judges that criticised the restrictive and deferential approach of the Court to state surveillance. In the words of Judge Pinto De Albuquerque:[80]

---

[77] *Danish secret service helped US spy on Germany's Angela Merkel*, Deutsche Welle, 30 May 2021, at: https://www.dw.com/en/danish-secret-service-helped-us-spy-on-germanys-angela-merkel-report/a-57721901
According to this report, the Danish Defense Intelligence Service, FE, had helped the NSA to spy on leading politicians in Sweden, Norway, the Netherlands and France, as well as Germany, and at least initially without the Danish Government being aware of this.

[78] See Douwe Korff & Ian Brown, *The inadequacy of UK data protection law*, Part Two, *UK Surveillance* (footnote 68), section 2.4, *The UK – USA (and wider "Five Eyes") data sharing arrangements*, with reference, in particular, to the witness statement of *Privacy International*'s then deputy director, Eric King, to the Investigatory Powers Tribunal in the case brought by PI against the agencies, at:
https://privacyinternational.org/sites/default/files/2018-03/2014.06.08%20Eric%20King%20witness%20statement.pdf

[79] See footnote 77.

[80] On more specific points, Judge Pinto De Albuquerque, "*do[es] not agree that 'States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for [national security] purposes*" (para. 33) He notes that "*non-targeted bulk interception is prohibited explicitly or implicitly in twenty-three European States*" and that "*if there is a consensus in Europe on non-targeted bulk interception, the consensus is that it should be prohibited, but this has been ignored by the Court*" (para. 11). Also (with reference to the Venice Commission Report) that "*nothing precludes the possibility that foreign intelligence*

> **This judgment fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests, in that it admits non-targeted surveillance of the content of electronic communications and related communications data, and even worse, the exchange of data with third countries which do not have comparable protection to that of the Council of Europe States.**
>
> This conclusion is all the more justified in view of the CJEU's peremptory rejection of access on a generalised basis to the content of electronic communications , its manifest reluctance regarding general and indiscriminate retention of traffic and location data and its limitation of exchanges of data with foreign intelligence services which do not ensure a level of protection essentially equivalent to that guaranteed by the Charter of Fundamental Rights . On all these three counts, the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe.
>
> For good or ill, and I believe for ill more than for good, with the present judgment the Strasbourg Court has just opened the gates for an electronic "Big Brother" in Europe. If this is the new normal that my learned colleagues in the majority want for Europe, I cannot join them, and this I say with a disenchanted heart, with the same consternation as that exuding from Gregorio Allegri's *Miserere mei, Deus*.
>
> (Dissenting Opinion of Judge Pinto De Albuquerque, concluding paras. 59 – 60)

The judgment and the "*dangerous convergence of the two European courts on the acceptability of the good old 'inevitability of securitisation' narrative in context of intelligence collection and sharing*" are also criticised by leading academics including Monika Zalnieriute, who wrote:[81]

> This convergence around procedural fetishism, and the GC's rulings in *Big Brother Watch* and *Centrum för Rättvisa* are shadowing the global pandemic, when world governments are increasingly relying upon intrusive methods of data collection and contract tracing to prevent the spread of COVID-19. Such convergence is dangerous, as it would most likely justify any surveillance measure deployed in the context of the pandemic in Europe.

---

gathering itself may be pursued by means of bulk interception based on a requirement of reasonable suspicion of the involvement of the targeted person or group of persons involved in activities harmful to national security, even if they are not criminal offences" (*idem*) and (with reference to the Additional Protocol to the Council of Europe Data Protection) that "*[a]ccording to the consolidated Council of Europe and European Union standards, the sharing of personal data should be limited to third countries which afford a level of protection essentially equivalent to that guaranteed within the Council of Europe and the European Union respectively [with judicial oversight [that] should here be as thorough as in any other case*" (para. 31)He also more generally noted the "arbitrary" distinctions drawn by the Court in relation to data sharing (paras. 50 – 54). In his view, in the majority judgment: "*purely opportunistic considerations prevailed over the assessment of the necessity and proportionality of the additional interference with the intercept subject's rights constituted by the disclosure of the intercepted material to other parties. In simple words, the individual's communication is treated as a possession of the State, a commodity that the State can share with other parties at its discretion in order 'to see if the haystack contains a needle'*" (para. 54).

See also the joint opinions of Judges Lemmens, Vehabović and Bošnjak, who said that the Court "*has … missed an excellent opportunity to fully uphold the importance of private life and correspondence when faced with interference in the form of mass surveillance*" (para. 1), and the Joint Partly Dissenting Opinion of Judges Lemmens, Vehabović, Ranzoni and Bošnjak, that was also highly critical of the limited scrutiny of and restrictions imposed by the Court on data sharing between intelligence agencies of different countries including non-European ones.

[81] Monika Zalnieriute, *A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence*, EJIL Talk! 4 June 2021, at:

https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/

See also, e.g., Nora Ni Loideain, *Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment*, Information Law and Policy Centre, 28 May 2021, at: https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/

Prof. Mark Klamberg wrote the *Rättvisa* judgment "begs the question whether courts – domestic and international – will ever be in a position to exercise effective control when states are conducting surveillance for national security reasons."[82]

We share these concerns.

In the next sub-section, we will discuss the differences between the case-law of the CJEU and the case-law of the ECtHR in these respects, in the light of accusations of hypocrisy and "double standards", levelled against the EU and the EU Member States by the USA.

Hypocrisy and "Double standards"? US criticism of the EU and the EU Member States

The USA has criticised the EU approach to EU-US data transfers in comments on the EDPB's recommendations on supplementary measures for such transfers.[83] These criticisms carry some weight, even if we do not fully agree with them. In particular, the USA was right when it noted that:[84]

> under *LQDN* no EU legislation governs direct access by Member State authorities to personal data for national security purposes—not the e-Privacy Directive, not GDPR, and not the Law Enforcement Directive.

And that: [85]

> … EU law provides no privacy protections relating to EU Member State governments' direct access to personal data for national security purposes …

But it was not quite right when it claimed that: [86]

> a data exporter would [therefore] have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law.

Rather, as Christakis has pointed out,[87] the data exporter could and should look at the case-law of the European Court of Human Rights (summarised in the previous sub-section) – which is binding on all EU Member States, and compliance with which is also required of any EU Member State under EU law (see section 2.2.2.3).

It nevertheless remains true that in the EU different standards apply to surveillance carried out by Member States under orders issued to providers of e-communication services (the standards set by the CJEU in *Schrems II* and *LQDN*, discussed previously), and to surveillance carried out by their national security agencies through direct, surreptitious "hacking" into the providers' systems (the ECHR standards discussed above) – while surveillance laws and practices of third countries have to

---

82 Mark Klamberg, *Big Brother's Little, More Dangerous Brother: Centrum för Rättvisa v. Sweden*, Verfassungsblog, 1 June 2021, at: https://verfassungsblog.de/raettvisa/

83 US Government, *Comments on proposed EDPB Recommendations 01/2020* (December 21, 2020), at: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf
These comments related to the original version of those recommendations, adopted on 10 November 2020.

84 *Idem*, p. 9.

85 *Idem*, p. 9.

86 *Idem*, p. 9.

87 Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations*, Part 1, *Countering the US arguments*, 12 April 2021, at: https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/
See the quote from this article in the *Korff Transfer Paper* (footnote 9), p. 47.

"essentially" meet the CJEU standards in relation to both kinds of surveillance if a third country is to be held to provide "essentially equivalent/adequate" protection in relation to data transfers. In chart form:

Table 1 European standards applied to state surveillance

	EU Member States:	**Third countries:**
Indirect access (access under orders issued to providers.)	EU CJEU *Schrems II* & *LQDN* standards	"Essentially equivalent" standards to the EU CJEU *Schrems II* & *LQDN* standards
Direct access (access through surreptitious "hacking" into providers' systems.)	ECHR standards	

As Eskens notes, in an important sense, there should be a higher level of protection for *direct* access, since a layer of protection for the target of surveillance (the provider) is removed.[88] The multistakeholder Global Network Initiative has called on governments "to use only targeted measures proportionate to their justifiable need to access user data, and refrain from implementing or broadening direct access approaches" (which it defines more broadly, to include opaque "black box" interception equipment placed in providers' systems.)[89]

The main difference between the CJEU and the ECHR requirements for bulk data collection is that the CJEU holds that the EU (and by extension the Member States) have only **limited discretion** in relation to the setting of the parameters for such activities and must apply such exceptional collection only insofar as **strictly necessary** (*DRI* judgment, paras. 48 and 52: see above), while the ECtHR feels it must grant Contracting States a **wide margin of appreciation** in this respect (*BBW* GC judgment, para. 338: see above).

Consequently, the CJEU holds that **"generalised, indiscriminate" collection of personal data is basically incompatible with the Charter** (while making a very limited exception in relation to bulk collection to deal with a most serious, real threat to the very foundations and functioning of the state, which however must then still be strictly limited in time and place), while the ECtHR holds that **the decision to operate a bulk interception regime falls within the wide margin of appreciation** it granted (*BBW* GC judgment, para. 340) – but then adding very strong oversight and very demanding supervisory procedures, and that all the relevant parameters be spelled out on the face of the relevant law.

The main point to be made in that respect is that it would in our opinion be highly unlikely that the European Commission would deny "adequacy" status to a third country that in all general respects provided "essentially equivalent" protection to the EU and that in relation to the surveillance carried out by its intelligence agencies met all the requirements of the ECHR as interpreted and applied by the Strasbourg Court (also in applying any limitations on such surveillance equally to individuals who are not nationals of or resident in the third country). Whether that would also satisfy the Luxembourg Court is a question that cannot be conclusively answered at present. We have serious doubts, in particular, about the lax approach of the Strasbourg Court to intelligence data sharing. Suffice it to note that (as

[88] Footnote 20.

[89] Global Network Initiative, *Defining Direct Access: GNI calls for greater transparency and dialogue around mandatory, unmediated government access to data*, 3 June 2021, at: https://globalnetworkinitiative.org/defining-direct-access-2/

we will see in the next section), current US surveillance laws fall significantly short of both the CJEU and the ECtHR standards.

A more pertinent claim of hypocrisy can be laid against the EU and the EU Member States in relation to actual compliance with either the ECtHR or the CJEU standards. As we noted in section 2.3.1.2, there have been serious questions about the general effectiveness of enforcement by the supervisory authorities in the EU Member States. More specifically, as mentioned in section 2.3.1.3, under the heading "*CJEU requirements relating to personal data retention obligations imposed on entities that are subject to EU data protection law, for the purpose of allowing access to the retained personal data by EU Member State intelligence agencies for national security purposes*", the EU and the Member States have been reluctant to come up with laws that actually meet the CJEU standards laid down in its *DRI* and *Tele-2/Watson* judgments, in spite of strong criticism by the European Parliament and civil society.[90] The current laws in the EU Member States have also not yet been brought into line with CJEU judgments in *PI* and *LQDN*. And the surveillance laws and practices in many EU Member States would clearly fail the tests applied to the laws and practices of the USA in *Schrems II*.

We therefore suggest in chapter 4 that not only should the USA bring its surveillance laws into line with international human rights standards, but the EU and the EU Member States should ensure this in the EU and Member States' legal orders as well.

Before turning to those wider issues, we feel that for completeness' sake we should briefly mention the EU rules on transfers to "non-adequate" third countries.

2.3.2 Transfers to "non-adequate" third countries

2.3.2.1 Regular transfers to "non-adequate" third countries on the basis of "appropriate safeguards"

Outside of exceptional, occasional cases (see below, at 2.3.2.2), regular transfers of personal data from the EU to any third country that has not been held to provide adequate protection by the European Commission may only take place provided that "appropriate safeguards" are adopted to ensure the continued protection of the data in the third country, also after transfer (Article 46(1), which adds that "enforceable data subject rights and effective legal remedies for data subjects" must be made available).

Article 46(2) further clarifies that:

> The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
>
> (a) a legally binding and enforceable instrument between public authorities or bodies;
>
> (b) binding corporate rules in accordance with Article 47 [i.e., approved by a competent supervisory authority];
>
> (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
>
> (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

[90] See footnote 52.

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Appropriate safeguards can also be provided for by non-standard contractual clauses and by "provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights", but these latter two types of safeguards must be authorised by the competent supervisory authority (Article 46(3)).

The most important for the purpose of this study are "**standard data protection clauses** adopted by the Commission" (**SCCs**, Article 46(2)(c) GDPR),[91] to which the CJEU made express reference in its *Schrems II* judgment, and, for multinational corporations, SA-approved **Binding Corporate Rules** (**BCRs**, Article 47 GDPR) that similarly regulate transfers within the associated entities. We will also briefly note **codes of conduct** and **certifications**.

The Commission has recently issued a series of new **standard contract clauses (SCCs)**, in a modular format.[92] In principle, these can be used to enable transfers to non-adequate third countries.

However, in relation to the issue of access to transferred data by the authorities of a third country, SCCs suffer from the same inherent limitation as the previous SCCs, as discussed by the CJEU in *Schrems II*, i.e., they cannot bind the authorities of the third country or override the laws of the third country. "**Supplementary measures**" may therefore have to be adopted in addition to the SCC clauses to protect personal data transferred under them against undue access by the third country's authorities.[93] The EDPB moreover noted that:[94]

> The reasoning put forward by the Schrems II judgment also applies to other transfer instruments pursuant to Article 46(2) GDPR since all of these instruments are basically of contractual nature, so the guarantees foreseen and the commitments taken by the parties therein cannot bind third country public authorities.

Such supplementary measures may include full, state of the art encryption, anonymisation or strong pseudonymisation or detaching part of the data.[95] However, no effective measures have been identified in relation to situations in which the transferred data are needed in the clear in the third country:[96]

---

[91] Individual supervisory authorities have tended to not issue standard clauses of their own, but rather, encourage controllers and processors to use the SCCs adopted by the Commission.

[92] European Commission, Commission implementing decision (EU) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021)3972, OJ L199, 7 June 2021, pp. 31 – 61, at:
http://data.europa.eu/eli/dec_impl/2021/914/oj
The SCCs are contained in an Annex to the decision.

[93] CJEU, *Schrems II* judgment (footnote 3), paras. 131 – 133.

[94] EDPB *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (footnote 24), para. 62.

[95] See Use Cases 1 – 5 in the "*Examples of scenarios referring to cases in which* effective *measures are identified*" in the EDPB *Recommendations 01/2020*, para. 79ff.

[96] *Idem*, Use Cases 6 and 7 under the heading "*Examples of scenarios referring to cases in which* effective *measures are not identified*", para. 93ff. The quote is from para. 97.

> In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

In other words if, in a third country, the authorities of that third country can demand or gain access to personal data under laws or rules that do not meet the EU standards on such access (as discussed above), then not only can the country not be held to provide "adequate"/"essentially equivalent" protection to the GDPR, but personal data also may only be transferred to that country under SCCs or BCRs if appropriate, effective "supplementary measures" are adopted in addition – but this can only provide continued protection to the data if the data transferred under the relevant SCCs or BCRs are not transferred in the clear.

The implications were recently illustrated when the Portuguese data protection authority, CNPD, suspended transfers of census data on Portuguese citizens to the US-based "Cloudflare" service provider, even though the data were transferred under EU SCCs, because the provider was subject to US surveillance laws,[97] and when the French Government announced a "cloud" strategy under which public sector data must be stored in France, using European providers certified as "trusted".[98]

Three observations may be added. First of all, as both the text of Article 46 and the EDPB guidance and recommendations stress, the issue of ensuring "enforceable data subject rights and effective legal remedies for data subjects" will always remains fundamental: mere contractual stipulations requiring an importer to meet EU standards are not enough if the data subjects in question cannot effectively rely on them. The SCCs adopted by the Commission therefore contain "third party beneficiary" clauses that data subjects can invoke if the parties to a transfer fail to meet their obligations. Any laws or legal rules in a third country that would prevent a data importer from granting EU data subjects the effective exercise of their rights would therefore mean that the relevant instrument – SCCs or BCRs – cannot be used: in such cases, they do not, cannot, provide "appropriate safeguards".

Second, the CJEU and the EDPB stress that EU data exporters, working with their third country data importer partners, must carefully assess the risks of undue access by the authorities of the relevant third country (or countries), and adopt appropriate supplementary measures in the light of the findings of this assessment:[99]

> [You, data exporters and importers, must] assess if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer. Your assessment should be focused first and foremost on third country legislation that is relevant to your transfer and the Article 46 GDPR transfer tool you are relying on. Examining also the practices of the third country's

---

97 Comissão Nacional de Proteção de Dados Notícias: Censos 2021: *CNPD Suspende Fluxos para os EUA*, 27 April 2021, at: https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/

Summary in English at:

https://dataprivacymanager.net/portuguese-data-protection-authority-suspends-transfers-of-census-2021-data-to-the-u-s/

98 See:

https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/ Cf. also the recommendations of a working party of the German data protection authorities against the use of Microsoft Office 365 (see:

https://www.datenschutz.saarland.de/ueber-uns/oeffentlichkeitsarbeit/detail/pressemitteilung-vom-02102020-stuttgart-muenchen-ansbach-wiesbaden-saarbruecken) and the Dutch critical assessments (footnote 57).

99 EDPB *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (footnote 24), Executive Summary, pp. 3 – 4.

> public authorities will allow you to verify if the safeguards contained in the transfer tool can ensure, in practice, the effective protection of the personal data transferred.

Such an assessment should not be a one-off, done only prior to the (first) transfer, but conducted on an ongoing basis: risks could arise over time, e.g., because of new laws being introduced in the third country, or existing laws being amended or newly interpreted. In that respect, measures suggested by the Commission in its work on the Digital Services Act (DSA) and the Digital Markets Act (DMA), such as audits by independent organisations, monitoring tools (such as secure logs), ex-post evaluations and infringement alert mechanisms, could all play roles – although surveillance laws will also often render such measures useless. For instance, new rules or new interpretations of existing rules could be kept secret (see the discussion of secret rules in section 3.2.2, below); and laws in third countries can demand (a) an importer creates or maintains back doors in or facilitates access to personal data or systems, or that the importer must be in possession of and on demand hand over decryption keys and (b) the importer may not inform the data exporter of such requirements, either before transfer or later.

The third point is that recently the Commission has suggested in two different contexts that SCCs need not, and indeed cannot, be used for transfers of personal data to a data importer in a non-adequate third country, if the data importer in that non-adequate third country is itself subject to the GDPR, because the processing relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union (cf. Article 3(2) GDPR).[100] There is some sense in this: the whole point about SCCs is that they seek to impose on the data importer, by contract, the relevant GDPR obligations that apply if the processing took place in the EU, and it does not make much sense to try and impose such obligations in this way if they already rest on the importer by virtue of the law (the GDPR) itself.

However, that does not mean that transfers of personal data to an importer in a non-adequate third country who is *de iure* subject to the GDPR (by virtue of Article 3(2)) can take place without the need for (supplementary) safeguards. The same reasoning as was applied by the Court to transfers to the USA under SCCs also applies here: the mere fact that the EU says the importer is subject to the GDPR does not mean that the data will not be subject to undue access by the authorities of the third country. After all, the data importer can be required under its domestic law to provide such undue access – and even though Article 48 GDPR stipulates that controllers or processors who are subject to the GDPR may not comply with orders from third country courts or public bodies, in practice data importers will not be able to refuse to comply with such orders (and may be compelled to keep them secret). Clearly, therefore, all that was said about the need for "supplementary safeguards" when SCCs are used also applies, *mutatis mutandis*, in relation to transfers of personal data to data importers in non-adequate third countries who are subject to the GDPR by virtue of Article 3(2) GDPR.

We will conclude this section with brief comments on the other main types of transfer instrument mentioned in Article 46: codes of conduct and certifications.

As noted above, Article 46(2) envisages that personal data may be transferred to a third country, "without requiring any specific authorisation from a supervisory authority", if they are made under (and in accordance with the stipulations in) a **code of conduct** that has been adopted in accordance with the procedure laid down in Article 40 GDPR. Under this article, sectors can submit a draft code to their

[100] European Commission, Commission implementing decision (EU) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (footnote 92, above), para. 7. The same view is reflected in the EU Commission GDPR Adequacy Decision on the UK of June 2021, which says that "This Decision should not affect the direct application of Regulation (EU) 2016/679 to organisations established in the United Kingdom where the conditions regarding the territorial scope of that Regulation, laid down in its Article 3, are fulfilled." (Introduction, para. (7)).

relevant competent supervisory authority. If that authority finds the code "provides sufficient appropriate safeguards" (also in relation to the rights of data subjects), it can approve the code if it only applies to processing activities in that Member State. If the code applies to activities in more than one Member State, the draft opinion of the relevant SA must be submitted to the EDPB for its opinion. If the EDPB opinion is positive, the Commission may approve the code.

The EDPB recently adopted opinions on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, and on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE).[101] These were the first ever such opinions. However, not only have the relevant codes not yet been approved by the Commission, the EDPB also stresses, in both opinions, that:[102]

> The present code is not a code of conduct according to article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation shall take place only if the provisions of chapter V of the GDPR are respected.

In other words, to date there are no EU Commission-approved codes of conduct that can be relied upon as a legal basis for transfers to non-adequate third countries including the USA.

Article 46(2) also allows transfers of personal data a non-adequate third country, "without requiring any specific authorisation from a supervisory authority", if they are made under (and in accordance with the stipulations in) **certifications** as envisaged in Article 42 GDPR. That article and the following article, Article 43, make detailed provision for the establishment and accreditation of the relevant **certification schemes**. One of us has noted the risk that lax schemes of this sort could lead to inappropriate transfers.[103] But in fact, the creation of such schemes has proved to be difficult and complex. After inordinate delays, the EDPB adopted guidelines on certification and identifying certification criteria in May 2018;[104] a "document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal", in January 2020;[105] and

---

[101] EDPB, Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, adopted on 19 May 2021, available at: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf
EDPB, Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE), adopted on 19 May 2021, available at: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202117_cispecode_en_0.pdf

[102] EDPB Opinion 16/2021, para. (7); Opinion 17/2021, para. (7).

[103] Douwe Korff, *Privacy seals in the new EU General Data Protection Regulation: Threat or Facilitator?*, in: Rote Linien zur EU-DSGVO, in: Datenschutznachrichten (DANA), 3/2015 (August 2015), p.128, at: https://www.datenschutzverein.de/wp-content/uploads/2015/08/DANA_3-2015_RoteLinien_Web.pdf
Douwe Korff, *Privacy seals in the new EU General Data Protection Regulation: Threat or facilitator? Part 2: What has it turned out to be?*, in: Datenschutznachrichten (DANA), 2/2016 (July 2016), p.77, at: https://www.datenschutzverein.de/wp-content/uploads/2016/07/DANA_2-2016_RoteLinienRevisited_Web.pdf

[104] EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, adopted on 25 May 2018, available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_1_2018_certification_en.pdf

[105] EDPB, Document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal, adopted on 28 January 2020, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpbprocedureforeudataprotectionseal_postplencheck_en.pdf

guidance on certification criteria assessment in April 2021.[106] **But to date, no accredited certification schemes have been established, and controllers and processors can therefore still not obtain a certification that they could use as a legal basis for transfers to non-adequate third countries including the USA.**

It is doubtful whether codes of conduct or certifications could really provide "adequate"/"essentially equivalent" protection to that accorded by the GDPR in the EU. At best, they might in future do so (subject to the *caveat* noted next) if adherence to an approved code, or to a proper certification (seal) were to be announced by a US-based importer and the FTC could then hold that non-compliance with the code or the certificate constitutes an "unfair or deceptive act or practice" (see section 3.1.1 and 4.2, below). But even if that were to be possible – in particular, under an enhanced/reinforced FTC supervisory arrangement as we propose in section 4.2.3, coupled with enforceable data subject rights and effective legal remedies for data subjects (*idem*) – there would still be the issue of undue access to the transferred data by US intelligence agencies. Such a putative code or certification solution to the general adequacy issue could therefore, like SCCs and BCRs, not provide an "appropriate safeguard" in terms of Article 46 GDPR, unless the issue of undue access was also addressed (as again we propose in chapter 4.)

2.3.2.2 Derogations for occasional, ad hoc transfers:

Article 49 GDPR sets out a number of "derogations [from the main data transfer rules] for specific situations". These include (in paraphrase). They consist of several fairly specific derogations and a broadly phrased but more heavily circumscribed one. The specific derogations cover:

- transfers on the basis of the "explicit consent" of the data subject, given after the data subject is "informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards" (Art. 49(1)(a));
- transfers that are "necessary" in a contractual context, more specifically "for the performance of a contract between the data subject and the controller", or for "the implementation of pre-contractual measures taken at the data subject's request", such as a credit check, or for "the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person" (Art. 49(1)(b) and (c));
- transfers that are "necessary for important reasons of public interest" that is "recognised in [EU] law or in the law of the Member State to which the controller is subject" (Art. 49(1)(d) and (4));
- transfer that are "necessary for the establishment, exercise or defence of legal claims (Art. 49(1)(e))";
- the rare situation in which a transfer is "necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent" (Art. 49(1)(f)); and
- the special case of transfers of personal data from a publicly accessible register – which must comply with the conditions for access to such registers and must not "involve the entirety of

[106] EDPB, Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation), Certification criteria assessment, version for public consultation, adopted on 06 April 2021, available at: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_certification_criteria_assessment_formatted_en_0.pdf

> the personal data or entire categories of the personal data contained in the register" (Article 49(1)(g) and (2)).

However, the first three of these derogations do not apply to "activities carried out by public authorities in the exercise of their public powers" (Art. 49(3)); those will more usually have to rely on the fourth derogation (transfers that are necessary for important reasons of public interest).

The use of the term "***explicit* consent**" in the first derogation, and the use of the term "***necessary***" in the second, third, fourth and fifth derogation, indicate that these derogations must be restrictively interpreted (see below).

In the second sub-paragraph of Article 49(1), the GDPR adds to the above **a broadly phrased but even more strictly circumscribed derogation**:

> Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is **not repetitive**, concerns only a **limited number of data subjects**, is ***necessary*** for the purposes of **compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject**, and **the controller has *assessed* all the circumstances surrounding the data transfer** and has on the basis of that assessment provided **suitable safeguards** with regard to the protection of personal data. The controller shall ***inform* the supervisory authority** of the transfer. The controller shall, in addition to providing the [general information about processing that must be provided to data subjects under Articles 13 and 14 GDPR], ***inform* the data subject** of the transfer and on the compelling legitimate interests pursued.
>
> (emphases added)

The limited scope of all the derogations (not just the last one) is stressed by the European Data Protection Board. Briefly, with reference to further detail in detailed guidelines on the application of Article 49, the EDPB holds that:[107]

> **Article 49 GDPR [read: as a whole – DK/IB] has an exceptional nature. [All] [t]he derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.**
>
> Before relying on an Article 49 GDPR derogation, you must check whether your transfer meets the strict conditions this provision sets forth for each of them.

Of particular importance is the reference to "**suitable safeguards**":

> This requirement highlights the special role that safeguards may play in reducing the undue impact of the data transfer on the data subjects and thereby in possibly influencing the balance of rights and interests to the extent that the data controller's interests will not be overridden.
>
> When assessing these risks and what could under the given circumstances possibly be considered as "suitable safeguards" for the rights and freedoms of the data subject, the data exporter needs to particularly **take into account** the nature of the data, the purpose and duration of the processing as well as **the situation in** the country of origin, **the third country** and, if any, the country of final destination of the transfer.

[107] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, paras. 25 – 26, briefly summarising the detailed guidance in the EDPB's Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018.

> Furthermore, the law requires the data exporter to apply **additional measures** as safeguards in order **to minimize the identified risks** caused by the data transfer for the data subject. This is set up by the law as a mandatory requirement, so it can be followed that in the absence of additional safeguards, the controller's interests in the transfer will in any case be overridden by the interests or rights and freedoms of the data subject. As to **the nature of such safeguards**, it is not possible to set up general requirements applicable to all cases in this regard, but these **will** rather **very much depend on the specific data transfer in question**. Safeguards might include, depending on the case, for example measures aimed at ensuring deletion of the data as soon as possible after the transfer, or **limiting the purposes for which the data may be processed following the transfer**. Particular attention should be paid to whether it may be sufficient to transfer **pseudonymized or encrypted data**. Moreover, **technical and organizational measures aimed at ensuring that the transferred data cannot be used for other purposes than those strictly foreseen by the data exporter** should be examined.

These references to "additional safeguards" are clearly reminiscent of the "supplementary measures" that may be required in relation to transfers based on SCCs and BCRs (see the previous sub-section, 2.3.2.1), and the references to potential use of the transferred data "for other purposes than those strictly foreseen by the data exporter" clearly also covers the possibility of authorities in the third country accessing the data for law enforcement and/or national security purposes.

In other words, the views of the EDPB on "supplementary measures" that may be adopted in relation to SCCs and BCRs also apply to transfers under Article 49, as does our conclusion in that respect, *mutatis mutandis*:

If, in a third country, the authorities of that third country can demand or gain access to personal data under laws or rules that do not meet the EU standards on such access (as discussed above), then not only can the country not be held to provide "adequate"/"essentially equivalent" protection to the GDPR, but in addition personal data may only be transferred to that country under the Article 49 derogations if appropriate, effective "additional measures" are adopted – but this can only provide continued protection to the data if the data transferred under the relevant derogation are not transferred in the clear.

At a conference in January 2021, Thomas von Danwitz, the judge-rapporteur in the CJEU *Schrems I* and *II* cases and in the *LQDN* case, appeared to take a somewhat less restrictive view. He said:[108]

> Article 49 derogations are in particular an option for intra-group transfers and that they should be more attentively explored. "(…) In my opinion, the opportunities granted by Article 49 have not been fully explored yet. I believe they are not so narrow that they restrict any kind of transfer, especially when we're talking about transfers within one corporation or group of companies."

The reference to the use of Article 49 for transfers within a corporation or group of companies is somewhat puzzling, given the GDPR provides a specific basis for such transfers in the form of BCRs. In any case:[109]

> Von Danwitz indicated that the conditions from the text of the GDPR in any case must be met. For example, in the case of the derogation relying on necessity to enter a contract or for the

[108] Rob van Eijk and Gabriela Zanfir-Fortuna, Future of Privacy Forum report on the German Federal Ministry of the Interior conference celebrating the 40th Data Protection Day, 28 January 2021, *Schrems II: Article 49 GDPR derogations may not be so narrow and restrictive after all?*, available at: https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all/

[109] *Idem*.

> performance of a contract, the first test is to ask "*is the transfer of that data* ***really required****? Is* ***it really necessary*** *to fulfill the contract?*" He added: "*In my opinion, this gives people sufficient scope of action*".

He also did not address the issue in the context of access to transferred data by third country authorities. Rather:[110]

> The judge didn't go into further details and also clarified that questions related to the scope of Article 49 derogations might be posed to the court in the future, and he doesn't want to "preempt any judgments by making a statement now".

In our opinion, the prudent view still is that for organisations that need or want to transfer personal data from the EU to any non-adequate third country on a regular basis, in a structured context (e.g., a commercial relationship, or inside a group of companies, or between public bodies), the Article 49 derogations are of very limited use. In particular, they do not offer any work-around in relation to the regular use of cloud-based services provided from any non-adequate third country (unless the data in the "cloud" are fully encrypted and unreadable to state authorities). They also do not remove the obligation from EU data exporters to assess, in relation to each proposed transfer, whether there is a risk of undue access to the to-be-transferred data by authorities of the third country in question – or the obligation to not go ahead with the transfer if effective "supplementary measures" cannot be put in place to protect the data against such undue access.

2.3.2.3 Stopping transfers

Finally, in this overview of EU data protection law, we should note that apart from the rules that transfers should in certain cases not take place, or only if certain tools and possibly supplementary measures are adopted, there is of course also the question of who will enforce this. In that respect, there is firstly **a duty on the part of any data exporter to stop any transfers if there are indications that they may result in the EU data protection rights and interests of EU persons being undermined**, in particular (but not only) if there is a risk that the authorities in the third country in question will seek undue access to the data. Failure to do so will render the data exporter (and the data importer if that entity is subject to the GDPR by virtue of Article 3(2)) liable for damages and sanctions.

But in addition, the CJEU has stressed in *Schrems II* that if the transfer is based on SCCs:

> **the competent supervisory authority is required to suspend or prohibit a transfe**r of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer. (Final ruling, point 3, on p. 61, emphasis added)

If there is an adequacy decision in place, the process is more cumbersome but still not absent: as the Court pointed out in *Schrems II*:

> when a person lodges a complaint with the competent supervisory authority, that authority must examine, with complete independence, whether the transfer of personal data at issue complies with the requirements laid down by the GDPR and, if, in its view, the arguments put forward by that person with a view to challenging the validity of an adequacy decision are well founded, bring an

[110] *Idem*.

action before the national courts in order for them to make a reference to the Court for a preliminary ruling for the purpose of examining the validity of that decision. (para. 157)

- o – O – o -

3 US PRIVACY AND SURVEILLANCE LAWS

KEY FINDINGS

A US Congressional Research Service review found a "patchwork" of federal data protection laws which "primarily regulate certain industries and subcategories of data." The rather limited protections accorded to "US persons" by the Fourth Amendment are largely non-existent in relation to non-US individuals outside the USA, while "privacy torts" are too limited to even compare to EU data protection concepts.

Several broad federal privacy bills have been introduced to Congress since 2019. While such legislation would clearly offer very significant improvement in protection of personal data, as currently drafted, none of them achieve "essential equivalence" to the GDPR.

Consumer privacy bills have been passed or introduced in dozens of the individual states. California's Privacy Rights Act (CPRA) which will enter into force in 2023) is closest to the GDPR, but still falls short of "essential equivalence" in scope and exceptions. Nor is it likely any other US state will adopt a law going beyond the CPRA.

The Foreign Intelligence Surveillance Act (FISA) regulates US national security and foreign intelligence-related electronic surveillance. Outside the US, electronic surveillance activities of the US intelligence community targeting non-US persons are generally governed by Executive Order 12333. Presidential Policy Directive 28 (PPD-28) contains limits on the use of signals intelligence collected in "bulk" by the intelligence community. **The CJEU invalidated the Privacy Shield adequacy decision because FISA s.702 and E.O. 12333, even as limited by PPD-28, are too permissive to meet the GDPR's standards of necessity and proportionality and do not provide EU data subjects with effective judicial redress.**

3.1 US privacy laws

3.1.1 Introduction

As explained in a US Congressional Research Service paper[111] of 2019:

> Despite the increased interest in data protection, the legal paradigms governing the security and privacy of personal data are complex and technical, and lack uniformity at the federal level. The

[111] In this section, as indicated in the quotes and footnote references, we draw extensively on the US Congressional Research Service report, *Data Protection Law: An Overview*, 25 March 2019 (hereafter: "CRS Data Protection Report", at https://fas.org/sgp/crs/misc/R45631.pdf). We have done this because the CRS overviews can be regarded as fair summaries of this very complex area of US federal and state law, without any "European" bias. The US government has stated: "There is a wealth of public information about privacy protections in U.S. law concerning government access to data for national security purposes, including information not recorded in Decision 2016/1250, new developments that have occurred since 2016, and information the ECJ neither considered nor addressed." *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, White Paper, September 2020, at:
https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF
See also Chris Hoofnagle, *New Challenges to Data Protection - Country Report: United States*, study for the European Commission, 2010, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1639161
We have updated the information and added our own observations as appropriate.

> Supreme Court has recognized that the Constitution provides various rights protecting individual privacy, but these rights generally guard only against government intrusions and do little to prevent private actors from abusing personal data online. At the federal statutory level, while there are a number of data protection statutes, they primarily regulate certain industries and subcategories of data. The Federal Trade Commission (FTC) fills in some of the statutory gaps by enforcing the federal prohibition against unfair and deceptive data protection practices. But no single federal law comprehensively regulates the collection and use of personal data.
>
> In contrast to the "patchwork" nature of federal law, some state and foreign governments have enacted more comprehensive data protection legislation. Some analysts suggest these laws, which include the European Union's (EU's) General Data Protection Regulation (GDPR) and state laws such as the California Consumer Privacy Act (CCPA), will create increasingly overlapping and uneven data protection regimes. This fragmented legal landscape coupled with concerns that existing federal laws are inadequate has led many stakeholders to argue that the federal government should assume a larger role in data protection policy. However, at present, there is no consensus as to what, if any, role the federal government should play, and any legislative efforts at data protection are likely to implicate unique legal concerns such as preemption, standing, and First Amendment rights, among other issues. [112]

This "patchwork" still persists. Below, after a short section on US common law and constitutional law privacy protections, we will provide brief overviews of US federal and state privacy laws, before turning to proposals for more comprehensive legislative action in this area.

We analyse the situation in the USA from a European perspective in chapter 4, and discuss the various policy options, and the problems they raise in US law and policy making.

3.1.2 US common law and constitutional law

The CRS Data Protection Report discusses in some detail the historical development of the common law and the emergence of so-called "privacy torts" in the century that followed Brandeis's and Warren's seminal 1890 article *The Right to Privacy*, [113] and the still evolving case-law under the Fourth Amendment to the US Bill of Rights. [114] Here, it must suffice to quote its overall conclusions in this respect, that:[115]

> All of the constitutional rights involving privacy, like the common law privacy torts, focus on public disclosure of private facts. This focus limits their potential influence on modern data privacy debates, which extends beyond the disclosure issue to more broadly concern how data is collected, protected, and used. [116] Perhaps more importantly, whatever the reach of the constitutional right to privacy, the "state action doctrine" prevents it from being influential outside the realm of government action. Under this doctrine, only government action is subject to scrutiny under the Constitution, but purely private conduct is not proscribed, "no matter how unfair that conduct may be." [117] As a result, **neither the common nor constitutional law provides a complete framework for considering many of the potential threats to digital privacy and consumer data. Rather, the most important data protection standards come from statutory law.**

---

[112] CRS *Data Protection report* (footnote 111), pp. 2–3, footnote references omitted.

[113] 4 HARV. L. REV. 193 (1890), at: https://scholarship.law.pitt.edu/cgi/viewcontent.cgi?article=1062&context=fac_articles

[114] See CRS *Data Protection Report* (footnote 111), pp 3–7. For details, see Daniel J. Solove, *A Brief History of Information Privacy Law*, 2006, at: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076

[115] *Idem*, p. 7.

[116] [footnote omitted]

[117] *National Collegiate Athletic Ass'n v. Tarkanian*, 488 U.S. 179, 191 (1988). [original footnote].

(emphasis added)

We will limit our summary of US common law and constitutional law to the above, partly for the reason stated in the CRS report – that in the USA "*the most important data protection standards come from statutory law*" – and partly because, differently from the EU (and the wider international community including the UN and the Council of Europe), the USA does not accept the principle of "universality of human rights" (as discussed in chapter 2). In relation to the UN International Covenant on Civil and Political Rights, it has expressly and emphatically stressed that in the US view the ICCPR applies "*only to individuals who are BOTH within the territory of a State Party and subject to its jurisdiction*".[118]

More specifically, as noted by the Ad-hoc EU-US Working Group on Data Protection, set up to investigate the US surveillance activities exposed by Snowden:

> The protection of the Fourth Amendment of the US Constitution, which prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause"[119] extends only to US nationals and citizens of any nation residing within the US. According to the US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment.[120]

The rather limited protections accorded to "US persons" by the Fourth Amendment are therefore largely non-existent in relation to non-US individuals who are outside the USA – such as most people in the EU,[121] while "privacy torts" are too limited to even compare to EU data protection concepts. This affects the question of whether US law provides "adequate"/"essentially equivalent" protection to personal data compared to the EU. At the highest, constitutional level, it clearly does not. But this in itself does not prevent the USA from according adequate/essentially equivalent protection by statute.

3.1.3 US federal privacy laws

Overview

As the CRS data protection report points out (with useful references in footnotes):[122]

---

[118] From the statement of Matthew Waxman, Principal Deputy Director for Policy Planning at the State Department, to the UN Human Rights Committee on 17 July 2006, at:
https://opiniojuris.org/2006/07/18/does-the-iccpr-apply-extraterritorially/

[119] "Probable cause" must be shown before an arrest or search warrant may be issued. For probable cause to exist there must be sufficient reason based upon known facts to believe a crime has been committed or that certain property is connected with a crime. In most cases, probable cause has to exist prior to arrest, search or seizure, including in cases when law enforcement authorities can make an arrest or search without a warrant. [original footnote]

[120] According to the US Supreme Court, foreigners who are not residing permanently in the US can only rely on the Fourth Amendment if they are part of the US national community or have otherwise developed sufficient connection with the US to be considered part of that community: *US v. Verdugo-Urquidez* – 494 U.S. 259 (1990), pp. 494 U.S. 264-266. [original footnote] The case is at: https://supreme.justia.com/cases/federal/us/494/259/

For academic discussion see, e.g., Michele L. Cohen, *United States v. Verdugo-Urquidez, the Fourth Amendment Has Limited Applicability to Aliens Abroad*, 14 Md. J. Int'l L. 175 (1990), at:
http://digitalcommons.law.umaryland.edu/mjil/vol14/iss2/3

[121] See also Francesca Bignami, *The US legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens*, European Parliament, 2015.

[122] CRS *Data Protection Report* (footnote 111), pp.7–8. For overviews see, e.g.:
Varonis, *Complete Guide to Privacy Laws in the US*, at: https://www.varonis.com/blog/us-privacy-laws/
IAPP Topic Page *US Federal Privacy*, at: https://iapp.org/resources/topics/us-federal-privacy/ ($)
Ieuan Jolly, Loeb & Loeb LLP, *US Privacy and Data Security Law: Overview*, 2016, at:

> Given the inherent limitations in common law and constitutional protections, Congress has enacted a number of federal laws designed to provide statutory protections of individuals' personal information. In contrast with the scheme prevalent in Europe and some other countries, rather than a single comprehensive law, the United States has a "patchwork" of federal laws that govern companies' data protection practices.[123]
>
> These laws vary considerably in their purpose and scope. Most impose data protection obligations on specific industry participants—such as financial institutions, health care entities, and communications common carriers—or specific types of data, such as children's data.[124] Other laws, however, supplement the Constitution's limited privacy protections and apply similar principles to private entities. The Stored Communications Act (SCA), for instance, generally prohibits the unauthorized access or disclosure of certain electronic communications stored by internet service providers.[125] Lastly, some laws prohibit broad categories of conduct that, while not confined to data protection, limit how companies may handle personal data. Most notably, the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices."[126] As some scholars have pointed out, the FTC has used its authority under the FTC Act to develop norms and principles that effectively fill in the gaps left by other privacy statutes.[127]

The CRS *Data Protection Report* discusses the following:[128]

- the 1999 Gramm-Leach-Bliley Act (GLBA) that regulates the use of "consumer" "non-public information" by financial institutions.
- the 1996 Health Insurance Portability and Accountability Act (HIPAA) that regulates the use of "protected health information" by health care providers, health plans, and health care clearinghouses (covered entities), as well as certain "business associates" of such entities.

---

https://blog.richmond.edu/lawe759/files/2016/08/US-Privacy-and-Data-Security-Law-Overview.pdf

123 Zachary S. Heck, *A Litigator's Primer on European Union and American Privacy Laws and Regulations*, 44 LITIG. 59, 59 (2018) ("*[T]he United States has a patchwork of laws at both the federal and state levels relating to data protection and information sharing.*"), at 59; see also Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 587 (2014) ("*The statutory law is diffuse and discordant . . . . Unlike the privacy laws of many industrialized nations, which protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors. . . . This sectoral approach also leaves large areas unregulated . . . .*") [original footnote].

124 See *infra* §§ Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), The Communications Act, and Children's Online Privacy Protection Act (COPPA). [original footnote].

125 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004) ("*The [SCA] creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.*"). [original footnote]).

126 15 U.S.C. § 45(a). [original footnote].

127 Solove & Hartzog, *supra* note 123, at 587–88 ("*It is fair to say that today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States . . . . Because so many companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation.*"); Anna Karapetyan, *Developing a Balanced Privacy Framework*, 27 S. CAL REV. L. & SOC. JUST. 197, 213 ("*The Federal Trade Commission ('FTC') . . . steps in to fill gaps in statutory protections. The FTC uses its broad authority to restrict 'unfair or deceptive acts or practices' to protect consumer privacy. Unlike federal statutory laws, the FTC is not limited to specific sectors of the economy and its authority applies to most companies acting in commerce.*"). [original footnote].

128 The laws are listed in the order in which they are discussed in the CRS *Data Protection Report,* on pp.8–36, to which we refer for details. As explained in that report, "*These laws are organized below, beginning with those most narrowly focused on discrete industries and moving toward more generally applicable laws.*" The latter being the FTC Act and Consumer Financial Protection Act. As that report also explains, "*This section focuses on federal laws applicable to companies that collect and maintain personal information. It does not cover federal laws primarily applicable to government agencies or government employees, such as the Privacy Act (5 U.S.C. § 552a) or the E-Government Act (44 U.S.C. § 3501 note)*" (footnote 65, on p. 8). We have also omitted those laws from our study, for the same reason. We also do not discuss the various Federal Securities Laws: they address the issue of data security breaches but do not more broadly deal with data protection or privacy.

- the 1970 Fair Credit Reporting Act (FCRA) that regulates the collection and use of information bearing on a consumer's creditworthiness by credit reporting agencies (CRAs), entities furnishing information to CRAs (furnishers) and individuals who use credit reports issued by CRAs (users).
- the 1934 Communications Act (as amended, in particular in a major overhaul of US communications law in 1996), that provides a "comprehensive scheme" for the regulation of interstate communication, including data protection provisions applicable to common carriers, cable operators, and satellite carriers.
- the 1988 Video Privacy Protection Act (VPPA) that prohibits "video tape service providers"—a term that includes both digital video streaming services and brick-and-mortar video rental stores—from knowingly disclosing "Personally Identifiable Information (PII) concerning any "consumer" without that consumer's opt-in consent (subject to a series of rather broad exceptions)
- the 1974 Family Educational Rights and Privacy Act (FERPA) that created privacy protections for student education records;
- the 1998 Children's Online Privacy Protection Act (COPPA) that regulates the online collection and use of children's information (defined as children under 13) by website "operators";
- the 1986 Electronic Communications Privacy Act (ECPA), comprised of the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act. While primarily aimed at providing "Fourth Amendment like privacy protections" to electronic communications in relation to law enforcement activities, these acts also contain privacy obligations relevant to non-governmental actors;
- the 1986 Computer Fraud and Abuse Act (CFAA) that "was originally intended as a computer hacking statute and is centrally concerned with prohibiting unauthorized intrusions into computers, rather than addressing other data protection issues such as the collection or use of data".
- the 1914 Federal Trade Commission Act (FTC Act) that is aimed at countering "unfair or deceptive acts or practices" (UDAP), but under which the FTC "has used its authority … to become the 'go-to agency for privacy,' effectively filling in gaps left by the aforementioned federal statutes." It also of course was the body responsible for enforcing the (since invalidated) EU – US Safe harbour and Privacy Shield Agreements;
- the 2010 Consumer Financial Protection Act (CFPA) that seeks to counter "unfair, deceptive, or abusive acts or practices" done in connection with the offering or providing of a "consumer financial product or service", and under which the Consumer Financial Protection Bureau (CFPB) that it created has developed similar approaches to privacy and data protection-related issues as the FTC.

Current sector specific federal laws

Under the next heading, we will look more closely at the last two of the above-mentioned federal laws that are apply broadly, across sectors. As concerns the other, sector specific federal laws, it will suffice to observe in more general terms that (quite apart from the fact that by their very nature they are not

"omnibus" laws) none of them can be said to come anywhere near to providing "essentially equivalent" protection to the GDPR, even in the areas where they apply (which are mostly quite limited). Thus:[129]

The Gramm-Leach-Bliley Act imposes obligations on financial institutions in relation to data stewardship of "consumer" "non-public personal information" (NPI) and only imposes limitations on sharing of such information with "non-affiliated" third parties. NPI is clearly more limited than the EU concept of "personal data". The Act is also essentially limited to requiring financial institutions to provide their customers with notice of any intention to share their NPI, and with an opportunity to opt out. Although the non-taking of such an opportunity to opt out is, in the USA, often considered to constitute consent, it clearly does not constitute consent in the EU GDPR sense. The Act does not provide for a private right of action and does not limit sharing of information if the sharing is deemed to be in furtherance of providing a requested service..

The Health Insurance Portability and Accountability Act regulates stewardship, sharing and disclosure of "protected health information" (PHI) by "covered entities" – health care providers, health plans, and health care clearinghouses (also known as "medical claims clearinghouses", these are third-party intermediaries between providers of healthcare and health insurers) and certain "business associates" of such entities. It provides for a right of access to a person's health record and requires consent for the sharing of PHI – but the transparency requirements fall short of the EU ones (it suffices if the relevant notices are "prominently posted" on the relevant entity's website and provided "upon consumer request"). This Act too does not provide for a private right of action.

The Fair Credit Reporting Act covers the collection and use of information bearing on a consumer's creditworthiness by three kinds of entities involved in credit rating: credit reporting agencies (CRAs), entities furnishing information to CRAs (furnishers), and individuals who use credit reports issued by CRAs (users). In contrast to HIPAA or GLBA, there are no privacy provisions in FCRA requiring entities to provide notice to a consumer or to obtain his opt-in or opt-out consent before collecting or disclosing the consumer's data to third parties. FCRA's requirements generally focus on ensuring that the consumer information reported by CRAs and furnishers is accurate and that it is used only for certain permissible purposes (essentially, creditworthiness assessments).

The Communications Act first of all imposes some privacy and security requirements relating to "customer proprietary network information (CPNI)" (data on the use of a service) on "common carriers", i.e., providers of telecommunication services. However, an attempt by the relevant regulatory authority, the Federal Communications Commission (FCC), to impose broader data protection limitations on such common carriers under the Act was overturned by Congress, partly on the basis that it "restrict[ed] the free speech of its regulatory target".

The Act also protects a broader category of subscribers' "personally identifiable information" (PII) in relation to cable operators and satellite carriers. PII is not defined in the statute except in the negative, in that the Act stipulates that the term "does not include any record of aggregate data which does not identify particular persons.". This would appear to be closer to the concept of "personal data" in the EU GDPR. However, it is still not interpreted quite as broadly as the EU term, e.g., in relation to data being identifiable "by the controller or by another person". In the US generally, information from which the entity holding the data cannot identify the person concerned, including pseudonymised data, is not considered to constitute "personally identifiable information" (PII) for that entity – which contrasts with the EU view that:

[129] For details, see the relevant sections in the CRS *Data Protection Report* on each of the laws mentioned, and the entries on these laws in the overviews listed in footnote 122.

> Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person (GDPR Recital 26).

However, the Act allows for the disclosure of subscribers' name and address data (and presumably, the fact that they are a subscriber to the relevant entity's service) without consent, apparently for any purpose, as long as an opt out was offered and not used, provided the disclosure does not reveal the "extent of any viewing or other use by the subscriber" of the service provided or "the nature of any transaction made by the subscriber".

The Act does provide for a private right of action for "[a]ny person aggrieved by any act" of a covered entity in violation of the Act's requirements, but this is apparently little used.[130]

The Video Privacy Protection Act prohibits "video tape service providers" from knowingly disclosing personally identifiable information concerning any "consumer" without that consumer's opt-in consent. PII is again not defined, other than that the Act clarifies that it "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider". But not only does the above general view on identifiable meaning "identifiable by the person holding the data" apply, the law also contains sweeping exceptions, including that video tape service providers may disclose PII to "any person if the disclosure is incident to the ordinary course of business." The private right of action that the law does provide for consequently is of rather limited use other than in relation to clearly abusive uses and disclosures of the relevant PII.

The Family Educational Rights and Privacy Act limits disclosures of student education records, whereby "education records" are defined broadly to generally include any "materials which contain information directly related to a student" and are "maintained by an educational agency or institution." Relevant entities must not have a "policy or practice" of permitting the release of education records or "personally identifiable information contained therein" without the consent of the parent or the adult student – but this does not appear to prevent *ad hoc* disclosures. There are also (by European standards) rather sweeping exceptions to the rule against disclosures without consent, including for "studies", "audits" and "evaluations" or "any compliance or enforcement activity in connection with Federal legal requirements that relate to [education] programs". More sweeping still, educational institutions may also disclose without consent (apparently, for any purpose) "directory information" – which is very broadly defined as:

> "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most previous educational agency or institution attended by the student."

There is a right to complain to the Department of Education, but no private right of action.

The Children's Online Privacy Protection Act prohibits operators of websites or online services that are directed to children from collecting or using "personal information" from children under the age of thirteen without first obtaining parental consent. In this Act, "personal information" is again quite broadly defined to include names, addresses and email addresses, IP addresses, cookies, "unique

---

[130] Sam Castic, Aravind Swaminathan and Antony P. Kim, *FCC Privacy Regulations: The Next Litigation Trend?*, 21 June 2016, at: https://blogs.orrick.com/trustanchor/2016/06/21/fcc-privacy-regulations-the-next-litigation-trend/

("*The Communications Act has a rarely used provision that sets forth a private rights of action for violations of the Act itself or related regulations.*")

device identifiers", as well as any "photograph, video, or audio file where such file contains a child's image or voice"; or "geolocation information sufficient to identify street name and name of a city or town." There is no private right of action under the Act. Rather, privacy and data protection in this area is mainly provided through the "safe harbour" arrangement under which covered operators will be deemed to have satisfied the requirements of the Act if they follow self-regulatory guidelines the FTC has approved. Breaches of such guidelines by entities that have declared they will abide by them can be sanctioned by the FTC under its broad, general powers against "unfair" practices, discussed under the next sub-heading.

The Electronic Communications Privacy Act (ECPA, which is composed of the Wiretap Act, the Stored Communications Act [SCA] and the Pen Register Act) is largely directed at law enforcement, with limited application to private sector actors. In particular, ECPA "was designed to regulate wiretapping and electronic snooping rather than commercial data gathering," and litigants attempting to apply ECPA to online data collection have generally been unsuccessful.[131] Thus, "most courts have excluded personal computers from the reach of the SCA[132] (although some have disagreed).[133] Similarly, several federal courts held that the placement, by third-party advertising companies, of cookies on users' computers that track their activities on affiliated websites did not violate the Wiretap Act because the affiliated sites were "parties to the communication" and had consented to the interception (although again another court took a different view).[134]

Finally, the Computer Fraud and Abuse Act (CFAA) was originally intended as a computer hacking statute and is centrally concerned with prohibiting unauthorized intrusions into computers, rather than addressing other data protection issues such as the collection or use of data. As with ECPA, Internet users have attempted to use the private right of action under the law to sue companies tracking their online activity, arguing that companies' use of tracking devices constitutes an unauthorized access of their computers. In practice, however, such claims have typically been dismissed due to plaintiffs' failure to meet CFAA's damages threshold (minimum pecuniary damages in excess of $5,000 or other specific type of damages such as physical injury or impairment to medical care).

In sum: the current sector specific federal laws are all limited in their scope of application and often in relation to the data they protect (which is generally more narrowly defined or applied than the European concept of "personal data") and the acts they cover. None of the above-listed

---

131 Solove & Hartzog, *supra* note 123, at 592 ("*An attempt was made early on to apply existing statutory law to online data gathering practices. . . . ECPA was indeed a poor fit, as it was designed to regulate wiretapping and electronic snooping rather than commercial data gathering. . . . These rare attempts to apply existing law nearly all failed . . . .*"). [original footnote 242 on pp. 25 – 26].

132 See, e.g., *Morgan v. Preston*, No. 13–cv–0403, 2013 WL 5963563, at *5 (M.D. Tenn. Nov. 7, 2013) ("*[T]he overwhelming body of law" supports the conclusion that "an individual's personal computer is not a 'facility through which an electronic communication service is provided.'*"). [original footnote 258 on p. 27].

133 See, e.g., *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) ("*Viewing this factual dispute in the light most favorable to the nonmovant, as is required on summary judgment, it is possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the Act.*"). [original footnote 259 on p. 27]

134 *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) (holding that third-party advertising company's placement of cookies on users' computers that track their activities on affiliated websites did not violate the Wiretap Act because the affiliated sites were "parties to the communication" and had consented to the interception); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F. 3d 125, 139–142 (3d Cir. 2015) (holding that third-party advertising companies were parties to the communications because the users' servers sent a request to their servers asking them to populate the websites with ads, and in response to these requests the advertising companies either placed a cookie on the users' browsers or collected information from an existing cookie). But see *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003) (reversing district court's dismissal of plaintiffs' Wiretap Act claim and holding that defendants' actions constituted an "interception" and defendants did not have "consent"). [original footnote 253 on p. 27].

Acts can be said to ensure "essentially equivalent" protection to the EU GDPR, even within their limited scope of application.

Current federal laws with broad application in relation to privacy

As noted earlier, there are two federal laws in the USA that have broader application in relation to privacy, i.e., the 1914 **Federal Trade Commission Act (FTC Act)** and the 2010 **Consumer Financial Protection Act (CFPA)**. The former is the most important for the purpose of this study.

The FTC Act

The FTC Act, originally enacted to strengthen competition law, was amended to prohibit a broad range of unscrupulous or misleading practices harmful to consumers by most, though not all, commercial entities or actors (it does not apply to common carriers, not-for-profit organisations and financial institutions). At its core is the granting of powers to the Federal Trade Commission to take action against "unfair or deceptive acts or practices" (UDAP) by covered entities. Hundreds of such enforcement actions have been taken, usually resulting in "consent decrees" requiring a company to take measures to prevent further violations, and developing a "common law of privacy" where:

> companies are bound by their data privacy and data security promises. The FTC has taken the position that companies act deceptively when they gather, use, or disclose personal information in a way that contradicts their posted privacy policy or other statements, or when they fail to adequately protect personal information from unauthorized access despite promises that that they would do so. In addition to broken promises, the FTC has alleged that companies act deceptively when they make false representations in order to induce disclosure of personal information… The FTC has further maintained that companies act deceptively when their privacy policies or other statements provide insufficient notice of their privacy practices. For instance, in *In the Matter of Sears Holdings Management Co.*, the FTC alleged that Sears acted deceptively by failing to disclose the extent to which downloadable software would monitor users' internet activity, merely telling users that it would track their "online browsing."
>
> Along with "deceptive claims," the FTC has also alleged that certain data privacy or data security practices may be "unfair." Specifically, the FTC has maintained that it is unfair for a company to retroactively apply a materially revised privacy policy to personal data that it collected under a previous policy. The FTC has also taken the position that certain default privacy settings are unfair. In the case *FTC v. Frostwire*, for example, the FTC alleged that a peer-to-peer file sharing application had unfair privacy settings because, immediately upon installation, the application would share the personal files stored on users' devices unless the users went through a burdensome process of unchecking many pre-checked boxes. [135]

However, the broad principles of "deception" and "unfairness" cannot as such be relied on by themselves to read all of the many detailed requirements of EU data protection law into US law. The (since invalidated) EU – US Safe Harbour and Privacy Shield agreements were (not wholly successful) attempts to redress this, by setting out many detailed principles and rules that were supposed to reflect EU data protection law in the relevant documentation, with US companies then being able to self-certify that they would abide by them – which then gave the FTC the right to sanction them if they did not abide by those relatively detailed (EU data protection law-reflecting) stipulations and promises.

In the next chapter, we will assess whether (the other main issue, of access to data by US authorities, aside) such a structure could in the future again be used as a basis for data transfers (perhaps with the

[135] CRS *Data Protection Report* (footnote 111), pp.32–33, footnote references omitted.

FTC issuing "trade regulation rules" [TRRs] to reinforce the structure).[136] However, it should be noted that, like most of the other federal laws noted earlier, the FTC Act does not provide a private right of action –in the next chapter, we will address that issue.

Consumer Financial Protection Act (CFPA)

The CFPA is similar to the FTC Act, in that it seeks to counter "unfair and "deceptive" acts or practices, and in addition also "abusive acts or practices" – but only in relation to the offering or providing of a "consumer financial product or service". It therefore partially filled a gap in the FTC Act which, as noted above, does (*inter alia*) not apply to financial institutions. It created the Consumer Financial Protection Bureau (CFPB) as an independent agency within the Federal Reserve System. The CRS report also notes that in principle:[137]

> the CFPB has some powerful procedural advantages in comparison with the FTC. In particular, the CFPB can enact rules identifying and prohibiting particular [unfair, deceptive, or abusive act or practice] violations through [a simpler] process …; [can] bring civil or administrative enforcement actions against entities engaging in [such practices]; [and] [u]nlike the FTC, the CFPB can seek civil penalties in all such enforcement actions, as well as equitable relief such as disgorgement or injunctions.

However, these powers are rarely used:[138]

> As some commentators have noted, the CFPB could follow in the FTC's footsteps and use its UDAAP authority to regulate data protection. However, the CFPB has generally been inactive in the data privacy and security space. Indeed, to date, it has brought only one such enforcement action, which involved allegations that an online payment platform, Dwolla, Inc., made deceptive statements regarding its data security practices and the safety of its online payments system.

Moreover, like the FTC Act, the CFPA also does not provide for a private right of action.

<u>In sum</u>: The FTC Act has some potential to again be used as a basis for ensuring that personal data transferred from the EU to the USA will be subject to "essentially equivalent" protection to the EU GDPR – but significant reservations in that respect remain (as will be discussed in chapter 4). The potential under the CFPA is more limited.

Proposed broadly phrased federal privacy laws

As explained by Cameron Kerry and John Morris in June 2020:[139]

> Since debate on [federal] privacy legislation began in earnest following the 2018 midterm elections, members of Congress have released over 20 comprehensive information privacy bills or drafts.

More specifically and most recently, in November 2019, Senator Maria Cantwell (D-WA) introduced the **Consumer Online Privacy Rights Act (COPRA)**,[140] and on 3 December 2019, Senator Roger Wicker (R-

---

[136] On TRRs, see the CRS *Data Protection Report*, at p. 31, where obstacles to the creation of such rules are set out, and where it is noted that (because of these) "*FTC rarely uses its TRR rulemaking authority and has not enacted any TRRs regarding data protection.*" We will return to that in the next chapter.

[137] CRS *Data Protection Report* (footnote 111), p. 35.

[138] *Idem*.

[139] Cameron F. Kerry and John B. Morris, Jr., *Framing a privacy right: Legislative findings for federal privacy legislation*, Brookings Institution, 8 December 2020, at: https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/

[140] Consumer Online Privacy Rights Act of 2019, S. 2868, 116th Cong. (2019), at: https://www.congress.gov/bill/116th-congress/senate-bill/2968/text

MS) released the draft **United States Consumer Data Privacy Act (USCDPA)**.[141] As Cameron Kerry noted at the time:[142]

> these two Senate Commerce proposals "frame[d] the issues for this discussion going into the next session of Congress" and introduced clarity to the broader privacy debate.

Shortly after, on 18 December 2019, the House Energy and Commerce Committee staffers circulated a "**bipartisan staff discussion draft**" for comment.[143]

Next, on 12 March 2020, Senator Jerry Moran (R-KS) introduced the **Consumer Data Privacy and Security Act (CDPSA)**.[144] And on 17 September 2020, Senator Wicker and three other Republican Senators introduced another broad national privacy legislation bill, known as **The SAFE DATA Act**, that is "an updated version of the discussion draft of the USCDPA" and actually is:[145]

> a conglomeration of three previously introduced legislative proposals: the discussion draft of the U.S. Consumer Data Protection Act, Filter Bubble Transparency Act and Deceptive Experiences To Online Users Reduction Act.

There are other bills,[146] but as Cameron et al. noted in December last year:[147]

> the bills that are the most likely starting points for legislation in 2021 [are] Sen. Maria Cantwell's (D-Wash.) **Consumer Online Privacy Rights Act**, Sen. Roger Wicker's (R-Miss.) **SAFE DATA Act**, and the House Energy and Commerce "**bipartisan staff draft**" …

---

[141] See: *Fact Sheet: Chairman Wicker's Discussion Draft The United States Consumer Data Privacy Act,* Senate Committee on Commerce, Science, and Transportation, 3 December 2019, at:
https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-statesconsumer-data-privacy-act/

[142] Cameron F. Kerry, *Game on: What to make of Senate privacy bills and hearing*, The Brookings Institution, TechTank, 3 December 2019, at: https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-tomake-of-senate-privacy-bills-and-hearing
Referenced in Cameron F. Kerry, John B. Morris, Jr., Caitlin T. Chin, and Nicol E. Turner Lee, *Bridging The Gaps, A path forward to federal privacy legislation*, Brookings Institution, June 2020, Background, p. 2, at:
https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf

[143] The bill is at:
https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf
See also: Margaret Harding McGill, *Federal privacy legislation shows signs of life in House*, Axios, 19 December 2019, at: https://www.axios.com/federal-privacy-legislation-shows-signs-of-life-inhouse-e519ac0b-b512-47e1-8c84-aaf57d4144cf.html

[144] Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020), at:
https://www.congress.gov/bill/116th-congress/senate-bill/3456/text

[145] Müge Fazlioglu, *Consolidating US privacy legislation: The SAFE DATA Act*, 21 September 2001, IAPP, at:
https://iapp.org/news/a/consolidating-u-s-privacy-legislation-the-safe-data-act/

[146] A year ago, Wendy Zhang of McDermott Will & Emery mentioned the Online Privacy Act, the Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data (DASHBOARD) Act, the American Data Dissemination Act (ADD Act), the Social Media Privacy Protection and Consumer Rights Act of 2019 and the Privacy Bill of Rights Act and noted that the latter, supported by Senate Democrats, "*combines GDPR-like terms (including 'consent prior to collection of personal information') with the CCPA's broad definition of 'personal information'.*" See: *Comprehensive Federal Privacy Law Still Pending*, 9 January 2020, at:
https://www.lexology.com/library/detail.aspx?g=16398ba4-99f2-4250-83fe-37e05ee6ba32

[147] See footnote 139.

US privacy scholar Peter Swire believes that "*This new Congress has the best chance for comprehensive federal legislation that I've ever seen.*"[148]

This is not the place to analyse in detail each and every one of the various proposals – or even these "most likely starting points" three – because if there is going to be a federal privacy law, perhaps even in 2021 (which we feel is still rather optimistic), it will look quite different from any of these texts (and will even then likely not come into effect for a couple of years after adoption). Rather, it will suffice to note the main issues they have in common and the main issues that arise under US law that have not yet been addressed but are still left open. These include in particular the main contentious issues of "pre-emption", i.e., of whether any new broad federal privacy law should override state law or allow states to set higher standards, and of whether to include a right of private action.

The previous US Congress' House Energy and Commerce Committee staff published a bipartisan draft privacy bill at the end of 2019, which helpfully highlighted areas of agreement and disagreement between the two major political parties. The bill would create an FTC enforcement bureau with rulemaking and fining powers, a business support office, and enforcement powers for state attorneys general. Hunton Andrews Kurth has analysed the areas of agreement and disagreement as follows:[149]

Table 2 Areas of Congressional bipartisan agreement and disagreement on 2019 draft House Energy and Commerce Committee staff privacy bill

Agreements	Disagreements
provide individuals with several new privacy rights, including the rights to access, delete and correct their data; require companies to maintain privacy policies and for large companies to provide annual filings to the FTC, including the results of an internal risk assessment and the measures taken to address those risks; require companies to implement a privacy program and establish reasonable policies, practices and procedures for the processing of covered data. It would also require larger companies to have a designated privacy protection officer; require express affirmative consent for the processing of covered data unless the processing is "consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual." It specifically notes that express affirmative consent is required for all processing of sensitive information, and that consent must be given separately for each use of information;	preemption of state laws; a private right of action; the list of exceptions for when consent is not required to process covered data and how to treat pseudonymized and publicly available information; the specific thresholds (such as annual revenue and amount of data processed) for enhanced requirements for large companies; the sections where the FTC does and does not have rulemaking authority; an entire sub-section on opt-out requirements for the processing of covered information for first-party marketing purposes; an entire section on the prohibition of discriminatory use of data; an "Additional Prohibitions" section which includes prohibitions conditioning the provision of a product or service on an agreement to waive rights granted by the bill and a prohibition on financial incentives for waiving those rights;

[148] Quoted in Jennifer Bryant, *2021 'best chance' for US privacy legislation*, IAPP, 7 December 2020, at: https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/

[149] Hunton Andrews Kurth, *House Energy and Commerce Committee Staff Release Bipartisan Draft Privacy Bill*, 20 December 2019, at: https://www.huntonprivacyblog.com/2019/12/20/house-energy-and-commerce-committee-staff-release-bipartisan-draft-privacy-bill/

prohibit certain practices such as obtaining covered information by false pretenses and processing biometric information to identify an individual; require that companies not keep or store data for longer than is reasonably necessary for the purpose for which the data was processed; impose safeguards on data transferred to processors and third parties that limits further use of that data; require companies to implement reasonable data security "policies, practices and procedures to protect and secure covered information against unauthorized access and acquisition"; exclude de-identified information from the definition of covered information; and require data brokers to disclose publicly that they are data brokers and register with the FTC.	the size of the new FTC Bureau of Privacy; and several definitions, such as covered information, de-identified information, health information, information broker, pseudonymized information, sell and sensitive information.

There are clearly a number of areas – such as stricter requirements for valid, informed, "affirmative, express consent", tighter restrictions on the use of sensitive data, limitations on automated (algorithmic) decision making, greater data subject rights, privacy impact assessments and improved supervision and enforcement – in which US federal law would move closer to the European standards discussed in chapter 2, if a federal law on the above lines would be adopted.

In some respects, the proposed laws may even go beyond EU law, e.g., by both COPRA and SAFE classifying as "sensitive covered data", *inter alia*: financial account details that allow access to an account, online account log-in details including passwords, "precise geolocation information", certain browsing information, phone logs, photos and videos held on a device for private use (as well as data revealing a person's race or ethnic origin, health, biometric data, etc., that are also defined as sensitive in EU data protection law). (To some extent, e.g., *re* "precise geolocation", the data would often also be classified as sensitive under the GDPR, but not necessarily always.)

The proposed laws also contain important and interesting provisions that seek to protect individuals from uses of their personal data that would result in their discrimination on grounds of race, religion, sexual orientation, etc. (processing resulting in discrimination would also be contrary to the GDPR, because it would be "unfair" – but the GDPR does not provide similarly detailed rules, in particular not in relation to algorithms, although there is EDPB guidance on this).

On the other hand, "[trade] union membership" is included (in a limited way: see below) in the list of sensitive data in COPRA, but not in SAFE, and the rules on the processing of sensitive data are not as strict as the ones in the GDPR (cf. the section on "exceptions to affirmative express consent" in COPRA), and some categories are limited in ways not done in the EU. For instance, under both COPRA and SAFE, data revealing an individual's racial or ethnic origin, religion, sexual orientation or sexual behaviour, and under COPRA also data on [trade] union membership, are subject to the (stricter) rules on the processing of sensitive data – but only to the extent that such information is used "in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer [read disclosure] of such information" (SAFE; COPRA has "… regarding disclosure of such information").

The proposed laws also contain numerous provisions that rest on vague terms such as "reasonably linkable", "information that could readily be used to reidentify [an individual]", "the expectation of a

reasonable individual", "reasonable due diligence", "information that cannot reasonably be used to infer information about, or otherwise be linked to, an individual", "what is reasonably necessary, proportionate, and limited to [the specific purpose of the processing". SAFE refers to the "right to reasonably access [one's data]". These terms and the rules in which they are used are likely to be less strictly interpreted and applied than the corresponding European terms.

Overall, in terms of substance, both bills and the bipartisan staff draft clearly offer very significant improvement in protection of personal data (as seen from Europe). However, as currently drafted, none of them actually achieve "essential equivalence" in protection compared to the EU GDPR in all material respects.

Most importantly, the proposed laws are still much more limited in scope than the European ones and cannot be said to constitute "omnibus" laws. For instance, both COPRA and the SAFE Act exclude "de-identified data" (which under COPRA includes pseudonymised data provided the controller "publicly commits" to not attempting to re-identify the data; SAFE also excludes "aggregated data", i.e., "information that relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual"), "employee data" and data from "public records" (COPRA)/"publicly available information" (SAFE) from their protection. Neither COPRA nor SAFE, if adopted, would apply (at all) to entities that are not subject to the FTCA (such as financial institutions). COPRA also excludes "small businesses" from its scope. These are defined as entities with an annual average gross revenue of less than $25,000,000 that do not process data on more than 100,000 individuals, households, or devices used by individuals or households and that do not derive 50 percent or more of their annual revenue from transferring (read in particular: trading in) personal data. The SAFE thresholds for "Internet platforms" are $50,000,000 and 1,000,000 individuals. In both the EU and the USA, these conditions would exclude most companies from the rules.

<u>In sum</u>: Given the rather vague and sometimes weakly phrased principles and rules in the proposed laws, the likely broad exemptions, and the many still unresolved issues, any broad federal privacy law on the lines of the current proposals would not provide "essentially equivalent" protection to personal data as is provided by the GDPR. Unless a law very significantly stronger than any of the bills currently proposed is adopted, no future federal US law is likely to meet the EU standards discussed in chapter 2.

3.1.4 US state privacy laws

Overview

According to the OneTrust/DataGuidance "USA State Law Tracker",[150] consumer privacy bills have been passed in the following US states: Arkansas, California, Connecticut, Maine, Nevada, Utah, Vermont, and Virginia. There are proposed laws (bills) in the following further states: Alabama, Arizona, Colorado, Connecticut, Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Minnesota, New Hampshire, New Jersey, New York, Oklahoma, Rhode Island, South Carolina, and West Virginia. Proposed laws failed to pass in Florida, Mississippi, Nebraska, Texas, Utah, Virginia, Washington, and Wisconsin.

[150] https://www.dataguidance.com/comparisons/usa-state-law-tracker
The Tracker page is undated but appears to be fairly up to date: the entry for Alabama, for instance, refers to a bill that was introduced on 2 February 2021. The Tracker excludes laws and bills that deal specifically with issues such as biometric information, facial recognition, and data breaches. Such specific laws and bills are also not assessed in the present study, which focusses on general privacy laws in the context of EU adequacy issues.

The State Law Tracker information notes nine issues covered (or more often not covered) by the state laws: right of access, right of deletion, data portability, opt-out (from disclosures to third parties), automated decision-making, data security, the use of processors/service providers, privacy notices, and enforcement. This is of course a rather more limited list than the list of issues that must be evaluated in an adequacy assessment: the nine data subject rights recognised in the EU GDPR, unambiguously expressed consent (rather than opt-out/implied consent), scope, purpose specification and -limitation, restrictions on the processing of sensitive data (and the categories of data that concept covers), informing of data subjects (rather than just requiring privacy notices), general restrictions, and restrictions on onward transfers. The EDPB's Adequacy Referential list even more: 13 issues.

It is not useful or necessary to look at even the passed laws in any detail: even a quick click-through through the State Law Tracker shows that the majority of US state laws do not even address – let alone address in an "essentially equivalent" way to the EU GDPR – the limited issues noted in the Tracker. Only Massachusetts and Minnesota "tick all the boxes" in the Tracker – but both still only have bills, not passed laws.

Of the states that have laws in place, there is no doubt that California is the most advanced – even if the laws (the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)) do not "tick all the boxes" in the Tracker. We will look at those laws in detail in the next sub-section.

Here, it will suffice to conclude as follows:

In sum: The CCPA and CPRA are the most advanced comprehensive state privacy laws. At most, other US state laws may move closer towards the CCPA, and in due course the CPRA. But for the foreseeable future, the CPRA will be the highest standard for privacy in the USA.

The most advanced state laws: the CCPA and the CPRA

In 2018, the CCPA was adopted; it came into effect on 1 January 2020. The CCPA gave California consumers the right to learn what information a business had collected about them, to delete their personal information, to stop businesses from selling their personal information, including using it to target them with ads that follow them as they browse the Internet from one website to another, and to hold businesses accountable if they did not take reasonable steps to safeguard their personal information. It is still the most advanced privacy law of any US state, but in many respects, it still falls significantly short of the EU standards, e.g., by not requiring a legal basis for processing, having only a limited focus on accountability and, especially, by very broad exclusions from its scope.[151]

In order to enhance privacy protection in the state, the California Privacy Rights Act (CPRA) was adopted on 3 November 2020. It significantly amends and expands upon the CCPA (and is therefore also referred to as "CCPA 2.0"). It will take effect on 1 January 2023 and will become fully enforceable on 1 July 2023 (but will apply to data collected from 1 January 2022, except for the right of access) – but it is already casting its shadow forward (and sideways, to other US states and other countries, as noted towards the end of this section).

[151] For details, see the DataGuidance/Future of Privacy Forum booklet, *Comparing privacy laws: GDPR v. CCPA*, 2018, at: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

Below, we will look first at the scope of the CPRA and then at its more specific contents, compared to the European standards we summarised in chapter 2.[152]

Scope of the CPRA

The CPRA applies to any "**business**" that "**controls**" the "**collection**" and/or the "**use**", "**retention**", "**sharing**", "**selling**" or "**disclosing**" of "**personal information**" of a "**consumer**".

However, each of these terms is defined in crucially restrictive ways in section 1798.140:

- the Act only applies to **businesses** (companies etc.) that "do[ ] business in the State of California" and that meet one or more of the following thresholds:[153]
  - annual gross revenues of >$25 million;
  - buys, sells, or shares the personal information of 100,000 or more consumers* or households; or
  - derives 50 per cent or more of its annual revenues from selling or sharing consumers'* personal information.

  (S. 1798.140(d)(1))

By limiting the scope of the law to "businesses", the law does not cover processing of personal data by not-for-profit organisations such as charities, civil society associations, churches, political parties, many educational establishments, etc, that are subject to EU data protection law. Moreover, even for for-profit entities, the thresholds are high. They mean that even in California most small or medium-sized companies are not mandatorily subject to the Act, and that most non-Californian SMEs are also not subject to the Act, even if they "do business in California" and collect personal information on consumers* in California (unless trading in consumer data is a main part of their business).

However, a company that does business in California but that does not meet any of these thresholds can "**voluntarily certif[y]**" to the California Privacy Protection Agency "that it is in compliance with, and agrees to be bound by, [the CPRA]" – and is then also bound by it (albeit also still only in relation to data on Californian consumers/residents: see below).

(S. 1798.140(d)(4))

- A "**consumer**" is defined as "a natural person who is a California resident".[154]

  (S. 1798.140(i))

In other words the Act does not apply to individuals resident elsewhere in the USA, or anywhere outside the USA (such as the EU). The Californian legislator, like the US federal legislator (but unlike the EU one), does not subscribe to the principle of universality of human rights (or at least of data protection/privacy rights).

---

[152] We draw on Graham Greenleaf, *California's CCPA 2.0: Does the US finally have a data privacy Act?,* (2020) 168 Privacy Laws & Business International Report, 13-17, December 2020, in which he compares the CPRA standards to the standards set in what he terms the three "generations" of data protection instruments (1980 OECD Guidelines and 1981 Council of Europe Convention No. 108; 1995 EC Data Protection Directive; and the GDPR and the Modernised Council of Europe Convention, Convention 108+"). The report is at: https://ssrn.com/abstract=3793435

[153] Entities that share common control and common branding to also share consumer personal information are considered to be the same "business."

[154] As Greenleaf (footnote 152) notes, "[b]y complex means, the Act's protections are also to some extent extended to employees and 'independent contractors'" (footnote 4).

- "**Personal information**" is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

  (S. 1798.140(v)(1), which adds a long list of examples in sub-sections (A) to (L)).

On the face of it, this definition is close to the EU GDPR definition of "personal data".[155]

However, it is doubtful whether the CPRA applies to information on a person who is "singled out" from others in a larger group without being otherwise "identified". There are also likely to be differences in the application of the CPRA and the GDPR in relation to pseudonymised data.[156] Moreover, the Act stipulates that:

> "'Personal information' does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means:
>
> - information that is lawfully made available from federal, state, or local government records, or
> - information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or
> - information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience."
>
> (S. 1798.140(v)(2), bullet points added.)

Note that this actually expands the carve-out from the CCPA that only applied to information made available through government records. Moreover, as HoganLovells note:[157]

> There are ambiguities here that will need to be sorted out. … [I]t is not clear how broad the exception in the third bullet is. That exception would apply to product reviews and similar information that consumers provide to businesses, unless the consumer stated, "This is for your eyes only." But would the exception apply to home addresses, phone numbers, or other information that consumers provide to businesses if consumers do not expressly restrict the scope of disclosure? Regardless of how these ambiguities are resolved, the expanded exception removes from the scope of the CPRA information that a consumer makes available to the general public via social media. The term "available to the general public" is not defined in the CPRA, but presumably it would include social media content

[155] The reference to information on a household also constituting "personal information" could be read as being wider than the EU concept of personal data (see the next footnote). However, in the EU, information on a household, if applied to all or any persons in the household, will be treated as personal data relating to the person(s) to which it is applied – and in certain cases there could be doubts as to whether data on a household can be said to be sufficiently accurate in relation to (the taking of decisions on) one person in the household. If it is not, the data should not be used in that way/in relation to that person.

[156] Cf. Recital 26 to the GDPR that expressly mentions "singling out" of an individual as a form of identification, and that expands on the concepts of pseudonymisation and anonymisation, and the guidance on the concepts of "personal data" and on pseudonymisation issued by the EU Article 29 Working Party (the predecessor to the current European Data Protection Board).

[157] HoganLovells, *CPRA countdown: Changes to the definition of "personal information"*, 29 January 2021, at: https://www.engage.hoganlovells.com/knowledgeservices/news/countdown-to-the-california-privacy-rights-act-changes-to-the-definition-of-personal-information

available to all users and would not include social media content made available only to limited audiences.

Most if not all of the categories of information excluded from the concept of "personal information" under this sub-section (v)(2) would, in the EU, be classified as "personal data"[158] (even if the use of some of them, such as information [manifestly] made public by the data subject or obtained from a publicly accessible register, may be subject to fewer restrictions). The GDPR of course clearly applies to "information made available by a person to whom the consumer has disclosed the information". **This carve-out is reminiscent of the "third party" doctrine.**[159] **It suggests a very significant deficiency in protection from a European point of view.**

- the concept of "collecting" is quite widely defined and notably includes "accessing" personal information: see Section 1798.140, sub-section (f) (definition of "collects", "collected" and "collection"). The concepts of "using" and "retaining" of personal data are also broad (even without being specifically defined), and the concept of "selling" personal information extends to the making available of such data to a third party "for monetary or other valuable consideration" (sub-section (ad), defining "sell", "selling", "sale" and "sold"). On the other hand, the term "sharing" of personal data only applies to sharing of personal information "for cross-context behavioral advertising (sub-section (ah), defining "share", "shared" and "sharing".

In our opinion, there are likely to be acts that can be performed upon personal information that would constitute "processing" as (very broadly) defined in the EU GDPR[160] that may not be caught by the CPRA – such as, for instance, erasing or destroying such data.

Crucially, the CPRA retains **a number of sweeping exemptions** that were also included in the CCPA. Thus, the Act does not apply (at all) to:

- conduct that takes place wholly outside of California and that relates to a consumer who (although normally resident in California) was not in California when her data were collected (which may not always be easy to establish, especially in an online context);
- information collected from employees, job applicants, owners, directors, officers, medical staff, members or contractors of a business (collectively referred to as "employee information"); and
- data that are subject to other US laws including some that we discussed earlier, including:
    - "Protected Health Information" (PHI) that is collected by entities that are subject to HIPAA (and California's analogous law, the Confidentiality of Medical Information Act, CMIA) (S. 1798.145(c)(A);
    - Personal information subject to the Fair Credit Reporting Act (FCRA) so long as the activity is authorized by the FCRA (but this exemption does not apply to the data breach liability provision) (S. 1798.145(d));

[158] Cf. the GDPR definition of "personal data", quoted in full in footnote 30.

[159] The third-party doctrine is a United States legal doctrine that holds that people who voluntarily give information to third parties—such as banks, phone companies, internet service providers (ISPs) and e-mail service providers—have "no reasonable expectation of privacy." Although recently heavily criticised by Members of Congress and individual judges on the Supreme Court (most notably Justice Sotomayor), it has not (yet) been overturned or significantly changed. See the US Congressional Research Service report by Richard M. Thompson II, *The Fourth Amendment Third Party Doctrine*, 2014, at: https://fas.org/sgp/crs/misc/R43586.pdf and Francesca Bignami, footnote 121.

[160] Cf. the GDPR definition of "processing", quoted in full in footnote 31.

- Financial information that is processed pursuant to the Gramm Leach Bliley Act (GLBA) or the California Financial Information Privacy Act (CalFIPA) (S. 1798.145(e)).

Graham Greenleaf holds that: [161]

> [The CPRA] is the first US law [applicable to private sector data] with more than a narrow sectoral scope which can usefully be described as "a data privacy law" [what we have referred to as an "omnibus law" – DK/IB] rather than just "a law including some privacy protections".

However, it will be clear from the above that the law is far from all-encompassing. This alone would make it difficult to see how the CPRA could be a basis for any EU adequacy finding, as some have suggested. At best, any such decision would have to be limited to data transfers to US entities that are subject to the CPRA, or that have self-certified that they will abide by its provision, and would only cover personal data covered by the law and the categories of processing mentioned earlier. It could not cover any information excluded from the law, or from the concept of "personal information".

The comparative analysis of the CPRA and GDPR in the following sections partially draws on the charts in Greenleaf's report, on pp. 2–3 and 4–5, respectively. In these, full references are provided to sections and quotations from the Acts for each assessment. The comments in the right-hand columns in our text are our own, but essentially tally with Greenleaf's assessments. We colour-code each assessment as dark green (fully met), light green (largely met), orange (not met) and blue (exceeded).

Purpose specification and limitation (and related matters)

Personal data must be collected fairly, for lawful and legitimate purposes	Partially reflected in the CPRA (specific purposes but nothing about their legitimacy)
The purposes for which personal data are collected must be specified	Fully reflected
Personal data must only be used or disclosed for the specified purposes or for compatible purposes	Fully reflected
Data must be necessary for the specified or compatible purpose(s)	Largely reflected (data must be "*reasonably* necessary and proportionate" for the relevant purpose(s)
Personal data must be relevant, accurate, up to date, etc., for the specified purpose(s)	**Not reflected** (but there are obligations to correct inaccuracies and to delete data after intended use)
Data must not be retained in identifiable form when no longer necessary for the specified or compatible purpose(s)	Largely reflected (data must not be retained for longer than is "*reasonably* necessary" for the relevant purpose(s)

[161] Graham Greenleaf, o.c. (footnote 152), p. 7.

Grounds for lawful processing (selection)

Personal data must only be processed on the basis of a specified legitimate ground (legitimate basis)	**Not reflected** (except as indicated below)
- Processing on the basis of express consent	Fully reflected
- Processing that is necessary to perform a contract (or pre-contractual checks)	Partially reflected in that consumers have the right to direct a business that collects *sensitive* personal information about them to limit its use to what is necessary to perform the services or provide the goods.
- Processing on the basis of a controller's "legitimate interests" (balance)	
- Processing on the basis of laws that meet rule of law requirements	**Not reflected** (There are extensive carve-outs allowing processing when required or authorised by law – but no stipulations that the laws must meet certain requirements)*

Special categories of data ("sensitive data")

Processing of sensitive data must be more strictly regulated	Partially reflected (interesting, very broad definition of sensitive data, but the restrictions are less strict than the EU ones)

Informing of data subjects

There must be general openness about processing of personal data	Fully reflected (by detailed requirements on prominently providing privacy notices.
Data subjects must be informed about the purposes of the processing and of other details	

Data subject rights

Right of access	Basically reflected (but further regulation to come)
Right of correction and deletion	Basically reflected (but further regulation to come)
Right to restriction of processing (i.e., the blocking of data pending a dispute);	Basically reflected (but further regulation to come)
Right to have third parties to whom the data were disclosed informed of any rectifications, erasures or restrictions (unless this is impossible or involves disproportionate effort);	
Right to data portability	**Not reflected**
Right to object to processing	Basically reflected

	(but further regulation to come)
Right not to be subject to fully-automated decisions	Basically reflected (but further regulation to come)

General restrictions

Laws that impose restrictions on any of the rights and obligations must meet basic rule of law requirements (legitimate purpose, necessity, proportionality, etc.)	Not expressly reflected (see the extensive list of exemptions in S. 1798.185), but of course US constitutional legal constraints apply to the exercise of statutory powers by authorities. (But some of those may not apply to non-US persons).

Restrictions on onward transfers (data exports)

Arrangements must be put in place to ensure that any onward transfers of EU personal data from the third country to another third country that has not been held to provide "adequate"/"essentially equivalent" protection compared to the GDPR do not undermine the protection of the data.	**Not reflected** (other than in stipulations requiring third-party recipients of personal information to offer the same level of protection (see S. 1798.140(i) re 'contractors'). As Greenleaf notes, "[e]nforceability and other issues remain."

Greenleaf concludes on the basis of the above assessments that CPRA meets all but one of the "first generation" principles (as contained in the 1980 OECD Guidelines and the 1981 Council of Europe Convention No. 108) and seven out of ten "second generation" principles (as contained in the 1995 EC Data Protection Directive), and is therefore broadly in line with the average standard of protection provided by existing non-European laws: the average number of "second generation" principles included in data privacy laws outside Europe in 2012 was also 7/10,[162] and this also appears to be broadly the case in relation to the current, much greater number of non-European countries that have such laws.[163]

However, while the CPRA meets some of the latest, higher, "third generation" EU GDPR (and Council of Europe Convention 108+) standards, and indeed exceeds those in one respect, it does not meet many others, as indicated below:

Additional GDPR standards

The controller must be able to demonstrate compliance, in particular through mandatory records ("accountability principle")	**Not reflected** (although there are sanctions on non-compliance)

[162] Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, in:' International Data Privacy Law, Vol. 2, Issue 2, 2012, at: https://ssrn.com/abstract=1960299

[163] Graham Greenleaf, *European Data Privacy Standards Implemented in Laws Outside Europe*, (2017) 149 Privacy Laws & Business International Report 21-23, at: https://ssrn.com/abstract=3096314

Data protection must be provided "by design and by default"	**Not reflected**
The competent data protection authority must be informed of any personal data breaches (unless they pose no risk)	Not reflected in the CPRA but a duty to report data breaches to the California A-G is contained in other laws
Data subjects must be informed of high risk personal data breaches	**Not reflected**
Controllers must carry out a data protection impact assessment for high risk operations	Regulations to be issued on mandatory annual cybersecurity audits and "regular" risk assessments for processing that carries a "significant risk"
Controller must consult the competent data protection authority over processing operations that pose high risks that cannot be sufficiently mitigated, prior to the operation	**Not reflected**
Certain controllers must appoint a data protection officer	**Not reflected**
Data subjects must have the right to be represented by a not-for-profit body in "representative actions" (quasi class actions)	**The CPRA grants wider class action rights than the EU GDPR.**[164]
The data protection authorities can impose administrative fines of up to 4% of a company's annual turnover on controllers for violations of the rules	Fully reflected, in that the California PPA can impose fines of up to $2,500 for each violation or $7,500 for each intentional violation – whereby an act that violates the rights of a multitude of individuals counts as a violation in respect of each of them (meaning that for a violation affecting, say, 10,000 consumers, the PPA can impose a fine of up to $25,000,000).

Matters that are still to be properly regulated

After public consultations, initially the California Attorney-General and later[165] the California Privacy Protection Agency, are to issue regulations on a range of matters including for the purposes of:

[164] See: JDSupra, *The Expanded Private Right of Action under the CPRA*, 7 December 2020, at: https://www.jdsupra.com/legalnews/the-expanded-private-right-of-action-99187/

The authors point out that the CPRA adds email address in combination with a password or security question and answer that would permit access to the consumer's account to the list of data types that can be actionable under the law in the event of a breach, and note that "[t]his information is widely available on the dark web and also is often reused by consumers, making credential stuffing and related tactics particularly effective tools for gaining access to consumer accounts. Consequently, it seems inevitable that there will be a sharp rise in class action litigation as plaintiff's attorneys and consumers make claims for statutory damages available under this provision."

[165] From 1 July 2021 or "six months after the agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title", whichever is the latest (S. 1978.185(22)(d)).

- updating or adding categories of personal information to the definitions of "personal information" and "sensitive personal information";
- updating the definitions of "de-identified" information and of "unique identifier";
- establishing exceptions (in particular, to the right of access) to protect intellectual property rights and trade secrets;
- further regulating opt-outs from data sharing and selling and the use of standard logos or an "opt-out preference signal" for that purpose;
- clarifying the modalities for the exercise of data subject rights of access and correction;
- "identifying [the] business purposes … for which service providers and contractors may use consumers' personal information received pursuant to a written contract …, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy";
- further defining "precise geolocation";
- requiring "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to both "perform a cybersecurity audit on an annual basis" (and clarifying the factors to determine when such risks arise), and to submit to the California Privacy Protection Agency "on a regular basis", a broader privacy risk assessment, "with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public";
- regulating access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling, including creating a right of consumers to be provided with "meaningful information about the logic involved in such decision making processes, as well as a description of the likely outcome of the process with respect to the consumer' involved" (but the repeated emphases elsewhere on the need to protect IP rights and trade secrets suggest that this is unlikely to lead to a right to be provided with access to the actual algorithms or software)

(S 1798.185)

Any full assessment of whether the CPRA meets the EU standards set out in chapter 2, and can therefore be considered to provide "essentially equivalent" protection to the EU GDPR, will have to await many of the above further clarifications and regulations. However, this does not stand in the way of the tentative assessment below.

<u>In sum</u>: The CCPA and especially the CPRA constitute significant developments in terms of US privacy laws. The CPRA in brings California privacy law in line with the average standard of protection provided by existing non-European laws and the 1981 Council of Europe Convention – but even when fully in force in 2023, the CPRA will still not meet the EU standards discussed in chapter 2, and exempts broad areas such as financial services and health data from its scope altogether. Nor is it likely that any other US state will adopt any law going beyond the CPRA. At most, other US state laws may move closer towards the CCPA, and in due course perhaps the CPRA. US state privacy laws will not provide "essentially equivalent" protection to the EU GDPR for some time (if ever).

3.2 US surveillance laws

3.2.1 Overview of FISA s.702, E.O. 12333 and PPD-28

The US surveillance laws assessed by the CJEU in the *Schrems II* judgment are summarised by the US Congressional Research Service as follows:[166]

Foreign Intelligence Surveillance Act (FISA) Section 702

FISA regulates US national security and foreign intelligence-related electronic surveillance. "Foreign intelligence information" (i.e., information that may be collected under FISA) is very broadly defined. In relation to non-US persons, it includes not only information that relates to threats against the USA (§ 1801, para. (e)(1)), but also:

> information with respect to a foreign power or foreign territory that relates to, … —
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.
>
> (§ 1801, para. (e)(2). In relation to US persons the information must be "necessary" for these purposes.)

Snowden revealed that the Act had been widely used by the US intelligence agencies to carry out economic espionage and to spy also on allies and leading allied politicians, and revelations of such abuses continue to appear.[167] Former US Assistant Attorney-General Jack Goldsmith has noted: "Given the USG's broad economic interests, and the tight link between economics and national security, one can assume that NSA collection of commercial and economic information is very robust… of course I tend to trust the word of U.S. intelligence agencies, while the rest of the world does not, and has little reason to do so, especially since the policy of not giving stolen economic secrets to U.S. firms is a policy without (to the best of my knowledge) any basis in law."[168]

The US government must generally obtain a warrant from the specialized Foreign Intelligence Surveillance Court for "US person" targets; but section 702 allows foreign intelligence-related information to be gathered targeting non-US persons outside the US, following FISC reviews of "generally applicable targeting and minimization procedures and guidelines" from the U.S. Attorney General and the Director of National Intelligence. Once approved, the government may require electronic communications service providers (such as telecommunications companies, Internet Service Providers, and "remote computing service providers" such as cloud computing storage or processing

---

[166] CRS, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, 17 March 2021, available at: https://fas.org/sgp/crs/row/R46724.pdf

The US CRS report refers in particular to the *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and CIVIL LIBERTIES OVERSIGHT BD., 107, n. 471 (July 2, 2014) (abbreviated reference *PCLOB Report*), at:

https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

As noted in chapter 2, section 2.3.1.3, the CJEU assessed these regimes and in particular the limitations and guarantees inherent in them by reference to their descriptions in the Commission's Privacy Shield adequacy decision (quoted in the section in the judgment headed "*The Privacy Shield Decision*", at paras. 42 – 49 of the judgment). For the reasons set out in footnote 111, above, we here prefer to use the US CRS summaries, but believe there are no significant differences between them.

[167] See footnote 77.

[168] Jack Goldsmith, *Reflections on U.S. Economic Espionage, Post-Snowden*, Lawfare, 10 December 2013, at: https://www.lawfareblog.com/reflections-us-economic-espionage-post-snowden

services) to give "all information, facilities, or assistance" needed. FISA does not necessarily govern acquisition of information outside the US. These powers were used in the "downstream" (also known as "PRISM") and "upstream" surveillance systems revealed by Edward Snowden in 2013 to widespread criticism, including from the European Parliament, as the CRS noted:

> For example, the government has used FISA 702 to implement *downstream* (previously referred to as "PRISM") and *upstream* collection programs.[169] In downstream collection, the government typically directs consumer-facing communications service providers—such as ISPs, telephone providers, or email providers—to provide all communications "to or from" a "selector" (e.g., an email address). Upstream collection similarly involves the collection of all communications "to or from" a selector, but the requests are directed at telecommunications "backbone" providers (i.e., companies that operate the long-distance, high-capacity internet cables that interconnect with ISPs' local networks) and it does not involve collection of telephone calls.[170] Under the government's procedures, the National Security Agency (NSA) is the primary intelligence agency that collects data through the downstream and upstream programs, although the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA) also receive data from these programs in more limited circumstances.

Executive Order (E.O) 12333

Outside the United States, electronic surveillance activities of the US intelligence community targeting non-US persons are generally governed by US Presidential Executive Order 12333. The order allows the National Security Agency to "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions". The order also provides it does not "create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person."[171]

Presidential Policy Directive 28 (PPD-28)

PPD-28 was issued by President Obama following the Edward Snowden leaks.[172] It contains limits on the use of signals intelligence collected in "bulk" by the intelligence community for the purposes of detecting and countering:

> (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States

---

[169] See *PCLOB Report* [note 102], at 7 ("There are two types of Section 702 acquisition: what has been referred to as 'PRISM' collection and 'upstream' collection."); NSA Stops Certain Section 702 "Upstream" Activities, NSA (April 28, 2017) ("Under Section 702, NSA collects internet communications in two ways: 'downstream' (previously referred to as PRISM) and 'upstream.'") (hereinafter *NSA Press Release*). [original footnote]. At:
https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/

[170] While upstream collection used to include communications "about" the selector (e.g., the target email address is referenced in the body or text of the email but they are not a party to the communication), the NSA announced in 2017 that it would no longer collect communications that are solely "about" the target. *NSA Press Release*, *supra* note [108]. [original footnote]

[171] *Executive Order 12333: United States Intelligence Activities* (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), sec. 1(7)(c)(1) and sec. 3(7)(c), at:
https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf

[172] *Presidential Policy Directive – Signals Intelligence Activities*, Policy Directive PPD-28, 17 January 2014, at:
https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

> and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

Section 4 of the Directive also requires:

> All 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. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.

This section includes principles familiar from the GDPR: minimisation, data security and access, data quality, and oversight. It also requires the identification of an executive branch Privacy and Civil Liberties Official to support policy development, and a Coordinator for International Diplomacy to "serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States."

3.2.2 "Secret law"

While the publication of E.O. 12333 and PPD-28 provides a greater level of transparency than in many other countries,[173] it is still the case 'the president may "modify" or "waive" them simply by departing from their terms, without providing any notice to the public.'[174]

Even with statutory provisions, the US Department of Justice's Office of Legal Counsel (OLC) regularly issues classified legal interpretations on national security matters which are binding on the executive branch. If a court later disagrees, the Justice Department will still not "investigate or prosecute somebody for acting in reliance" on such an opinion.[175] Such opinions were used during the George W. Bush administration to justify US torture and warrantless surveillance, with a later Bush-appointed attorney-general (Jack Goldsmith) observing OLC lawyers dealt with the Foreign Intelligence Surveillance Act "the way they dealt with other laws they didn't like: they blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations."[176]

Congressional committees, particularly the permanent intelligence committees, frequently issue reports with classified annexes. Some of these are important for the interpretation of statutes, and in some cases their provisions are incorporated by reference into legislation.[177] And the Foreign Intelligence Surveillance Court's decisions, such as authorising surveillance programmes under FISA s.702, can contain significant legal interpretations. One example was the Court's interpretation of s.215

---

[173] Ian Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, Towards Multilateral Standards for Surveillance Reform, In Russell A. Miller (ed., 2017) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, pp.461–491.

[174] Elizabeth Goitein, *The New Era of Secret Law*, Brennan Center for Justice at New York University School of Law, 2016, p.5, at: https://www.brennancenter.org/sites/default/files/2019-08/Report_The_New_Era_of_Secret_Law_0.pdf

[175] *Ibid.* p.37.

[176] *Ibid.* p.38.

[177] *Ibid.* pp.29—31.

of the Patriot Act, on whether business records sought by the government were "relevant" to a terrorism investigation, to cover almost every American's phone records.[178]

While important FISC opinions have been declassified and published by the Director of National Intelligence, which is now required by the USA Freedom Act of 2015, one 2016 assessment "ascertained that most of the significant pre-Snowden FISA case law remains undisclosed, including 25-30 still-classified opinions or orders issued between mid-2003 and mid-2013 that were deemed significant by the Attorney General."[179]

3.2.3 Assessment by EU standards

At the highest level, it will suffice to simply reiterate that (as the US CRS report also notes), the CJEU invalidated the EU Commission Privacy Shield decision because it determined that FISA Section 702 and E.O. 12333, even as limited by PPD-28, are too permissive to meet the GDPR's standards of necessity and proportionality and do not provide EU data subjects with effective judicial redress.

See section 2.3.1.3, above, Requirements relating to access to personal data by third country authorities, and in particular the detailed discussion of the CJEU *Schrems* II judgment in the sub-section on *CJEU requirements relating to indirect or direct access to personal data by third country intelligence agencies*.

More specifically, we have assessed the US laws with reference to the following specific EU standards:

EU standard: Protection of personal data should apply (and apply equally) to all persons irrespective of their nationality, status or where they are

See section 2.2.1, above, In Europe, data protection is a fundamental right, and in particular the discussion under the heading *The principle of universality of human rights (and therefore of data protection)*.

Assessment: This is not reflected in US surveillance laws which limits crucial protections to US nationals and residents.

See section 3.1.1 and 3.1.2, and the reference to the view of the USA on the UN ICCPR, noted there.

EU standard: All personal data and all forms and stages of processing of personal data should be protected

See the reference to the need, in the European view, for "omnibus" data protection laws, mentioned in section 2.2.1, above. The principle is reflected in the 1981 Council of Europe Convention which requires the state-parties to apply their laws broadly, to (all) "automated personal data files and automatic processing of personal data in the public and private sectors" (Art. 3(1))[180] and in the broad application of the EU GDPR. Note also the express application of the GDPR by the CJEU to all processing of personal data including collection and retention (*DRI* judgment), and the express application of the ECHR by the ECtHR, too, to all stages of intelligence bulk data collection (*BBW*, judgment, para. 330, paraphrased in the second bullet-point on p. 45, above).

Assessment: This is not fully reflected in US privacy and surveillance laws which do not protect all personal data (as widely defined in EU law), and which protect metadata less than content data (and both barely at all if they relate to non-"US persons"). The US authorities also consistently argue that there is only an interference with a person's privacy rights when that person's information is accessed by an official – i.e., that "mere" collecting and retaining of personal data (such as communication data)

[178] *Ibid*. p.58.

[179] *Ibid*. p.6.

[180] This is subject to the stipulation that any State of automated personal data files" (Art. 3(2)(a)).

does not constitute an interference with privacy as long as no official has looked at the data (even though the data may well be subject to automated filtering, etc.).

See the observation in section 3.1.3, that "*Most [US federal privacy laws] impose data protection obligations [only] on specific industry participants—such as financial institutions, health care entities, and communications common carriers—or [in relation to] specific types of data*", usually referred to as "covered entities" and "covered [personally identifiable] information"; the discussion in that section of the limitations in the proposed broadly phrased federal privacy laws; and our conclusion in section 3.1.4, that even the most advanced state laws, the CCPA and the CPRA, are still "far from all-encompassing", i.e., are too limited in terms of scope and definitions of "personal information" [and the exceptions to that concept] to be considered "omnibus" laws.)

European standard: All surveillance measures and actions must comply with rule of law standards

See in general section 2.2.1, above, In Europe, data protection is a fundamental right, in particular the first bullet-point under the heading "*Other implications of viewing data protection as a fundamental right* (the principles of legality, legitimate purpose, necessity and proportionality) and the discussion of "*General restrictions*" in section 2.3.1.1 on General substantive requirements for adequacy; more specifically, the application of these principles to data retention in the CJEU judgments in *Digital Rights Ireland* (see in particular para. 52, quoted on p. 34, above) and in *Tele-2/Watson* (see in particular para. 109, quoted on p. 35, above); the application of these principles by the CJEU to access to data by third country intelligence agencies in *Schrems II* (see in particular paras. 174 – 176, quoted on p. 40, above); and the application of these principles to surveillance by Council of Europe Member States by the ECtHR in *Big Brother Watch* (see in particular para. 332, referenced on p. 45, above).

Assessment: The US laws described in section 3.2, above, do not meet the European standards that the legal rules on surveillance must be accessible (i.e., published), legally binding, clear, precise and "foreseeable" in their application.

See section 3.2.2, above, on *"Secret law"*.

The laws (in particular FISA) do not require surveillance measures to serve a "legitimate purpose" in a democratic society: they allow, e.g., espionage for political or economic purposes.

See the definition of "foreign intelligence information" in FISA § 1801, para. (e), discussed in section 3.2.1, above, and the reference there (and in footnote 77) to political espionage.

They do not in themselves define the scope and application of the relevant surveillance measures – but rather, leave many matters to executive discretion. Nor do they require that any specific measures imposed in a specific context be "necessary" and "proportionate" to such a purpose (or even to the purpose of safeguarding national security where that is the purpose).

Cf. Section 4 of Presidential Policy Directive 28, quoted on p. 84, above, which (as we note) mentions "principles familiar from the GDPR", but leaves the application of those principles to executive officials.

European standard: All surveillance measures and actions must be subject to effective, independent and impartial judicial oversight

See in general section 2.3.1.2, above, General procedural requirements for adequacy and in relation to state surveillance section 2.3.1.3, the section on *The issue of procedural/enforcement guarantees*; more specifically, the application of these principles by the CJEU to access to data by third country intelligence agencies in *Schrems I* and *II* (see in particular *Schrems I*, para. 89, quoted on p. 39, above, the requirements in this regard, set out in the EDPB's Adequacy Referential, paraphrased on p. 42, above, and the quotes from the *Schrems II* judgment, paras. 181 – 182 and 197, quoted on p. 43, above); and the application of these principles to surveillance by Council of Europe Member States by the ECtHR in *Big Brother Watch* (see in particular the requirements of "procedures and modalities for supervision by an independent authority" and "independent ex post facto review" in the list of ECHR requirements for surveillance, quoted on p. 46, above).

Assessment: The lack of such oversight was one of the main reasons for the CJEU to invalidate the Privacy Shield decision.

See *Schrems I*, paras. 181 – 182 and 197, quoted on p. 43, above.

EU standard: Individuals must have access to effective remedies

See the general discussion of *The issue of procedural/enforcement guarantees* in section 2.3.1.3, Requirements relating to access to personal data by third country authorities, above; more specifically, point D ("*Effective remedies need to be available to the individual*") in the EDPB's European Essential Guarantees for surveillance, quoted on p. 42, above.

Assessment: The absence of an effective remedial body that meets the EU Charter requirements (Article 47 CFR) was another main reason for the CJEU to invalidate the Privacy Shield decision. As the Congressional Research Service noted, "Like E.O. 12333, PPD-28 does not purport to provide judicially enforceable rights for private persons who may have been subject to surveillance in violation of the directive's provisions… An electronic communication service provider may challenge a government directive, in which case the [Foreign Intelligence Surveillance Court] reviews the directive to determine whether it complies with Section 702. Additionally, if the government elects to use evidence derived from Section 702 surveillance against an individual in a criminal prosecution or other enforcement action, the defendant must generally be given notice that such surveillance occurred, and a court may review the legality of the surveillance in that context. However, absent these circumstances, there is generally no opportunity for targets of surveillance to know whether their communications or information have been acquired by the government under Section 702, and as a result, fewer opportunities may exist to seek judicial review of that acquisition."

CJEU, *Schrems II* judgment, paras. 181 – 182, quoted on p. 43, above.

EU standard: There must be suitable and specific safeguards to protect individuals from being unduly profiled or subject to fully automated decisions

See in general section 2.3.1.1, General substantive requirements for adequacy, under the heading *Data subject rights* (last bullet-point).

Assessment: There are no serious protections of this kind in US surveillance laws – especially not in relation to non-"US persons".

EU standard: There must be safeguards to ensure that onward transfers of data (as in data sharing between intelligence agencies of different countries) do not undermine the protection to be accorded under EU law

See section 2.3.1.1, above, on General substantive requirements for adequacy, under the heading "*Restrictions on onward transfers*"; and the application of the principles to onward transfers of intelligence material by the ECtHR in *Big Brother Watch* (see in particular para. 395, quoted on p. 49, above). The issue was not (yet) addressed in the EDPB's European Essential Guarantees for surveillance,[181] but of course the principles on onward transfer set out in the GDPR – or in relation to law enforcement data, the LED – fully apply. Under these, recipients of personal data transferred from the EU must ensure that when those data are further ("onwardly") transferred, they will retain the same, "essentially equivalent" protection they were accorded under these EU data protection instruments.

Assessment: There are no serious protections of this kind in the US surveillance laws (and the stipulations in the UK – USA Agreement, noted by the ECtHR in its *Big Brother Watch* judgment, are extremely limited and fall far short of the EU data protection law requirements).

[181] See European Essential Guarantees for surveillance (footnote 61), footnote 24.

See the discussion of the UK – USA Agreement in section 2.3.1.3, above, Requirements relating to access to personal data by third country authorities, in particular the sub-section on *ECtHR and national constitutional requirements relating to direct access to personal data by EU Member States' intelligence agencies* and para. 395, quoted on p. 49, above.

Overall assessment: It is clear US surveillance laws manifestly fail to meet the standards adduced in the case-law of the European Court of Human Rights and the Court of Justice of the EU, as reflected in the European Data Protection Board's European Essential Guarantees for surveillance.

3.2.4 Proposals for reform

Academic proposals for legal reform have focused on the two key findings of the CJEU in *Schrems II* in relation to US national security access to transferred EU personal data: the need to **provide EU data subjects with effective judicial redress**, and to ensure access to data is **necessary and proportionate**. US academics have also identified an important **rule of law** issue: parts of key presidential orders (and even whether they are being followed), and the legal interpretation of the government's national security powers, are not available to the public in their totality.

Effective judicial redress

Prof. Peter Swire (a former White House adviser) suggests effective redress requires two stages: a fact-finding investigation, followed if required by judicial review in the Foreign Intelligence Surveillance Court (FISC).[182] Swire's proposal has been further analysed by Christopher Docksey, formerly head of the European Data Protection Supervisor secretariat and currently a member of Guernsey's data protection authority.[183]

Swire has proposed investigations could be conducted by existing Privacy and Civil Liberties Officers (PCLOs) within the US intelligence agencies, which were established by statute in 2007; existing agency Inspectors General; or the independent Privacy and Civil Liberties Oversight Board (PCLOB), whose members are confirmed by the US Senate. Docksey suggests PCLOs play a role closer to the GDPR's Data Protection Officers, and could refer complaints to the Inspectors General, *if* the independence of the IGs could be strengthened by statute (not least as several were removed arbitrarily by former president Donald Trump, including that of the intelligence community following his determination a whistleblower's complaint about the president's dealings with Ukraine was credible.[184])

Following a complaint by an EU data subject, the investigation would determine whether US legal requirements had been followed (including any specific additional protections agreed between the US and EU, such as notice requirements). The report to the claimant (or a representative data protection authority) would be either no violation had occurred; or a violation had been remedied. Such investigations could take place based simply on a legally-binding memorandum of understanding between PCLOB and an executive branch agency, although this would require significantly greater resourcing of PCLOB.

---

[182] Peter Swire, *Appendix 1 to U.S. Senate Commerce Committee Testimony on "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows"*, 9 December 2020, at: https://peterswire.net/wp-content/uploads/Appendix-1-to-Swire-Senate-Testimony-Individual-Redress.final-as-submitted.pdf

[183] Christopher Docksey, *Schrems II and Individual Redress—Where There's a Will, There's a Way*, Lawfare, 12 October 2020, at: https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way

[184] Melissa Quinn, *The internal watchdogs Trump has fired or replaced*, CBS News, 19 May 2020, at: https://www.cbsnews.com/news/trump-inspectors-general-internal-watchdogs-fired-list/

Swire suggests statutory reform would allow a complainant to obtain judicial review by the FISC (established in the US judicial branch), with the complainant given standing to "assess whether the agency has properly discharged its statutory duties." Such a reform would have to successfully navigate recent Supreme Court jurisprudence focusing on "physical, monetary, or cognizable intangible harm traditionally recognized as providing a basis for a lawsuit in American courts" as a basis for standing.[185] The American Civil Liberties Union (ACLU) and Center for Democracy and Technology (CDT, a US non-profit) have suggested Congress defines the protective measures an individual takes to avoid surveillance as a well-established, concrete diversion of time or resources as the required "injury".[186]

An appointed "friend of the court", with full access to classified information, could brief the court on "legal arguments that advance the protection of individual privacy and civil liberties." FISC decisions may be appealed to the Foreign Intelligence Surveillance Court of Review and the US Supreme Court. Docksey adds it would also be possible for the PCLOB to provide individual redress, with legal reforms to provide for its "independence and the power to impose binding decisions", with decisions appealed to the FISC.

The Open Technology Institute (a project of US think-tank New America) has also reviewed Swire's proposals, and emphasised Congressional action will be required to meet the CJEU's standards of binding decisions and impartial review by the Foreign Intelligence Surveillance Court (rather than executive branch officials or agencies), including broadening the FISC's jurisdiction and creating court "standing" for complainants.[187]

CDT has suggested similar reforms, noting in particular "U.S. courts, including the FISA Court, are the only existing mechanisms in the U.S. that could have the attributes and authorities that the CJEU deemed necessary to an adequate redress mechanism"; legislative reform would be needed to "to give the FISA Court the authority it would need to receive and act upon complaints of unlawful surveillance", including given affected European data subjects standing and enabling public hearings.[188]

Ensuring necessity and proportionality

Less academic research has taken place on updating the US legal framework to ensure surveillance is necessary and proportionate, the second main *Schrems II* criterion. Swire has catalogued the (relatively

[185] *TransUnion LLC v. Ramirez*, US Supreme Court, case no. 20–297, 25 June 2021, p.12, at: https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf

[186] American Civil Liberties Union, *RE: The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows*, Letter to US Senate Committee on Commerce, Science and Transportation Chairman and Ranking Member, 9 December 2020, pp.4—6, at: https://www.aclu.org/sites/default/files/field_document/2020-12-8_aclu_statement_for_the_record_senate_commerce_committee_hearing_on_privacy_shield.pdf

CDT, *Schrems II and the Need for Intelligence Surveillance Reform*, 13 January 2021, p.4, at: https://cdt.org/wp-content/uploads/2021/01/2021-01-13-CDT-Schrems-II-and-Intelligence-Surveillance-Reform-in-the-US.pdf

[187] Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman, & Spandana Singh, *Strengthening Surveillance Safeguards After Schrems II: A Roadmap for Reform*, Open Technology Institute, April 2021, pp.24-26, at: https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/

[188] CDT, footnote 186.

minor) changes that have taken place since his expert witness report for the Irish High Court case referred to the CJEU that led to the judgment.[189]

The Open Technology Institute (in a report co-authored by a former executive director of the US Privacy and Civil Liberties Oversight Board) has recommended non-legislative measures such as narrowing FISA s.702 and E.O. 12333 collection, targeting and use practices, as well as increased transparency, which are possible purely by executive action and "should be achievable in the near term."[190] Specifically, it suggests:

1. extending the six categories of "use" limits on bulk-collected signals intelligence in E.O. 12333 to bulk *collection* of data, which is currently permitted for any foreign intelligence purpose;
2. adopting binding rules to ensure bulk collection is only conducted when it meets tests of necessity and proportionality – already partly adopted in the Department of Defense's Attorney General-approved signals intelligence guidelines[191] under E.O. 12333;
3. narrowing the definition of foreign intelligence information (which under E.O. 12333 covers information relating to the activities of "any foreign person", and under FISA s.702 is within the scope of topics "certified" by the Foreign Intelligence Surveillance Court);
4. setting stronger standards to justify surveillance targets under FISA s.702, applying the definition applicable to US rather than foreign persons ("necessary to" rather than "relates to" the US' ability to protect against threats), narrowing the "reasonably likely to return" test, and permanently blocking collection of information "about" a target rather than communications specifically "from" or "to" a target;
5. requiring the Foreign Intelligence Surveillance Court to review post hoc the necessity and proportionality of FISA s.702 and E.O. 12333 targeting decisions (NSA analysts must now record a "targeting rationale" for selectors, to "memorialize why the analyst is requesting targeting, and provides a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked."[192] These are reviewed by intelligence oversight attorneys in the Department of Justice, who must report any violations of targeting procedures to the FISC[193]);
6. extending the requirement for agencies participating in FISA s.702 and E.O. 12333 to provide a statement of facts when querying intelligence databases for information about specific US persons to any specific person regardless of nationality or location;
7. reducing the default retention period for information collected under s.702 and E.O. 12333 from five years in most circumstances to three years (which would still allow indefinite retention of data assessed as constituting foreign intelligence information), and narrowing

[189] Peter Swire, *Updates to U.S. Foreign Intelligence Law Since 2016 Testimony*, Appendix 2 to U.S. Senate Commerce Committee Testimony on "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows", 9 December 2020, at: https://peterswire.net/wp-content/uploads/Appendix-2-to-Swire-Senate-Testimony.final-as-submitted-002.pdf

[190] See footnote 187, p.4.

[191] Unclassified version of *Signals Intelligence Annex to DoD Manual S-5240.01-A*, 7 January 2021, ss. 2(2)(a)(2) ("Will conduct targeted collection using selection terms whenever practicable, but may use other discriminants or conduct bulk collection when necessary due to technical or operational considerations" and 2(3)(a) (collection limitation and filtering "as soon as practicable after collection"). At:

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/S-524001-A.PDF?ver=SPh6FZicXc8uH192MI8o3w%3d%3d&timestamp=1610651794685

[192] Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the FISA, Submitted to the FISC by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, October 2018, p. A-6, at:

https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

[193] US government, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, footnote 111, p.8-9.

exceptions, while requiring the deletion of information assessed as *not* foreign intelligence; and

8. increasing transparency relating to US surveillance, in particular allowing technology and telecommunications companies to publish more data about legal demands they receive from the government, and making public the certifications approved by the Foreign Intelligence Surveillance Court.

The US administration can make changes to E.O. 12333 by amending/updating the order, while changes to FISA s.702 procedures could be approved and made binding by the Foreign Intelligence Surveillance Court, then codified by Congress.

The ACLU has suggested similar, and in some cases broader, legal reforms to Congress. It recommends FISA s.702 should require a reasonable suspicion targets are "foreign powers" or "agents of a foreign power" outside the US; FISA and E.O. 12333 definitions of "foreign intelligence" be narrowed; E.O. 12333 bulk collection be prohibited, with surveillance limited to specific targets; the Foreign Intelligence Surveillance Court should review targeting decisions on an ex post basis; limiting the default retention period of surveillance data to three years, with narrow exceptions for a subset of "foreign intelligence"; giving individuals standing to bring legal complaints; and requiring delayed notification of targets of foreign intelligence surveillance.[194] The Center for Democracy and Technology also recommended many of these measures, as well as a specific prohibition on "using Section 702 to collect foreign intelligence information for the purpose of burdening dissent or for disadvantaging people based on their ethnicity, race, gender, sexual orientation or religion."[195]

Making "secret law" public

In a 2016 review which included input from the US Department of Justice, Gotein suggested the following measures[196] to reduce the amount of "secret law", which determines important aspects of US government surveillance practices:

- requiring the approval of a US government inter-agency panel before withholding from publication an authoritative legal interpretation or requirement affecting the public;
- basing such a withholding only on a documented assessment disclosure is highly likely to directly or indirectly result in loss of life, serious bodily harm, or significant economic or property damage;
- banning certain categories of "secret law", such as pure legal analysis, imposing affirmative duties or criminal penalties on members of the public, or legal interpretations that attempt to free the executive branch from the constraints of statutory law or stretch its meaning;
- withheld rules or authoritative interpretations should be provided to members of Congress for review, and to courts where the government is party to relevant litigation, as well as oversight bodies such as Inspectors General and the Privacy and Civil Liberties Oversight Board;
- a sunset period (such as four years) for the withholding, and a higher standard for it to be renewed, along with a limit of renewals (such as two); and

[194] ACLU, footnote 186.

[195] Footnote 188, p.7.

[196] Footnote 174, p.63—69.

- a public index of secret laws, which would enable members of the public to make Freedom of Information Act requests and if necessary, obtain judicial review of the decision to withhold the law.

- o – o – o -

4 ANALYSIS AND RECOMMENDATIONS

KEY FINDINGS

Our analysis shows that no US federal or state privacy law is likely to provide "essentially equivalent" protection compared to the EU GDPR in the foreseeable future. Indeed, there are serious and in practice insurmountable US constitutional and institutional as well as practical/political obstacles to the adoption of such laws.

The EU should immediately identify stop-gap measures such as audits, logs and reporting mechanisms that can possibly be used to allow some transfers of non-sensitive data – but also identify categories of data (and/or of controllers and processors or contexts) in relation to which these will not suffice. The European Parliament should ask the EDPB to address these matters in yet further guidance on EU–US data transfers, drawing on the work of the Commission in relation to the Digital Services Act and the Digital Markets Act.

In the medium term, legal academics and civil society groups are clear federal surveillance legislative reform will be required to provide EU data subjects with "**an effective remedy before…an independent and impartial tribunal**" relating to personal data transferred to the US, as required by the Charter of Fundamental Rights. Complainants would need standing to obtain judicial review from the Foreign Intelligence Surveillance Court.

Presidential action and legislative reform will also be required to ensure the **necessity and proportionality of US surveillance** of data transferred under any adequacy finding. US civil society groups have recommended limiting bulk collection; narrowing the definition of foreign intelligence information and setting stronger standards to justify surveillance targets; reducing the default retention period for collected information from five years to three; and increasing transparency about surveillance activities.

Finally, reform of the FTC Act will be required to enable effective enforcement of self-certified compliance by US data controllers with the full GDPR, including strengthening rights of private action.

If (i) the US and the EU were to take the legislative steps we outline relating to substance, enforcement and individuals' rights of action **and** (ii) the US were to reform its surveillance laws and practices, ***then*** **a new EU-US arrangement for self-certification by US entities could be achieved**. Without these reforms, EU data protection authorities will be required to consider suspending transfers of personal data to the US even following an adequacy decision by the European Commission.

The EU institutions should stand up for the rule of law and demand both the Member States and third countries bring their intelligence practices and domestic law frameworks fully in line with international human rights law. A pragmatic starting point would be the development and ratification of **a "minilateral" treaty covering intelligence activities of, in particular, the 30 EU/EEA states and the "Five Eyes" countries (USA, UK, Australia, Canada and New Zealand)**. While full ratification might take several years, these states should much sooner come to an informal agreement against "spying on allies".

4.1 Introduction

In this chapter, we will first analyse whether US privacy law in any shape or form, or voluntary arrangements, can be held to provide (or be made to provide) "essentially equivalent" protection to the EU GDPR; then whether the issue of access by US authorities (in particular, the US intelligence[197] agencies) to personal data transferred from the EU to the USA (or directly accessed in the EU by those agencies) can be resolved in a way that meets the CJEU *Schrems II* and EDPB EEGs requirements.

4.2 Analysis of US privacy laws

4.2.1 Substantive issues to address

In section 3.1 we showed that privacy law in the USA is a patchwork of federal constitutional and common law, sectoral federal privacy laws and state laws, with the California laws being the most advanced – while still not meeting all the EU standards. These various laws all moreover operate in a thicket of other laws and requirements, such as data breach notification duties.

Although there are several broad federal privacy bills pending (as noted in section 3.1.3), the US Congressional Research Service stresses that there are major obstacles to the enactment of such broad laws, and:[198]

> some elements of the data protection proposals and models could implicate legal concerns and constitutional limitations… [There are both] legal issues related to the internal structure and definition of data protection-related rights and obligations and…external legal constraints.

These include the definition and scope of protected data, the issue of "pre-emption" (i.e., "how to balance whatever federal program is enacted with the programs and policies in the states") and "First Amendment" issues (i.e., the relationship and balance between privacy rights and freedom of expression).[199] **It follows that it will be difficult (if not impossible) to enact any broad federal privacy law that can "essentially" meet the substantive requirements of EU law and impose those standards on US corporations.**

In section 3.1.3, we also noted that the (since invalidated) EU – US Safe Harbour and Privacy Shield agreements were attempts to overcome some of these issues and constraints, by setting out many detailed principles and rules that were supposed to reflect EU data protection law in the relevant documentation, with US companies then being able to self-certify that they would abide by them – which then gave the FTC the right to sanction them if they did not abide by those relatively detailed (EU data protection law-reflecting) stipulations and promises.

This was undoubtedly ingenious, even to some extent elegant. By making participation in the arrangements voluntary, it avoided many pitfalls of US law (such as First Amendment issues relating to statutory proscriptions on using information, or the issue of pre-emption). However, there are still difficulties in this regard, from both a European and US perspective. The European Parliament:[200]

---

[197] Presidential Policy Directive – Signals Intelligence Activities, 17 January 2014, at: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[198] US CRS *Data Protection Report* (footnote 111), p. 55.

[199] *Idem*, see the sections on "*Defining Protected Information and Addressing Statutory Overlap*" (pp. 56–57), "*Preemption*" (pp. 62–63), and "*First Amendment*" (pp. 64–69).

[200] Footnote 28 §28.

> [c]onsiders that any future adequacy decision by the Commission should not rely on a system of self-certification, as was the case with both Safe Harbour and the Privacy Shield.

The Article 29 Working Party was also critical of the self-regulatory regimes – but neither it nor the CJEU completely dismissed the very concept. The WP29 said the following in its opinion on the (then draft) EU Commission decision on the adequacy of the Privacy Shield:[201]

> [T]he WP29 considers that some key data protection principles as outlined in European law are not reflected in the draft adequacy decision and the annexes, or have been inadequately substituted by alternative notions.
>
> For instance, the data retention principle is not expressly mentioned and cannot be clearly construed from the current wording of the Data Integrity and Purpose Limitation principle. Furthermore, there is no wording on the protection that should be afforded against automated individual decisions based solely on automated processing. The application of the purpose limitation principle to the data processing is also unclear. In order to bring more clarity in the use of several important notions, the WP29 suggests that clear definitions should be agreed between the EU and the U.S and be part of a glossary of terms to be included in the Privacy Shield F.A.Q.

The Article 29 Working Party also found that the issue of "onward transfers" was insufficiently addressed; that:[202]

> the new redress mechanism in practice may prove to be too complex, difficult to use for EU individuals and therefore ineffective;

and more generally noted:[203]

> The fact that the principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes makes the information both difficult to find, and at times, inconsistent. This contributes to an overall lack of clarity regarding the new framework as well as making accessibility for data subjects, organisations, and data protection authorities more difficult;

and that:[204]

> [s]imilarly, the language used lacks clarity.

However, the Article 29 Working Party clearly did not object to the structure of the arrangement itself – and the CJEU also did not hold, in either of its *Schrems* judgments, that adequacy could not be ensured through such a structure. On the contrary, it expressly held that:[205]

> recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 [now Article 45(1) GDPR] that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments' –

although it stressed, in that same sentence, that:

> the reliability of such a system, in the light of that requirement [i.e., self-certification], is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to

---

[201] Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (WP238), adopted on 13 April 2016, p. 3.

[202] *Idem*.

[203] *Idem*, p. 2.

[204] *Idem*.

[205] CJEU *Schrems I* judgment (footnote 1), para. 81.

> respect for private life and the right to protection of personal data, to be identified and punished in practice.

Moreover, in relation to the Safe Harbour agreement, it found that the Commission decision approving that agreement (Decision 2000/520) did not:[206]

> contain[ ] sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive [now Article 45 GDPR], by reason of its domestic law or its international commitments.

In principle, none of the above deficiencies in the substantive protections offered by the Safe Harbour and Privacy Shield arrangements are beyond remedy – although they are quite serious and the changes that would have to be made are considerable. In the next sub-section, we note that the same applies to the procedural/enforcement and remedies issues. In other words, we believe that – subject to one major caveat – the deficiencies in terms of general adequacy are not insurmountable. In sub-section 4.2.3, below, we suggest how they could be overcome. However, they cannot overcome the surveillance issues, which we discuss thereafter, in section 4.3. We bring are analyses in these two respects – general adequacy and access to data/surveillance – together in section 4.4, where we also set out our recommendations.

4.2.2 Procedural and remedial issues to address

From a European perspective, the issues of **enforcement** by a supervisory body and the **remedies** available to individuals are of particular importance. These are discussed in the US CRS report in two sections on "*Agency Enforcement*" and "*Private Rights of Action and Standing*".[207]

On the first issue, we should note the limitations on relying on the FTC as supervisory authority. As the CRS notes:[208]

> the FTC is often viewed—by industry representatives, privacy advocates, and FTC commissioners themselves—as the appropriate primary enforcer of any future national data protection legislation, given its significant privacy experience.
>
> There are, however, several relevant legal constraints on the FTC's enforcement authority. First, the FTC generally lacks the ability to issue fines for first-time offenses. In UDAP ["unfair or deceptive act or practice"] enforcement actions, the FTC may issue civil penalties only in certain limited circumstances, such as when a person violates a consent decree or a cease and desist order. Consequently, the FTC often enters into consent decrees addressing a broad range of conduct, such as a company's data security practices, seeking penalties for violations of those decrees. However, as the *LabMD* case[209] … suggests, if the FTC imposes penalties based on imprecise legal standards provided in a rule or order, the Due Process Clause of the Fifth Amendment may constrain the agency's authority. Second, the plain text of the FTC Act deprives the FTC of jurisdiction over several categories of entities, including banks, common carriers, and nonprofits. Third, the FTC generally lacks authority to issue rules under the APA [Administrative Procedure Act]'s notice-and-comment process that is typically used by agencies to issue regulations. Rather, the FTC must use a more burdensome—and, consequently, rarely used—process under the Magnuson-Moss Warranty Act.

---

[206] *Idem*, para. 83.

[207] On pp. 57 – 58 and 59 – 62, respectively.

[208] US CRS *Data Protection Report* (footnote 111), p. 57, footnotes omitted, but one footnote (footnote 543) in the report has been inserted into the quote as the third paragraph; this is indicated by the use of square brackets around that paragraph.

[209] *LabMD v. FTC*, 894 F.3d 1221.

> [In addition to these legal constraints, the Third Circuit recently held that FTC may not bring civil litigation based on past UDAP violations that are not ongoing or about to occur. *Shire ViroPharma*, 2019 WL 908577, at *9 ("In short, we reject the FTC's contention that Section 13(b)'s 'is violating' or 'is about to violate' language can be satisfied by showing a violation in the distant past and a vague and generalized likelihood of recurrent conduct. Instead, 'is' or 'is about to violate' means what it says—the FTC must make a showing that a defendant is violating or is about to violate the law."). This holding may limit the FTC's ability to bring actions in federal court based on past UDAP violations.[210]]
>
> As some FTC Commissioners and commentators have noted, these legal limitations may be significant in determining the appropriate federal enforcement provisions in any national data security legislation. While Congress may not be able to legislate around constitutional constraints, future legislation could address some of these limitations—for instance, by allowing the FTC to seek penalties for first-time violations of rules, expanding its jurisdictions to include currently excluded entities, or providing the FTC notice-and-comment rulemaking authority under the APA. These current legal constraints on FTC authority may also be relevant in determining whether national legislation should allow private causes of action or enforcement authority for state attorneys general, as some commentators have suggested that private causes of action and enforcement by state attorneys general are essential supplements to FTC enforcement.

Recent US Supreme Court jurisprudence in *AMG Capital Management, LLC v. Federal Trade Commission*[211] has also limited the scope of Section 13(b) of the FTC Act and the ability to obtain streamlined financial recourse for consumers through the courts.

Additionally, certain categories of privacy and security promises as they directly impact physical safety of persons may be deemed to more appropriately fall within joint or lone oversight of the Consumer Product Safety Commission, the Food and Drug Administration, and other similar sector-specific regulators. Similarly, material misrepresentations by publicly traded companies to investors in offering materials and periodic reports fall under the jurisdiction of the Securities and Exchange Commission. Memoranda of Understanding are creating shared enforcement teams across these agencies.

For the FTC to become an effective supervisory authority on the lines of the EU ones, even – or perhaps especially – in relation to any arrangement that is built on "voluntary self-certification", the FTC Act would likely have to be expanded or a new statute passed on the lines suggested. Additionally, new or expanded Memoranda of Understanding should be signed among multiple US agencies, creating shared, coordinating enforcement teams.

The FTC currently devotes limited resources to privacy enforcement. Hoofnagle noted:

> The Agency is also limited in resources. The FTC's budget is only $300 million. Consider that the Food and Drug Administration's budget is over $4 billion and the newly created Consumer Financial Protection Bureau's is over $400 million. Almost half of the FTC's budget is devoted to competition matters. The FTC's Bureau of Consumer Protection is modest in size (about 638 employees), and just a fraction of its staff handle privacy matters (the FTC estimates 57 employees).[212]

On the issue of access by individuals to judicial remedies, the CRS report makes clear that, because of the limits of the federal courts' "judicial power" under Article III of the US Constitution, "Congress

[210] For further discussion of this case, see note 327 [in the CRS report].

[211] Decided 22 April 2021, Docket no. 19-508.

[212] Chris J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge University Press, 2016, p. 335.

cannot elevate every privacy violation to the status of a concrete injury".[213] The CRS report concludes, with reference to a relatively recent case, that:[214]

> Congress can possibly resolve some of these disputes by elevating some otherwise intangible injuries to concrete status. But *Spokeo* illustrates that there may be a residuum of harmless privacy violations for which Congress cannot provide a judicial remedy.

This "residuum of harmless privacy violations for which Congress cannot provide a judicial remedy" appears to have been widened – and the category of individuals with standing correspondingly narrowed – in the recent US Supreme Court (USCC) opinion in *TransUnion LLC v. Ramirez*, in which the Court held that:[215]

> To have Article III standing to sue in federal court, plaintiffs must demonstrate, among other things, that they suffered a concrete harm. No concrete harm, no standing. Central to assessing concreteness is whether the asserted harm has a "close relationship" to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including (as relevant here) reputational harm.

However, we note that in the EU, there are also different views on the scope of the right to compensation under Article 82 GDPR, at least when it comes to compensation for non-material damage.[216] The differences between the USSC's view and the approach to Article 82 GDPR (at least in some EU Member States) may not be all that large.

In other words, it may not be possible to provide a right of action for individuals that is quite as broad as that envisaged in the EU GDPR. However, Congress could (in amending the FTC Act or in some other law), nevertheless still significantly strengthen the right of action – and standing – of individuals, *including non-US persons*, who are significantly affected by privacy-related "unfair or deceptive acts of practices" (UDAP) committed by US private entities.

In that respect, one aspect of US law should be noted that clearly offers remedies beyond what is offered in the GDPR: genuine class actions.

The GDPR requires the EU Member States to provided data subjects with the right to be "represented" by a not-for-profit body in the lodging of complaints, the seeking of a remedy against non-action by a supervisory authority, or against a controller or processor (Article 80, read together with Article 77, 78 and 79). However, Member States are left free to decide whether to allow such representation in relation to the exercise of the right to compensation under Article 82 (Article 80(1), final sub-sentence) and whether to allow such bodies to lodge complaints to their supervisory authorities generally (Article 80(2)).

Given the often very poor enforcement of the GDPR by some EU Member States' supervisory authorities, this is a major weakness – we would call it a major deficiency – in EU law.

By contrast, US law often allows for much broader and stronger class action suits. Thus, under the California CPRA, individuals can join class actions in which statutory damages of $100–$750 are payable for "each violation" – i.e., in relation to each person affected. When many people are affected (as is too

---

[213] *CRS Report* p. 61, with reference to the Supreme Court case *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016).

[214] *Idem*, p. 62.

[215] *TransUnion LLC v. Sergia L. Ramirez*, US Supreme Court No. 20-297, 25 June 2021, 594 U.S.___(2021), available at: https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf

[216] For a detailed discussion, see the commentary on Article 82, Right to compensation and liability, by Gabriela Zanfir-Fortuna in Kuner *et al*., *The EU General Data Protection Regulation – A Commentary* (footnote 41, above).

often the case in particular but not only in relation to data breaches), this can easily accumulate: if, say, information on 20,000 customers was lost, the damages could be $2–15 million.[217] **In this respect, US law may provide individuals with greater and stronger protection than is accorded under the GDPR, which relies too much on effective enforcement by the Member States' supervisory authorities (which is often not forthcoming) – and we believe the EU should seek to emulate that US level of protection.** We discuss this too in the next sub-section.

4.2.3 Proposed institutional, substantive and procedural reforms in relation to general adequacy

Given that (as we concluded at 4.2.1) it will be difficult (if not impossible) to enact any broad US federal privacy law that can meet the substantive requirements of EU law and impose those standards on US corporations, the basic idea of relying on voluntary self-certification by US corporations of compliance with EU level standards, with enforcement if they fail to adhere to their promises, remains the best way forward.

However, any arrangement on that basis would have to be very different from the (rightly invalidated) Safe Harbour and Privacy Shield arrangements – and would require legislative steps by the US (and, we suggest, in one respect by the EU) in relation to substance, enforcement and individuals' rights of action. (And of course the issue of undue access to data by US authorities also needs to be addressed.)

Substance

The deficiencies in the Safe Harbour and Privacy Shield arrangements, noted by the WP29, would have to be remedied. In particular, the substantive data protection requirements should be spelled out in clear and unambiguous language (rather than in the unclear, ambiguous and almost impossible to even determine specifications in a range of documents, letters, FAQs, etc., that were used in the old arrangements).

The simplest way to ensure that any self-certification would relate to compliance with substantive standards that are "essentially equivalent" to the EU GDPR ones, would be to simply make self-certification refer to those standards:

> "We, [US corporation XYZ] hereby certify that we will comply with all the requirements in the following sections of the EU General Data Protection Regulation, as interpreted and applied by the Court of Justice of the European Union, and with the guidance on the GDPR issued by the European Data Protection Board, in relation to all personal data on all data subjects whose data we process (with the terms "personal data", "data subjects" and "process[ing]" applied as defined in the GDPR):
>
> [Add references to applicable sections of the GDPR (essentially all substantive provisions)]"

Given that this is supposed to be an entirely free and voluntary act, by which US corporations themselves decide to be bound by certain requirements – *in casu*, the requirements of the EU GDPR – (or not) we cannot see why complex attempts would have to be made to try and spell out the requirements in separate, complex documentation that would inevitably differ, or over time come to differ, from the EU GDPR (and that in the case of the Safe Harbour and the Privacy Shield were meant to only partially be fully in line with the EU standards).

[217] See footnote 164.

Enforcement

The idea of enforcing compliance with voluntary self-certification under the US FTC Act through the system of sanctions against unfair or deceptive acts or practices (UDAP) is in principle sound (and, as we have noted, acceptable to the CJEU and the EDPB). However, as the US Congressional Research Service Data Protection Report makes clear, the FTC is currently not properly equipped to fulfil this role. As that report suggests, the deficiencies could to a large extent be remedied by the following:

- granting the FTC the power to seek penalties (such as fines) for any violations of the (voluntarily accepted) substantive GDPR requirements, including for first-time violations and past violations (at least to the extent that the GDPR requirements are sufficiently clear and precise to meet the Due Process Clause of the Fifth Amendment);
- allowing entities that are not as such covered by the FTCA (such as financial institutions and health providers) to also voluntarily self-certify compliance with the GDPR substantive standards, and expanding the FTC jurisdiction so it can also impose sanctions on such (otherwise not covered) self-certifying entities if they fail to adhere to their self-made promises; (Although the US banks in particular have fought fiercely – and so far successfully – against being made subject to any new privacy rules other than the GLBA, they and other currently not covered entities could in our view not really object to an entirely free option of such voluntary self-certification);
- giving the FTC the power to issue "trade regulation rules" (TRRs) under the US Administrative Procedure Act's notice-and-comment process rather than the more burdensome—and, consequently, rarely used—process under the Magnuson-Moss Warranty Act; such rules could, where necessary, expand on the substantive requirements of the GDPR where these may be too imprecise to meet the Due Process Clause; and
- giving the FTC the right to cooperate formally with the European Data Protection Board in clarifying and enforcing the GDPR standards, in particular in relation to US entities (cf. Article 50 GDPR on International cooperation for the protection of personal data).

Individuals' rights of action

Currently, as noted in section 3.1.3, the FTC Act does not provide a private right of action – but of course, rights of action are provided for in numerous US federal and state laws. The CPRA, for instance, expands the right of action that was already in the CCPA, albeit only in relation to personal data breaches, not in relation to any violation of the Acts. As explained in the previous sub-section, while "Congress cannot elevate every privacy violation to the status of a concrete injury", Congress "can possibly … elevat[e] some otherwise intangible injuries to concrete status." This limitation arises partially from First Amendment constraints.

As we concluded in the previous sub-section: it may not be possible to provide a right of action for individuals that is quite as broad as that envisaged in the EU GDPR. However, Congress could (in amending the FTC Act or in some other law), nevertheless still significantly strengthen the right of action – and standing – of individuals, *including non-US persons*, who are significantly affected by privacy-related "unfair or deceptive acts of practices" (UDAP) committed by US private entities.

Indeed, as also noted there, in this respect, US law provides individuals with greater and stronger protection than is accorded under the GDPR.

In our view, it would be a positive *quid pro quo* if the EU were to offer the US (and the rest of the world) the introduction of a genuine "American-style" class action remedy in relation to any violations of the

GDPR, in which anyone affected by such a violation (whatever their nationality, status or place of resident) could join actions initiated by not-for-profit groups (or law firms). That would show that it is not just the EU making "demands" of third countries in relation to data protection, but that, rather, the EU is also willing to raise its standards to those of such other countries in aspects of the legal regime under which those other countries provide the better, higher levels of protection.

We believe that if the US and the EU were to take the above legislative steps, a new EU-US arrangement for self-certification by US entities could be achieved, under which the EU could issue a new positive adequacy decision on the USA, limited to personal data transferred from the EU to entities that had self-certified their voluntary compliance with the EU GDPR substantive standards. However, the reforms we suggest above are the absolute minimum necessary if the US is to achieve adequacy in EU data protection terms. And of course, that is without taking into account the other main issue we address in this study: access to data by the US authorities. We will turn to this now.

4.3 Analysis of US surveillance laws

4.3.1 Substantive issues to address

In its *Schrems II* judgment, as discussed above in section 2, the Court of Justice was clear: "Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes". Nor does PPD-28, or E.O. 12333, "confer rights which are enforceable against the US authorities in the courts". PPD-28 also allows '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection', which does not "delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data." Finally, the Privacy Shield Ombudsperson appointed by and reporting directly to the US Secretary of State is insufficiently independent from the executive, and lacks "the power to adopt decisions that are binding on [US] intelligence services".[218]

4.3.2 Proposed institutional, substantive and procedural reforms in relation to surveillance

As we discuss in detail in section 3.2.4, some consensus appears to be developing in academic and civil society analysis of the US surveillance law reforms required to provide "essentially equivalent" protection to EU data subjects, particularly in terms of effective judicial remedies and redress, and the necessity and proportionality of surveillance. Fundamental rule-of-law reforms are also needed in relation to "secret law" interpretations within the executive branch and (to a lesser extent) Foreign Intelligence Surveillance Court.

Effective judicial redress

US legal academics and civil society groups are clear federal legislative reform will be required to provide EU data subjects with "an effective remedy before…an independent and impartial tribunal", as required by Article 47 of the Charter of Fundamental Rights.

Swire (and Docksey) have proposed such complaints could be initially investigated by US intelligence agency Privacy and Civil Liberties Officers, with their findings referred to the agency Inspector General or the Privacy and Civil Liberties Oversight Board (PCLOB). The complainant would be given standing

[218] *Schrems II* judgment, footnote 3, §§180-183 and §196.

to obtain judicial review from either the Foreign Intelligence Surveillance Court, or the PCLOB, *if* the latter's independence and power to impose binding decisions were strengthened, and its decisions could be appealed to the FISC.[219] As a practical matter, this would also require significant additional resourcing for Inspectors General and PCLOB, and a strengthening of their ability of obtain agency information. CDT has noted "U.S. courts, including the FISA Court, are the only existing mechanisms in the U.S. that could have the attributes and authorities that the CJEU deemed necessary to an adequate redress mechanism"; legislative reform would be needed to "to give the FISA Court the authority it would need to receive and act upon complaints of unlawful surveillance", including given affected European data subjects standing and enabling public hearings.[220]

Ensuring necessity and proportionality

The Court of Justice has determined "a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards."[221] And as the European Parliament noted in its resolution on the Schrems II judgment, the Court found in the first Schrems case "indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the right to confidentiality of communications provided for in Article 7 of the Charter".

To incorporate such limits, E.O. 12333 can be updated at any time by the US President, while FISA s.702 procedural changes can be approved and made binding by the Foreign Intelligence Surveillance Court, then codified by Congress.

In the most comprehensive analysis to date, the US Open Technology Institute suggests the extension of US government limits on *use* of bulk-collected data to *collection*; adopting binding rules ensuring the necessity and proportionality of bulk collection; narrowing the definition of foreign intelligence information and setting stronger standards to justify surveillance targets; requiring post hoc review by the Foreign Intelligence Surveillance Court of the necessity and proportionality of targeting decisions (at least partly addressing the gap highlighted by the CJEU in the Privacy Shield adequacy decision relating to whether 'individuals are properly targeted to acquire foreign intelligence information'); requiring agencies to provide statements of facts when querying intelligence databases about specific persons of any nationality; reducing the default retention period for collected information from five years to three; and increasing transparency about surveillance activities by the US government and targeted telecommunications and technology companies.

The American Civil Liberties Union proposes stronger limits, in particular banning bulk collection under E.O. 12333 and requiring delayed notification of surveillance targets – as the European Parliament has also called for.[222] And where specific legal processes are available for access to specific data – such as EU financial data used in the US Terrorist Finance Tracking Program, or passenger name records – these should not be circumvented using bulk collection powers (which in the case of TFTP, the European

[219] See footnotes 182 and 183.

[220] CDT, footnote 186.

[221] *Schrems II* judgment, footnote 3, §180.

[222] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) §T; European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II') (footnote 200, above), §21.

Parliament resolved "would constitute a clear breach of the Agreement").[223] CDT also recommended many of these measures, as well as a specific prohibition on "using Section 702 to collect foreign intelligence information for the purpose of burdening dissent or for disadvantaging people based on their ethnicity, race, gender, sexual orientation or religion."[224]

Making all "secret law" affecting EU data subjects available to the EU institutions

Article 52 of the Charter of Fundamental Rights requires "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law". As we concluded in section 2.3.1.1, **secret or excessively vague rules, or rules that grant unfettered discretion, do not constitute "law" in the European human rights sense.** The European Parliament resolved in 2014 "secret laws and courts violate the rule of law … any judgment of a secret court or tribunal and any decision of an administrative authority of a non-EU state secretly authorising, directly or indirectly, surveillance activities shall not be recognised or enforced".[225]

US academics and civil society groups have also called for much stricter limits on US "secret law", as objectionable to the very nature of the rule of law and protections for the public. But at a minimum, if the EU institutions are to be meaningfully able to review the "essential equivalence" of a reformed US legal regime with GDPR protections, such authoritative legal interpretations or requirements affecting EU data subjects must be shared with them by the US authorities, along with any changes to the E.O. 12333 regime. Enough detail should be made public to be "adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case".[226]

Statistics about the use of US surveillance powers against data shared under any new adequacy agreement should also be provided, equivalent to those regarding the use of surveillance powers shared by the US administration with the Congressional intelligence committees. And a regular monitoring and review mechanism should be included in any adequacy agreement, analogous to Article 13 of the EU-US Agreement on the Terrorist Finance Tracking Program, including EU data protection authorities, and making key findings public.[227] This could be part of the proactive Commission monitoring of "the use of mass surveillance technologies in the United States as well as in other third countries" requested by the European Parliament in its *Schrems II* resolution.[228]

4.3.3 Long-term intelligence reform by international agreement

The world's intelligence agencies – including those of the constitutional democracies – have been operating in important aspects outside of a clear rule-of-law framework, both in relation to their foreign intelligence gathering and in relation to their interactions. The European Court of Human Rights and especially the Court of Justice of the EU (the latter in spite of the limitations in EU law *re* national security) have made clear this is unacceptable.

---

[223] European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)), §3.

[224] Footnote 188, p.7.

[225] European Parliament mass surveillance resolution, footnote 222, §13.

[226] ECtHR, *The Sunday Times v the United Kingdom* (footnote 33), para. 49; cf. also *Kruslin v. France* (footnote 36), para. 30ff.

[227] OJ L 195/5 of 27.7. 2010. The latest report under this provision from the Commission to the Parliament and Council is COM(2019) 342 final, at: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20190722_com-2019-342-commission-report_en.pdf

[228] *Schrems II* resolution, footnote 222, §21.

At the member state level, the German constitutional court further held in 2020, against the position of the German government, that the Federal Intelligence Service "is bound by the fundamental rights of the Basic Law when conducting telecommunications surveillance of foreigners in other countries", and must comply with the constitution in "the collection and processing of data, the sharing of data thus obtained with other bodies and the cooperation with foreign intelligence services."[229]

This fundamental issue can only be resolved in a manner compatible with the international rule of law – UN charter, International Covenant on Civil and Political Rights, European Convention on Human Rights, EU treaties and Charter of Fundamental Rights – if the activities of those agencies are brought fully within a rule-of-law compatible legal framework. The EU institutions should stand up for the rule of law and demand the member states and third countries bring their practices in line with those standards. Otherwise, as Christakis and Propp note on a related issue, "If there is an eventual balance that excludes from the scrutiny of the CJEU the data retention laws and practices of European national security services, but not those of their U.S. counterpart, it might well be unstable."[230]

The activities of all states' intelligence agencies in relation to any individuals affected by those activities, wherever they may be, is subject to international human rights law. It is not impossible to see the parameters of a legal framework for such activities, viz. the EDPB's European Essential Guarantees.

Even if the USA in particular refuses to accept the principle that international human rights law applies as such to the activities of its agents and agencies outside its territory in relation to non-US persons, it is still free (in terms of its own laws) to enter into agreements that cover such activities.

While from the perspective of international law and international human rights law, a global treaty would be best, a pragmatic starting point would be a "minilateral" framework[231] for the main advanced economy democracies (which have the financial resources to undertake the large-scale technical surveillance at issue) – in particular, the 30 EU and EEA states and the "Five Eyes" countries (USA, UK, Australia, Canada and New Zealand – which are now all "third countries" in terms of EU law). Because of the (regrettable) national security exemption in the EU treaties, the EU cannot be a party to such an agreement, but there is no reason why it cannot be a midwife (or part of a midwifery team).

The drafting of such a treaty would take some time, especially if it is to lead to a treaty that is recognised as binding under US law (many international agreements of the US are adopted in the form of "executive agreements" that are not binding in US national law).[232] However, steps can also be taken pending the adoption and entering into force of such a treaty. In particular, the club of 35 countries should commit to each reviewing their existing legal frameworks governing the activities of their intelligence agencies in the light of the standards adduced at UN and European level to date (as

---

[229] *In their current form, the Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law*, English-language summary by the Federal Constitutional Court of its Judgment of 19 May 2020 (1 BvR 2835/17), footnote 9. See analysis by Marcin Rojszczak, *Extraterritorial Bulk Surveillance after the German BND Act Judgment*, European Constitutional Law Review, 12 April 2021, at:
https://www.cambridge.org/core/journals/european-constitutional-law-review/article/extraterritorial-bulk-surveillance-after-the-german-bnd-act-judgment/D6B51E73049E18D9EEB563F36CEB679E
See also Russell A. Miller, *The German Constitutional Court Nixes Foreign Surveillance*, Lawfare, 27 May 2020, at:
https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance

[230] Theodore Christakis and Kenneth Propp, *How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*, Lawfare, 8 March 2021, at: https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states

[231] Brown et al,. footnote 173.

[232]. See ASIL Insight, *International Agreements and U.S. Law*, 27 May 1997, available at:
https://www.asil.org/insights/volume/2/issue/5/international-agreements-and-us-law

reflected in the case law of the CJEU and the European Essential Guarantees) within a set (short) time period and bring them into line with these standards – as already requested by the European Parliament in 2014.[233]

The UK government commissioned an independent legal review in the aftermath of the Snowden leaks about the extensive intelligence activities of the "Five Eyes".[234] While complex and resource-intensive, it resulted in much greater transparency and a significantly improved legal framework – even if areas of human rights concern remain.[235]

We believe that within the club of 35, there should also be clear rules on the states concerned not surreptitiously spying on each other's citizens and residents. As German Chancellor Angela Merkel told then-US President Barack Obama: "spying on friends is unacceptable".[236]

The European Parliament resolution on UK data protection adequacy calls for "the Member States to enter into no-spying agreements with the UK and calls on the Commission to use its exchanges with its UK counterparts to convey the message that, if UK surveillance laws and practices are not amended, the only feasible option to facilitate the adequacy decisions would be the conclusion of 'no-spying' agreements with the Member States".[237] The Parliament will presumably take the same view with regards to the USA.

A new treaty and interim arrangements should therefore include transparent arrangements for mutual assistance between club members' intelligence agencies, subject to crucial rule of law and human rights safeguards and openness about practice (annual meaningful statistics, etc.) Furthermore, the principle of sincere cooperation in article 4(3) TEU 'means that national legislators are obliged to shape national law in such a way that Union law can enjoy full effectiveness (*effet utile*). This implies for example a restrictive application of the "public policy" and "national security" reservations to the fundamental freedoms'.[238] Lledo-Ferrar and Dietrich have noted in the intelligence and security context: "There is an increasing awareness that Europe has to play an enhanced role in building a new international order, or otherwise this order will be shaped and imposed by others."[239]

Article 11(3) of the Council of Europe's "modernised" Convention 108+ on data protection covers national security and defence. The 55 parties and over 25 observers (including the USA) could develop further guidance in the Convention 108 committee in its application.[240] The UN Special Rapporteur on

[233] European Parliament mass surveillance resolution, footnote 222, §§21-24.

[234] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

[235] D. Korff, *The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK*, submission to the EU institutions, 3 March 2021, at: https://www.ianbrown.tech/2021/03/03/the-inadequacy-of-the-eu-commissions-draft-gdpr-adequacy-decision-on-the-uk/

[236] *Merkel tells Obama: 'Spying on friends is unacceptable'*, BBC News, 24 October 2013, at: https://www.bbc.co.uk/news/av/world-europe-24659743

[237] European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)), §17, at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html

[238] H.-J. Blanke and S. Mangiameli, 'Article 4: The relations between the EU and the Member States', in The Treaty on European Union (TEU): A Commentary (Berlin, Heidelberg: Springer, 2013), pp. 185–253.

[239] Yvan Lledo-Ferrer & Jan-Hendrik Dietrich, *Building a European Intelligence Community*, 33 International Journal of Intelligence and CounterIntelligence 3, p.448.

[240] The first steps in producing such guidance have been taken with the development of a *Guidance note on Article 11 of the modernised Convention 108* by Thorsten Wetzling and Charlotte Dietrich, Council of Europe T-PD-BUR(2021)4, 7 June 2021.

Privacy, Joe Cannataci, has twice recommended to all UN member states to accede.[241] Recital 105 of the GDPR explicitly refers to the Convention in the context of adequacy decisions.

Going further, the Convention committee chair and the CoE's data protection commissioner have called for states to "agree at international level on the extent to which the surveillance performed by intelligence services can be authorised, under which conditions and according to which safeguards, together with independent and effective oversight… The time has come to use the numerous criteria developed by the Courts, including the US Supreme Court, in respect of what constitute adequate and effective guarantees, effective accountability, and independent oversight of intelligence services, and find consensus on this critical issue at global level."

The chair and commissioner suggest states "should accede to Convention 108+ and should also seize the unique potential offered by the Council of Europe, and the chance that is given to address the question of the operation of intelligence services, under the aegis of a globally respected human rights organisation."[242] We can only agree.

If the suggestions of a common legal framework for intelligence/national security activities can be agreed between the democracies, that would also address the criticism levelled by the USA at the EU about the application of different standards (even though, as we have shown, that criticism was not fully justified).

4.4 Overall conclusions & recommendations

4.4.1 Overall conclusions

On the basis of the existing available data, studies and analysis from various sources and documents from national and international institutions, set out and analysed in our study, we do not believe that any US federal or state privacy law is likely to provide "essentially equivalent" protection compared to the EU GDPR in the foreseeable future. Indeed, there are serious and in practice insurmountable US constitutional and institutional as well as practical/political obstacles to the adoption of such laws.

However, we also believe that ***if*** (i) the US and the EU were to take the legislative steps relating to substance, enforcement and individuals' rights of action we outlined in section 4.2.3, **and** ***if*** (ii) the US were to reform its surveillance laws and practices as discussed in section 4.3.2 (in terms of effective judicial remedies and redress, ensuring the necessity and proportionality of surveillance, and fundamental rule-of-law reforms in relation to "secret law" interpretations), ***then*** a new EU-US arrangement for self-certification by US entities could be achieved, under which the EU could issue a new positive adequacy decision on the USA, limited to personal data transferred from the EU to entities that had self-certified their voluntary compliance with the EU GDPR substantive standards.

We reach this conclusion somewhat reluctantly, given the strong views on self-certification of the European Parliament.[243] However, we believe it is the only workable solution, given that in the USA the issues cannot be resolved by new federal or state privacy laws. We should stress two matters. First, we are not talking about a revival of the disastrous and untenable Safe Harbour/Privacy Shield

[241] *2018 Annual Report on the Right to Privacy to the Assembly General* (Report A/73/45712) and *Annual Report of 1 March 2019 to the UN Human Rights Council* (Report A/HRC/40/63).

[242] "Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services". *Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe*, Strasbourg, 7 September 2020.

[243] See the European Parliament resolution of 20 May 2021 on Schrems II (footnote 200, above),) §28, quoted in sub-section 4.2.1, above.

arrangements, but about **a fundamentally different, enhanced system of self-certification**, with the self-certification itself **relating to the whole of the GDPR** (rather than to a watered-down reflection of the regulation in impenetrable collections of documents) and **much stronger enforcement** by the FTC (which should be given **much wider powers** to this end).

Second, **even the best scheme based on self-certification cannot overcome the deficiencies in the US legal regimes for access to data transferred from the EU to the USA (or directly accessed by the US intelligence agencies from the USA).** Any solution must comprise both elements: providing "adequacy"/"essential equivalence" (by means of a system of enhanced self-certification with reinforced enforcement) **AND** fundamental reforms to US surveillance laws.

We believe these twin aims are not only achievable if the political will is there (on all sides), but also essential if the rule of law is to be upheld in relation to both data protection and privacy generally, and specifically in relation to the activities of the intelligence agencies of the constitutional democracies. Indeed, **a common legal framework for intelligence/national security activities** (as discussed in section 4.3.3) would send a clear signal to the rest of the world that those countries are indeed committed to international law and international human rights law.

More broadly, as international relations experts Henry Farrell and Abraham Newman put it:

> For two decades, the U.S. has been able to have its cake and eat it too — behaving like a unilateral, imperialist power in an interdependent world. *Schrems II* shows how that strategy is reaching its limits. The U.S. is discovering that interdependence means that it too is vulnerable. Fixing these vulnerabilities is going to require much deeper international cooperation with like-minded democracies. And that in turn entails a very different relationship between national courts and international surveillance.
>
> America's security isn't being undermined by Europe's privacy demands. Instead, engaging these demands could provide politically robust foundations for the security architecture that both America and its allies need to confront the new threats associated with a changing world.[244]

As former US Acting Commerce Secretary Cameron Kerry has noted, "Arriving at a framework that can satisfy the CJEU will challenge both the European Commission and the U.S., but neither can afford a third strike in court."[245]

4.4.2 Recommendations

We were asked to provide clear recommendations to the European Parliament on proposed institutional, substantive and procedural reforms (also addressing prioritisation), with identification of the criteria (the rationale) for the recommendations and for such prioritising. As explained in more detail in the previous sections (and chapters), our recommendations effectively come down to four (we discuss their prioritisation after summarising them):

[244] Footnote 73.

[245] Cameron Kerry, *The oracle at Luxembourg: The EU Court of Justice judges the world on surveillance and privacy*, Brookings Institution, 11 January 2021, at: https://www.brookings.edu/research/the-oracle-at-luxembourg-the-eu-court-of-justice-judges-the-world-on-surveillance-and-privacy/

Recommendation No. 1 (achieving general adequacy *pace* the issue of undue access):

The EU and the US should enter into discussions on the establishment of a much enhanced and strengthened self-certification scheme for US corporations.

Criteria/rationale:

We somewhat reluctantly concluded that, since no US federal or state privacy law is likely to provide "essentially equivalent" protection compared to the EU GDPR in the foreseeable future (or ever), general adequacy can only be achieved under a new self-certification scheme enforced through the FTC.

However, any such new self-certification scheme would have to apply to all substantive requirements of the EU GDPR; the FTC would need to be given wider and stronger powers; and EU data subjects should be accorded rights of standing in relation to breaches of the scheme.

Recommendation No. 2 (addressing the issue of undue access to data by US intelligence agencies):

The US should be urged to reform its federal surveillance legislation as a matter of urgency. This should involve limiting bulk collection; narrowing the definition of foreign intelligence information and setting stronger standards to justify surveillance targets; reducing the default retention period for collected information from five years to three; increasing transparency about surveillance activities; and providing EU data subjects with "an effective remedy before…an independent and impartial tribunal" – which can be achieved by granting EU complainants standing to obtain judicial review from the Foreign Intelligence Surveillance Court.

Criteria/rationale:

Given the strong and unambiguous stand taken by the CJEU in its *Schrems II* judgment, unless such reform is carried out, no new positive "adequacy" decision on the USA can be issued by the EU Commission. (If one were to be issued in defiance of the judgment, that would both seriously undermine the credibility of the Commission as a guardian of the Treaties and lead to yet another defeat – a "third strike" – in the Court. That should be beyond contemplation.)

Recommendation No. 3 (bringing surveillance generally under the rule of law):

The EU institutions and in particular the European Parliament should stand up for the rule of law and demand that both the Member States and third countries bring their intelligence practices and domestic law frameworks fully in line with international human rights law.

They should urge, as a pragmatic starting point, the urgent development and ratification of a "minilateral" treaty covering intelligence activities of, in particular, the 30 EU/EEA states and the "Five Eyes" countries (USA, UK, Australia, Canada and New Zealand).

As an interim measure, these 35 countries should agree not to spy on each other's citizens (and their data) without the notification and agreement of the citizen's home state.

Criteria/rationale:

The intelligence agencies of the constitutional democracies have operated for too long outside of a clear and acknowledged framework of (international, and often even constitutional) law. As the European Court of Human Rights Grand Chamber judgment in the *Big Brother Watch* case makes clear, the ECHR (as interpreted and applied by that Court) is insufficient for this purpose. While, regrettably in our view, the activities of the EU Member States in relation to national security are outside the scope

of EU law, the EU (working with the Council of Europe) can be a midwife to a new international agreement in this area. However, this would take some years.

We therefore hope that an interim, less formal, "no spying on allies" agreement can be achieved in the meantime, within a relatively short timeframe.

Recommendation No. 4 (strengthening representative/class actions in the EU):

The EU should offer the USA (and the rest of the world) the introduction of a genuine US-style class action remedy in relation to any violations of the GDPR, which anyone who suffered material or non-material damage as a result of a violation (whatever their nationality, status, or place of residence) could join.

Criteria/rationale:

As the case of Max Schrems shows, EU data subjects' rights and interests are often not effectively enforced, or the individuals concerned supported, by the EU Member States' supervisory authorities, and court actions are costly and pose serious (financial) risks to them. In that regard, the EU can learn from the US (although the "Article III" jurisdictional issue imposes limits there too).

Overall, we concluded that if the above four recommendations were to be implemented, transfers of personal data from the EU to the USA could again be facilitated under the new self-certification scheme, with a new adequacy decision issued by the EU Commission that would not be invalidated by the Court.

Until this achieved, transfers of personal data from the EU to the USA must be based on "appropriate safeguards" including standard contractual clauses (SCCs) and Binding Corporate Rules (BCRs), or in due course approved codes of conduct or certifications issued by appropriate, accredited certification authorities – but in effectively all these cases, "supplementary measures" such as strong encryption will be required to protect transferred data against undue access by the US intelligence agencies. And no effective supplementary measures have yet been identified that could protect against such undue access if the data have to be accessible to the data importer in the USA in the clear. Some measures, such as audits, logs and reporting mechanisms could possibly be used in some such contexts (in particular, where the data are clearly not at all sensitive – in a broad sense – and unlikely to be of interest to the US intelligence agencies). But for sensitive data in the broad sense (sensitive data in the formal sense of the GDPR and other, more generally sensitive data such as communications data, financial data and travel data), these will generally not suffice.

The issues therefore need to be addressed **urgently**. This brings us to the final matter: prioritisation.

Prioritisation:

We believe the issues are best addressed in this order:

1. The EU should identify stop-gap measures such as audits, logs and reporting mechanisms that can possibly be used to allow some transfers of non-sensitive data – but also identify categories of data (and/or of controllers and processors or contexts) in relation to which these will not suffice. The European Parliament should ask the EDPB to address these matters in yet further guidance on EU–US data transfers, drawing on the work of the Commission in relation to the Digital Services Act and the Digital Markets Act.

   We believe this can be done in a matter of **a few months** at most.

2. The European Parliament should urge the EU Member States and the "Five Eyes" to adopt as a matter of urgency an interim, somewhat informal, "no spying on allies" agreement, while at the same time;

3. The EU Member States and the "Five Eyes" should commence a formal process towards the adoption of a formal "minilateral" agreement.

   We believe that (if the political will is there) an interim agreement could be possible within **a few months** – but ratification of a full treaty (which would also have to have internal effect in the USA – which not all US international agreements do) would take **several years**.

4. In parallel with the above, the EU should urge the USA to start the reforms of its surveillance laws and of the FTC Act that have been suggested by expert academics and civil society groups in the USA and the EU. It would be important to have a working group established on this issue that can exchange views on what is necessary (and possible) and report on progress; this working group should include representatives of the European Parliament.

   We believe that significant reforms could be achieved in US law **this (executive order)/next (statutory) year** (again, if the political will is there, and the EU forcefully urges this.)

- o – O – o –

REFERENCES

- Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review*, Presented to the Prime Minister pursuant to section 7 of the Data Retention and Investigatory Powers Act 2014, June 2015.
- Bignami, F. *The US legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens*, European Parliament, 2015.
- Blanke, H.-J. and S. Mangiameli, *Article 4: The relations between the EU and the Member States*, in The Treaty on European Union (TEU): A Commentary (Berlin, Heidelberg: Springer, 2013), pp. 185–253.
- Brown, I., M. H. Halperin, B. Hayes, B. Scott and M. Vermeulen, Towards Multilateral Standards for Surveillance Reform, In R. A. Miller (ed., 2017) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, pp. 461–491.
- Christakis, T. and K. Propp, *How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*, Lawfare, 8 March 2021.
- Council of Europe Commissioner for Human Rights, *Issue Paper* on *The Rule of Law on the Internet and in the wider digital environment*, 2014.
- Docksey, C. *Schrems II and Individual Redress—Where There's a Will, There's a Way*, Lawfare, 12 October 2020.
- Farrell, H. and A. Newman, *Schrems II Offers an Opportunity—If the U.S. Wants to Take It*, Lawfare, 28 July 2020.
- Franklin, S.B., L. Sarkesian, R. Schulman and S. Singh, *Strengthening Surveillance Safeguards After Schrems II: A Roadmap for Reform*, Open Technology Institute, April 2021.
- Goitein, E. *The New Era of Secret Law*, Brennan Center for Justice at New York University School of Law, 2016.
- Greenleaf, G. *California's CCPA 2.0: Does the US finally have a data privacy Act?* 168 Privacy Laws & Business International Report, 13-17, December 2020.
- Greenleaf, G. *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, in:' International Data Privacy Law, Vol. 2, Issue 2, 2012.
- Goldsmith, J. *Reflections on U.S. Economic Espionage, Post-Snowden*, Lawfare, 10 December 2013.
- Harris, D., M. O'Boyle, E. Bates & C. Buckley, *Law of the European Convention on Human Rights*, Oxford University Press, 2nd Ed., 2009.
- Heck, Z. S. *A Litigator's Primer on European Union and American Privacy Laws and Regulations,* 44 Litigation 59, 2018.
- Hoofnagle, C. J. *New Challenges to Data Protection - Country Report: United States*, study for the European Commission, 2010.
- Hoofnagle, C. J. *Federal Trade Commission Privacy Law and Policy*, Cambridge University Press, 2016.
- Kerr, O. S. *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 George Washington Law Review 1208, 1212, 2004.
- Kerry, C. F., J. B. Morris, Jr., C. T. Chin, and N. E. Turner Lee, *Bridging The Gaps, A path forward to federal privacy legislation*, Brookings Institution, June 2020.

- Kerry, C. F. and J. B. Morris, Jr., *Framing a privacy right: Legislative findings for federal privacy legislation,* Brookings Institution, 8 December 2020.
- Klamberg, M. *Big Brother's Little, More Dangerous Brother: Centrum för Rättvisa v. Sweden*, Verfassungsblog, 1 June 2021.
- Lledo-Ferrer, Y. & J-H. Dietrich, *Building a European Intelligence Community*, 33 International Journal of Intelligence and CounterIntelligence 3 440—451, 2020.
- Messaud, A. and N. Levain, *CJEU rulings v. French intelligence legislation*, about:intel, 14 May 2021.
- Miller, R. A. *The German Constitutional Court Nixes Foreign Surveillance*, Lawfare, 27 May 2020.
- Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe*, September 2017.
- Rojszczak, M. *Extraterritorial Bulk Surveillance after the German BND Act Judgment*, 17 European Constitutional Law Review 1 53-77, 2021.
- Solove, D. and W. Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia Law Review 583, 587, 2014.
- Swire, P. *U.S. Senate Commerce Committee Testimony on "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows"*, 9 December 2020.
- US Congressional Research Service report, *Data Protection Law: An Overview*, 25 March 2019.
- US Congressional Research Service report, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, 17 March 2021.
- Warren, S. and L. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193, 1890.
- Zalnieriute, M. *A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence*, EJIL Talk! 4 June 2021.
- Zerdick, T. Article 52, Independence. In C. Kuner, L. A. Bygrave, C. Docksey and L. Drechsler (eds.), *The EU General Data Protection Regulation – A Commentary*, Oxford University Press, 2020.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, examines reforms to the legal framework for the exchange of personal and other data between the EU and the USA that would be necessary to ascertain that the requirements of EU law are satisfied and that the rights of EU citizens are respected, following the Schrems II judgment of the EU Court of Justice.

PE 694.678
IP/C/LIBE/IC/2021-040

Print ISBN 978-92-846-8362-8| doi: 10.2861/448520 | QA-08-21-154-EN-C
PDF ISBN 978-92-846-8152-5 | doi:10.2861/85977 | QA-08-21-154-EN-N