UCL EUROPEAN INSTITUTE

UCL

UCL
EUROPEAN
INSTITUTE

POLICY
PAPER

EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows

Oliver Patel and Dr Nathan Lea

May 2020

EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows

Oliver Patel and Dr Nathan Lea
May 2020

CONTENTS

Recommended Audience

- Academics, researchers, students and others interested in data protection, EU law, Brexit or transatlantic relations
- Policy makers and regulators
- Data protection officers and professionals
- TMT lawyers and consultants
- Technology and services industry professionals

Methodology

The findings were informed by analysis of primary documents, an extensive literature review and over sixty anonymous interviews with EU, U.S. and UK politicians, civil servants, ambassadors, regulators, lawyers, business leaders, data protection officers and researchers conducted between 2018 and 2020.

Acknowledgements

Oliver Patel is Research Associate and Manager at the UCL European Institute. **Dr Nathan Lea** is Senior Research Associate at the UCL Institute of Health Informatics. **William Chantry**, Research Assistant at the UCL European Institute, and **Dr Uta Staiger**, Executive Director of the UCL European Institute, also made significant contributions to the writing of the paper. We thank UCL's Laidlaw Scholarship Programme for their generous support for this research.

Introduction

This report analyses the issues raised by EU-U.S. commercial data flows, including the future status of the Privacy Shield framework and standard contractual clauses (SCCs). It begins by comparing the systems of data protection in the EU and the U.S., highlighting key philosophical, legal and practical differences.

The next section assesses the history of EU-U.S. data flows and the upcoming judgement in the Schrems II case. It then outlines why a clash between U.S. national security laws and mass surveillance on the one hand, and EU data protection and fundamental rights law on the other, renders all transatlantic data transfer mechanisms vulnerable, with few alternative options.

The final section focuses on EU-UK data flows post-Brexit and the UK's quest for an EU adequacy decision, highlighting the key lessons which can be learnt from the EU-U.S. case study and the challenges which lie ahead. The main argument is that the EU-UK data flows relationship will be complex and could remain unresolved for years. Policy makers, businesses and data protection officers should prepare for a rocky few years ahead, not least due to the high possibility of any adequacy decision facing concerted legal challenges.

Key Messages

EU-U.S. Data Flows

- EU data protection law is comprehensive, harmonised and grounded in fundamental rights, in contrast to the limited and inconsistent patchwork of U.S. data privacy laws and lack of constitutional protection for privacy.
- The EU has been considerably more influential than the U.S. in the development of global data protection standards. However, EU data protection enforcement has been heavily criticised and much larger privacy enforcement fines have been issued in the U.S.
- Despite these differences, the EU-U.S. Privacy Shield framework facilitates unrestricted commercial data flows across the Atlantic. Over 5300 firms use Privacy Shield and it underpins transatlantic digital trade.
- It is highly plausible that Privacy Shield will be struck down by the European Court of Justice in future, due to unresolved concerns regarding U.S. government access to EU citizens' data for law enforcement and national security purposes. Political fallout is guaranteed should Privacy Shield be invalidated.
- Standard contractual clauses (SCCs), the main alternative legal mechanism for EU-U.S. data transfers, are also vulnerable. Complaints, investigations and potentially suspensions of SCCs used to transfer data to the U.S. are highly likely to increase in the coming years. This implicates major internet and telecommunications companies most affected by U.S. mass surveillance law.
- There is minimal scope for a political or legal resolution due to a clash between U.S. national security and surveillance laws and programmes, and EU data protection standards and fundamental rights.
- U.S. officials and businesses feel aggrieved at the situation, with a prevailing perception that the EU has been unfair in penalising the U.S. for its national security and intelligence gathering activities. The complication arises because the EU does not have competence over member state national security, but it assesses the national security legislation of third countries when undertaking data adequacy assessments.
- There is a lack of robust, empirical research on the value and importance of Privacy Shield and EU-U.S. data flows. It is thus difficult to assess how damaging severe restriction to transatlantic data flows would be.

EU-UK Data Flows

- The long-standing conflict over EU-U.S. data flows is an instructive case study for EU-UK data flows post-Brexit. Given the UK's insistence on not extending the transition period, this issue is of urgent, strategic importance.
- The UK will face very similar problems to those of the U.S. The EU-UK data flows relationship will be complex and could remain unresolved for years. Policy makers, businesses and data protection officers should prepare for a rocky few years ahead.
- The European Commission will likely grant the UK an adequacy decision. The flexibility and pragmatism which the Commission has demonstrated towards the U.S. indicates this.
- However, a UK adequacy decision would likely face multiple legal challenges that could take years to resolve. The threat of European Court of Justice invalidation would always loom large.
- The vulnerability of SCCs also impacts UK firms – especially 'telecommunications operators' most affected by Investigatory Powers Act notices – as complaints, investigations and suspensions of SCCs used to transfer data from the EU to the UK are increasingly likely.
- If there is no adequacy decision and important SCCs are suspended, this could lead to severe disruption to EU-UK data flows, with negative economic consequences.
- With the UK's national security and surveillance practices under scrutiny, UK officials and businesses may also feel aggrieved at the adequacy process, and political fallout in the case of no adequacy decision would be almost guaranteed.
- The U.S. pushes hard for unrestricted data flows in its trade negotiations. If the UK significantly liberalises data flows with the U.S. in a future trade agreement, this could undermine its prospects for EU adequacy.

SECTION 1: Comparing Data Protection in the EU and the U.S.

What is the U.S. system of data privacy?

Terminology: In the EU and the UK the term 'data protection' is used. In the U.S., it is 'data privacy' (or 'information privacy'). In this report, the terms will be used interchangeably according to the relevant context, but 'data protection' is used as the default.

There is no comprehensive, federal data privacy legislation which covers all economic sectors and commercial data processing. Instead, there are several federal laws which govern the processing and use of personal data in specific domains. Many economic sectors are not covered by these laws, and many of these laws were passed in response to specific incidents or concerns.[1] Below is a non-exhaustive list of the most important federal privacy laws:

Federal data privacy law	Core purpose
Fair Credit Reporting Act (FCRA, 1970)	Promotes the accuracy and privacy of personal data contained in credit report files.
Privacy Act of 1974	Governs the collection, use and dissemination of personal data that is processed by federal agencies.
Electronic Communications Privacy Act of 1986 (ECPA)	Extends restrictions on wiretaps to include electronic transmission of data by computer.
Video Privacy Protection Act (VPPA, 1988)	Protects the privacy of consumer video tape (and other audio-visual material) rental or sale records.
Children's Online Privacy Protection Act (COPPA, 1998)	Governs the online collection of personal data from children under 13 years of age.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Governs how personal data should be maintained and processed by the healthcare industry and insurers.
Gramm-Leach-Bliley Act (GLBA, 1999)	Requires financial institutions to explain their data-sharing practices to their customers and to safeguard sensitive data.
Health Information Technology for Economic and Clinical Health Act (HITECH, 2009)	Various enhancements to HIPAA legislation, such as stricter data breach notification requirements.

Over the years, many federal privacy bills have been presented to Congress, but there has never been the appetite to pass one.[2] The Federal Trade Commission (FTC) proposed such legislation in 2000, but after the 9/11 terrorist attacks Congress lost interest as priorities shifted away from privacy.[3]

However, there is increasing talk of Congress passing a comprehensive federal data privacy law, with many of our interviewees noting that bipartisan agreement is more attainable now than ever. A bigger question is whether there is political will to prioritise the issue. In 2012, the Obama Administration published a Consumer Data Privacy White Paper, with detailed proposals for a 'Consumer Privacy Bill of Rights'.[4] The draft Bill was published in 2015 and received significant pushback from the technology sector. It never passed and the plans were dropped by the Trump administration. More recently, several Senators have brought forward proposals.[5]

The U.S. data privacy system is highly fragmented, as there is a myriad of different laws and provisions at the state-level. Three states have passed comprehensive data privacy legislation: California, Nevada and Maine. A further thirteen laws are currently being reviewed by state legislatures, but it is unknown how many of these will be enacted.[6]

The California Consumer Privacy Act (CCPA) is the most significant state privacy law to date. It was passed in September 2018 and became effective on 1 January 2020. There are some notable similarities between the EU's GDPR and the CCPA. For example, both laws have a similar definition of 'personal data', similar rights to erasure/deletion of data, as well as similar rights to data portability and access to data. However, there are also key differences. For example, the CCPA is more limited in scope, is not strongly extraterritorial and does not require organisations to have a lawful basis to process data.

Just as the EU is setting global privacy standards, California is setting the U.S. standard. Several proposed state privacy laws, including in Hawaii, Massachusetts and New York, are to varying degrees modelled on the CCPA.[7]

Jim Halpert of DLA Piper predicted that, ***"federal privacy legislation is likely to pass in the next three to five years, modelled on but going somewhat beyond the CCPA. U.S. businesses urgently want one set of laws to follow and Republicans do not want California to set the standards for the whole U.S."***.[8]

An important shift in recent years is the increasing support for federal privacy legislation from the technology giants and corporate America more broadly. In September 2019, a group of 51 CEOs, including the bosses of Amazon, Salesforce and Visa, signed a letter to Congress calling for the establishment of a 'national privacy framework' via federal legislation.[9] The CEOs of Apple, Facebook and Microsoft have made similar calls,[10] with Apple CEO Tim Cook arguing that "privacy is a fundamental human right".[11]

The key driver of this shift is probably not an emerging realisation of the fundamental value of privacy. Rather, it is principally

1 Lee Bygrave, 'Transatlantic Tensions on Data Privacy' (2013) Transworld Working Paper, p. 7.
2 Matthew Humerick, 'The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?' (2018) Catholic University Journal of Law and Technology.
3 Shoshana Zuboff, 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' (2019) PublicAffairs, pp. 113-114.
4 The White House, 'Consumer Data Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (2012).
5 Müge Fazlioglu, 'Consensus and Controversy in the Debate Over Federal Data Privacy Legislation in the United States' (2019) International Association of Privacy Professionals.
6 Mitchell Noordyke, 'US State Comprehensive Privacy Law Comparison' (2020) International Association of Privacy Professionals.
7 Andy Green, 'Complete Guide to Privacy Laws in the US' (2020) Varonis Blog.
8 Research interview with U.S. privacy lawyer Jim Halpert (2019).
9 Business Roundtable Letter (2019).
10 Elizabeth Schulze, 'Mark Zuckerberg says he wants stricter European-style privacy laws — but some experts are questioning his motives' (2019) CNBC.
11 CNBC, 'Tim Cook: Privacy is a fundamental human right' (2018).

because firms do not want to have to comply with multiple different state and federal laws, all of which have slightly different obligations, stipulations, consumer rights and enforcement implications.

Many companies collect and use personal data from every U.S. state, as well as individuals worldwide. Such jurisdictional difference makes compliance messy, more complex and more expensive. For example, although all fifty states have similar data breach notification laws, there are some slight differences.[12] In the event of a data breach, firms need to identify which individuals are affected and notify individuals and state regulators in the correct way and within the required time period, which can vary according to which state they are from. As more states pass comprehensive privacy laws, such "nightmarish" compliance scenarios will worsen.[13]

U.S. federal data privacy laws are enforced by the FTC. The FTC was not set up as a dedicated data privacy regulator. Rather, it tackles 'unfair or deceptive practices' in commerce more broadly, which also includes competition and consumer fraud. However, its privacy enforcement division has become increasingly active, employing over seventy people, and has been creative in using its limited powers to become an 'activist privacy regulator'.[14]

Since 1997, the FTC has initiated over 270 cases concerning privacy and in recent years it has fined many organisations including Facebook, Cambridge Analytica, Google, Equifax, PayPal and Ashley Madison.[15] At the state-level, attorney generals enforce the patchwork of state laws, sometimes in cooperation with the FTC. The Federal Communications Commission (FCC) has also imposed fines on companies for privacy violations.

How does the U.S. data privacy system compare with the EU data protection system?

There are important practical and philosophical differences between data privacy in the U.S. and data protection in the EU. EU data protection laws are both comprehensive and harmonised. The GDPR covers the processing and use of personal data for any commercial purpose. It applies to all economic sectors, as well as all entities processing personal data both within the EU and those processing EU citizens' data but based outside the EU. As such, unlike the U.S. system, the GDPR is a comprehensive data protection law with extra-territorial applicability.

The GDPR provides for harmonised data protection standards across the EU. As a regulation, it is directly applicable in all EU member states. However, many member states have also passed separate data protection laws (e.g. the UK's Data Protection Act 2018), which either take advantage of GDPR derogations or strengthen its protections. This harmonised data protection framework enables the free flow of data within the EU and, in contrast to the patchwork of U.S. state laws, makes it easy for organisations to comply with the law across Europe.

Philosophically, the U.S. system is more laissez faire and neoliberal. Successive U.S. governments have prioritised innovation and the growth of the technology sector, and have been loath to regulate its activities in a substantial way.[16] Private sector self-regulation has long been favoured and promoted. In the 1990s, the Clinton administration sought to "embed the U.S. self-regulatory approach as the global standard". There was alarm at the EU's 1995 Data Protection Directive,[17] not least because it imposed restrictions on the transfer of personal data between the EU and the U.S., which was perceived as threatening transatlantic trade.[18] That Directive later evolved into the 2018 GDPR, which is commonly (and ironically) described as the most significant piece of U.S. internet legislation of the past decade.[19]

Respect for private life and data protection are fundamental rights under EU law, which are protected at the highest constitutional level, i.e. in Articles 7 and 8 of the EU's Charter of Fundamental Rights (the Charter). These rights are vigorously upheld by the European Court of Justice (CJEU). This underlies the EU's belief that data protection cannot be left to the free market. The CJEU also draws upon the separate European Convention on Human Rights (ECHR), which is upheld by the European Court of Human Rights (EctHR) and protects the right to respect for private life (Article 8). Several member states, including Germany, Czechia and Greece, have also enshrined the right to privacy in their constitutions.

The rights to privacy and data protection are not absolute and both the CJEU and the EctHR perform 'proportionality tests' when they conflict with other fundamental rights. However, the relevant case law (e.g. the 2014 Google Spain judgement on the right to be forgotten) demonstrates that the CJEU does not consider the economic benefit of free data flows as a higher value than the fundamental right to data protection.[20]

In the U.S., privacy is not a fundamental right and it is not protected by the Constitution. The U.S. Constitution is one of negative rights and was largely designed to limit government power. In some ways, the Constitution actually strengthens the rights of data processing organisations.[21] For example, the First Amendment, which prevents Congress from 'undermining freedom of speech', has been used to curtail data privacy in the U.S.[22] In 2011, the Supreme Court used the First Amendment to strike down a Vermont data privacy law. The law prohibited pharmacies and health insurers from selling prescribers' personal information or allowing such information to be used for marketing without the consent of the prescriber. By six votes to three, the Court concluded that these measures restrict the free speech rights of the affected companies.[23] Similarly, internet service providers (ISPs) are currently suing the state of Maine, claiming that Maine's new privacy law violates their rights to free speech.[24]

Legal scholars Schwartz and Peifer argue that the U.S. and the EU have constructed different legal identities around data privacy.[25] In the US, there is a 'marketplace discourse', as the FTC protects '*consumers*' from unfair practices in the '*marketplace*', but the legal system generally favours data processors over consumers. In the EU, by contrast, the right to data protection

12 Digital Guardian, 'The Definitive Guide to U.S. State Data Breach Laws' (2018).
13 Research interview with privacy lawyer (2020).
14 Kenneth Bamberger and Deirdre Mulligan, 'Privacy on the Books and on the Ground' (2011) Stanford Law Review, p. 273.
15 Federal Trade Commission, 'Cases Tagged with Privacy and Security' (2020).
16 Ioanna Tourkochoriti, 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection' (2014) The University of Arkansas at Little Rock Law Review.
17 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. 130.
18 Lee Bygrave, 'Transatlantic Tensions on Data Privacy' (2013) Transworld Working Paper, p. 9.
19 Remarks from several research interviews.
20 Judgement of the Court (Grand Chamber), 13 May 2014.
21 Paul Schwartz and Karl-Nikoloaus Peifer, 'Transatlantic Data Privacy' (2017) The Georgetown Law Journal, p. 155.
22 Shoshana Zuboff, 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' (2019) PublicAffairs, pp. 107.
23 Electronic Privacy Information Center, 'IMS Health v. Sorrell'.
24 Jon Brodkin, 'ISPs sue Maine, claim Web-privacy law violates their free speech rights' (2020) Ars Technica.
25 Paul Schwartz and Karl-Nikoloaus Peifer, 'Transatlantic Data Privacy' (2017) The Georgetown Law Journal, pp. 121-138.

is strongly anchored at the constitutional level. The EU's system is characterised by '*rights talk*' and protecting the '*fundamental rights of data subjects*'.

This philosophical difference gives rise to a major legal difference. Under EU law, organisations must have a lawful basis for processing personal data. Article 6 of the GDPR outlines the six lawful bases; at least one of these must apply for an organisation to process personal data: (a) Consent, (b) Contract, (c) Legal obligation, (d) Vital interests, (e) Public task and (f) Legitimate interests. There must be a legal basis for data processing irrespective of whether there is potential for harm. Under U.S. law, the default is that companies can process personal data, without a lawful basis, unless it causes harm or there is a specific legal requirement against that processing.[26] This means that organisations generally do not need the consent of individuals, or a valid contract, to collect and process personal data.

How do the U.S. and EU enforcement systems compare?

There are also important differences regarding data protection enforcement. Unlike the U.S., each EU member state has a dedicated data protection authority (DPA). DPAs are independent regulators whose primary purpose is to enforce data protection laws. They have a broad range of powers and can fine any organisation which processes EU citizens' data up to €20 million, or up to 4% of annual worldwide turnover (whichever is greater) for GDPR non-compliance.

The powers of the FTC are more limited, as there is no comprehensive federal privacy law to enforce. It can only fine companies for 'unfair and deceptive practices' as stipulated by the Federal Trade Commission Act. Citizens cannot bring private action using this Act, so they rely on FTC orders. The FTC has been criticised for being too reactive and it does not investigate every single complaint. However, in the EU, individuals can bring cases to their DPA, all of which must be investigated. Some believe that privacy enforcement is limited by the lack of a dedicated data privacy agency (as well as comprehensive, federal legislation). [27] The U.S. is the only OECD nation without a DPA.

However, in some ways, enforcement of data privacy law is stronger in the U.S. than the EU. Several FTC fines have been larger than any European DPA fines and there is no restriction or maximum fine in U.S. law. The recent $5 billion Facebook fine[28] for the Cambridge Analytica scandal and the Equifax fine of up to $700 million[29] are much larger than any GDPR fine to date. Notably, YouTube was also fined $170 million by the FTC and the New York attorney general for violating children's online privacy laws.[30] The largest GDPR fines have both been issued by the UK's Information Commissioner's Office (ICO). At £183 million for British Airways[31] and £99 million for Marriott[32], they are much smaller than the largest FTC privacy fines.

Furthermore, in the U.S., class action lawsuits have been used to impose major fines on companies for data privacy wrongdoing. These lawsuits are a form of representative litigation whereby one party represents a group of people to obtain collective relief for a civil wrong. Some privacy laws have led to both class action lawsuits and FTC fines. Jim Halpert claimed that, "there is a culture of compliance and degree of financial risk in the U.S. which does not exist in Europe".[33] However, the constitutional requirements for 'standing' in the U.S. make it difficult for individuals to pursue privacy wrongdoings through the courts, as it is often difficult to prove concrete harm.[34]

Several European DPAs have been criticised for being ineffective, poorly resourced and lacking teeth. Half of all EU governments provide annual budgets of €5 million or less to their DPAs, which also hire very few technical specialists. Ireland's Data Protection Commission (DPC) has been singled out, as many U.S. technology giants fall under its jurisdiction, but it has yet to issue any major GDPR fines.[35] Moreover, many privacy activists and even European Commission officials are underwhelmed and disappointed by the GDPR's progress, due to the lack of major enforcement action towards the technology giants and suspected or apparent mass non-compliance in sectors like digital advertising.

In sum, EU DPAs have the power to issue major fines, but so far have been more reluctant to do so than the FTC. However, EU DPAs have more powers and can take enforcement action for a much broader set of reasons than the FTC, due to the comprehensive nature of the GDPR compared to the limited powers of the FTC Act.

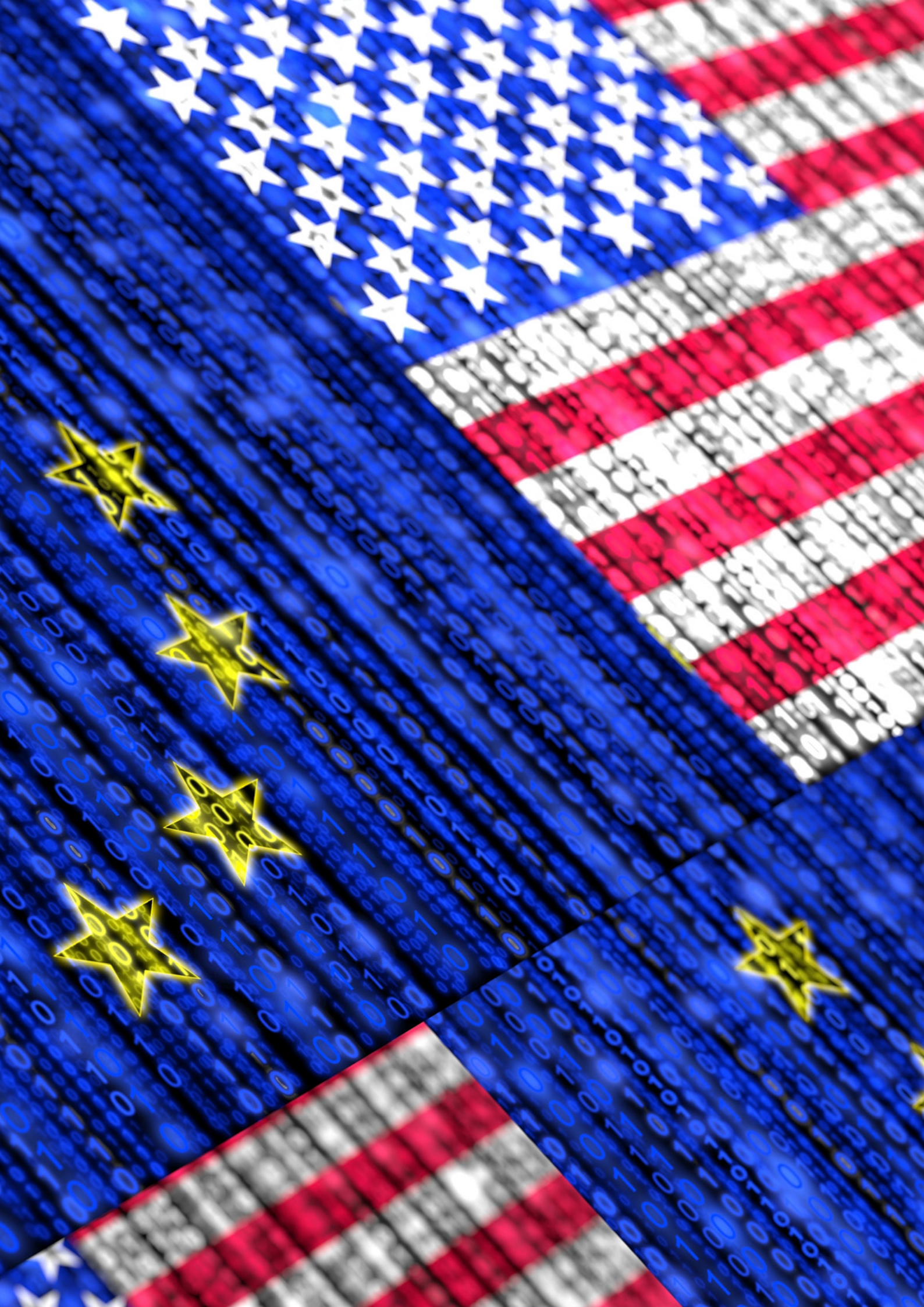
Despite the global influence of U.S. technology firms and innovation, the U.S. has not been influential in the development of global privacy standards.[36] In contrast, the EU has effectively become the world's 'privacy cop'. Worldwide, 132 jurisdictions have enacted data privacy laws, with many of these adopting EU-style privacy laws[37] and virtually all U.S. technology giants following the GDPR, which is a 'quasi global law' due to its extra-territorial applicability and the EU's economic power.[38] According to Schwartz, the EU's 'highly transplantable legal model' (i.e. the GDPR) has succeeded in the 'global marketplace of regulatory ideas',[39] while the U.S. continues to lag behind, with its patchwork of sectoral federal laws and inconsistent state laws. The lack of U.S. influence is remarkable when considering its regulatory influence in other technology domains, like intellectual property and telecommunications.[40] It is worth noting that the U.S. is increasingly unique amongst developed nations for not enacting comprehensive privacy legislation.

Despite these key differences, neither the EU nor the U.S. are monolithic actors. Rather, there exists a multiplicity of state and non-state actors on either side, which all prioritise and lobby for/against data protection to varying degrees.[41]

26 Ioanna Tourkochoriti, 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection' (2014) The University of Arkansas at Little Rock Law Review, p. 164.
27 Electronic Privacy Information Center, 'The U.S. urgently needs a data protection agency' (2020).
28 Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook' (2019).
29 Federal Trade Commission, 'Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach' (2019).
30 Federal Trade Commission, 'Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law' (2019).
31 Information Commissioner's Office, 'Intention to fine British Airways £183.39m under GDPR for data breach' (2019).
32 Information Commissioner's Office, 'Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach' (2019).
33 Research interview with U.S. privacy lawyer (2019).
34 Paul Schwartz and Karl-Nikoloaus Peifer, 'Transatlantic Data Privacy' (2017) The Georgetown Law Journal, p. 134.
35 Johnny Ryan and Alan Toner, 'Europe's governments are failing the GDPR' (2020) Brave, p. 3; and Nicholas Vinocur, 'How one country blocks the world on data privacy' (2019) Politico.
36 Matthew Humerick, 'The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?' (2018) Catholic University Journal of Law and Technology, p. 106.
37 Graham Greenleaf, 'Global Data Privacy Laws 2019: 132 National Law & Many Bills' (2019) Privacy Laws & Business International Report.
38 Matthew Humerick, 'The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?' (2018) Catholic University Journal of Law and Technology, p.106.
39 Paul Schwartz, 'Global Data Privacy: The EU Way' (2019) NYU Law Review, p. 803.
40 Lee Bygrave, 'Transatlantic Tensions on Data Privacy' (2013) Transworld Working Paper, p. 12.
41 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. xiv.

Comparison of U.S. and EU data protection systems

U.S. DATA PRIVACY SYSTEM	EU DATA PROTECTION SYSTEM
No constitutional right to data privacy	Privacy and data protection are fundamental rights in EU law
Self-regulation and a laissez faire approach favoured	Regulation, legislation and market intervention favoured
Data privacy laws and frameworks are fragmented and different in each state	Data privacy laws and frameworks are harmonised across EU member states
No comprehensive federal data privacy law covering all economic sectors	The GDPR is comprehensive and covers all economic sectors
FTC enforcement is limited but more robust, as very large fines are common	European DPAs have greater powers but have been reluctant to issue major fines
Organisations can process personal data by default	Organisations can only process personal data if they have a lawful basis



SECTION 2: EU-U.S. Data Flows and the Future of Privacy Shield and SCCs

How does data flow from the EU to non-EU countries?

Entities can transfer data freely from the EU to entities in a non-EU (i.e. third) country if there is an adequacy decision in place. An adequacy decision is the EU's way of 'protecting the rights of its citizens by insisting upon a high standard of data protection in foreign countries where their data is processed'.[42] The European Commission's DG JUST assesses the data protection landscape in third countries. If it is satisfied that the protection of data is sufficiently robust, it issues a unilateral adequacy decision. This is officially adopted following an Opinion by the European Data Protection Board (EDPB) and a qualified majority vote in the Standing Committee of member state representatives. There is no formal role for the European Parliament.

An adequacy decision is economically beneficial as it significantly lowers transaction costs for companies, opening up new business and trade opportunities. Given the high threshold and standards of data protection in the EU, not many countries are recognised as 'adequate'.

There are adequacy decisions for thirteen countries and territories: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the U.S. As will be explained below, the U.S. has a 'partial adequacy' decision.

The criteria for how adequacy decisions are made is outlined in the GDPR (Article 45), the EDPB 'Adequacy Referential'[43] and corresponding CJEU case law. The European Commission assesses the data protection laws and enforcement in the third country. It also looks at wider factors such as the country's judicial system, the rule of law, human rights, defence and national security legislation.[44] This has been controversial, as 'national security remains the sole responsibility of member states' and is not an EU competence.[45] The Commission therefore assesses aspects of third countries for which EU member states retain full independence.

This has led some scholars to question whether all EU member states would pass the adequacy test[46] and argue that it could be morally and politically dubious if the EU is seen to hold third countries to a higher standard than its own member states.[47] This point is of particular interest to the UK, which faces an uphill struggle to attain and retain an adequacy decision, despite the fact that data has flowed freely between the EU and the UK since at least 1995.

The overall system for data protection must be deemed 'essentially equivalent' (although not identical) to the EU's for a positive adequacy decision to be made. This means it should achieve the same level of data protection in practice, albeit with slightly different laws and frameworks. Adequacy decisions are periodically reviewed and can be revoked by the Commission, although this has never happened.

What if there is no adequacy decision?

If there is no adequacy decision in place, data can still flow from entities in the EU to entities in third countries. Most countries, after all, are not deemed 'adequate'. However, data cannot be transferred to any entity, and additional measures – ad hoc safeguards of a legal and administrative nature – must be put in place by individual organisations to facilitate lawful data transfers.

The two main measures are Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). SCCs are template contracts, pre-approved by the European Commission, which must be signed by both entities engaging in an EEA-third country data transfer. Once the contract is in place, data can flow freely, as the entity in the third country has legally committed to a level of data protection which meets EU standards.

BCRs are a legal mechanism, requiring approval from the relevant EU data protection authority (DPA), to facilitate data transfers within a company or group of companies. Once in place, they require the entire organisation or group to adhere to EU-approved data protection standards. They are almost exclusively used by large multinational corporations operating in multiple jurisdictions. SCCs and BCRs are relatively costly and burdensome for organisations to set up, as they require significant administrative and legal work, such as mapping all data flows. Also, SCCs and BCRs cover individual organisations, whereas an adequacy decision covers the entire economy. As such, it is far better for business if there is an adequacy decision, so that no additional compliance burdens are required.

What is the history of EU-U.S. data flows?

The EU has never recognised the U.S. data protection system as adequate. This is partly because of the lack of comprehensive, federal privacy legislation. However, driven by the economic importance of EU-U.S. digital trade, and the data flows which underpin this, the European Commission has been flexible and pragmatic in finding ways to maintain unhindered EU-U.S. data flows.[48] Indeed, the U.S. is the only country without comprehensive privacy laws to have a form of EU adequacy decision.

In 1999, European DPAs argued that "the current patchwork of U.S. laws and self-regulation is not adequate".[49] Nonetheless, in 2000, after two years of negotiation with the U.S., the European Commission issued the Safe Harbour decision.[50] Safe Harbour was a partial adequacy decision. It encompassed a set of data

42 Graham Greenleaf, 'Questioning 'Adequacy' Part II – South Korea' (2018) Privacy Laws & Business International Report, p. 6
43 Article 29 Working Party, 'Adequacy Referential' (2018).
44 General Data Protection Regulation, 'Article 45 Transfers on the basis of an adequacy decision' (Regulation (EU) 2016/679).
45 Treaty on European Union, Article 4.
46 Jan Xavier Dhont, 'Schrems II. The EU adequacy regime in existential crisis?' (2019) Maastricht Journal of European and Comparative Law, p. 599.
47 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal, p. 899.
48 Paul Schwartz, 'Global Data Privacy: The EU Way' (2019) NYU Law Review, p. 786.
49 Paul Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy' (2017) The Georgetown Law Journal, p. 118.
50 Safe Harbour Decision (2000/520/EC).

protection principles which individual firms could sign up to and implement, in exchange for the right to benefit from unrestricted EU-U.S. data transfers. However, it did not entail any changes to U.S. law and it was not a recognition of the U.S. system as adequate. Firms which signed up to Safe Harbour implemented more stringent data protection standards than U.S. law required. This policy innovation meant that certified U.S. companies, and even entire sectors, could enjoy the de facto benefits of an adequacy decision, without there being a full adequacy decision in place.

Although the European Commission hoped that Safe Harbour would result in a spread of European privacy principles among U.S. corporations, there was not much evidence of this. However, Safe Harbour was of tremendous economic benefit to U.S. technology firms, which developed lucrative business models tapping into European markets – predicated on unrestricted EU-U.S. data flows.[51]

Over the years, Safe Harbour was heavily criticised by European DPAs, MEPs and privacy activists, who cited a lack of FTC enforcement and widespread non-compliance with the Safe Harbour principles.[52] Nonetheless, it was a stable arrangement, used by thousands of firms.

In 2012, the European Commission and the U.S. Department of Commerce began to discuss reforming Safe Harbour. The Edward Snowden leaks of May 2013 represented a pivotal moment in the history of EU-U.S. data flows and the transatlantic relationship more broadly. Snowden revealed the mass surveillance programmes of the U.S. National Security Agency (NSA), many of which directly implicated EU citizens. The process of modifying Safe Harbour, which was well underway, now assumed a new dynamic, as the principal EU concern became U.S. government access to EU citizens' data.

In 2013, Max Schrems, an Austrian lawyer, filed a complaint with the Irish Data Protection Commission (DPC) in response to the Snowden leaks, in which he connected Safe Harbour with U.S. mass surveillance. Schrems argued that his Facebook data was not protected when it was transferred to the U.S., as the Snowden files revealed that this data was routinely passed from Facebook to the NSA. The DPC declined to investigate, calling the complaint "frivolous and vexatious".[53] As Facebook was Safe Harbour certified, the DPC claimed there was nothing to investigate. Schrems then appealed, raising the matter to the Irish High Court, which agreed with Schrems and referred the matter to the CJEU.

In the landmark October 2015 'Schrems' judgement, the CJEU invalidated the Safe Harbour decision, arguing that the Commission neglected relevant U.S. national security laws and practices in its adequacy assessment. Furthermore, the CJEU objected to the fact that the Safe Harbour principles were overridden by 'national security and law enforcement requirements', as this could result in violations to Articles 7 and 8 of the EU's Charter (for individuals whose data is transferred from the EU to the U.S.).[54]

Beyond invalidating Safe Harbour, the Schrems judgement was significant for several reasons:

- ◊ It was the first time an EU data adequacy decision was invalidated.
- ◊ It formally established the CJEU as the ultimate arbiter of EU data adequacy decisions.
- ◊ It settled questions on the meaning of adequacy, i.e. that the third country's data protection system must be 'essentially equivalent' to the EU's.
- ◊ It meant that the European Commission would now assess national security and mass surveillance legislation, frameworks and practices when undertaking adequacy assessments.
- ◊ It instructed national DPAs, like the Irish DPC, to investigate issues and complaints even if they concerned 'adequate' countries.

After the Schrems judgement, U.S. and EU companies were very concerned about major disruption to EU-U.S. data flows. However, European DPAs agreed upon a temporary transition period to avoid economic disruption and to enable EU and U.S. negotiators to conclude an alternative agreement. In July 2016, Privacy Shield, Safe Harbour's successor, was agreed and adopted by the EU and the U.S.

Privacy Shield is conceptually similar to Safe Harbour: certified firms adopt higher data protection standards than U.S. law requires, in exchange for unrestricted data flows from entities in the EU. However, there were important changes from Safe Harbour. Privacy Shield has stronger mechanisms for oversight and enforcement, including an independent Privacy Shield Ombudsperson, which was a significant U.S. concession.

The Privacy Shield Ombudsperson is Keith Krach, U.S. Under Secretary of State for Economic Growth, Energy, and the Environment. His role is to manage requests from EU citizens regarding the possible access of their personal data by U.S. intelligence authorities, transferred from the EU via Privacy Shield (or SCCs and BCRs).[55] Privacy Shield also contains additional restrictions on the onward transfer of data from the U.S.

Finally, it was accompanied by various letters, including from the U.S. Office of the Director of National Intelligence (ODNI) which stated that "the intelligence community does not engage in indiscriminate surveillance of anyone, including ordinary European citizens […] U.S. intelligence agencies do not have the legal authority, the resources, the technical capability or the desire to intercept all of the world's communications".[56]

51 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. 135.
52 Ibid.
53 EDRi, 'Europe V Facebook's Irish Complaint Again On The Table' (2013).
54 Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner.

55 U.S. Department of State, 'Privacy Shield Ombudsperson'.
56 Privacy Shield Decision (2016/1250) Annex VI 'Letter from General Counsel Robert Litt'.

Protest against mass surveillance in Washington D.C. (2013).

Why are EU-U.S. data flows important?

It is difficult to know exactly how important EU-U.S. data flows are for the economy as much of the evidence is anecdotal. There is a dearth of economic or empirical research and minimal legal obligations on firms to publicly report on their data transfers. Without this data, establishing the value and importance data flows, and therefore the value and importance of Privacy Shield and other adequacy decisions, is difficult.

Nonetheless, we can infer its importance from proxy indicators and key stakeholder views. The rate of adoption has been very fast, with just over 5300 companies now Privacy Shield certified. Also, many organisations use the services of Privacy Shield certified companies (e.g. cloud service providers).

The U.S. government, European Commission and most member states are extremely keen for Privacy Shield to be upheld, considering it a highly useful mechanism.

The volume of cross-border data flows between the EU and the U.S. is the highest in the world.[57] It is widely agreed that data flows are a crucial factor underpinning digital services trade, which can be measured. However, it is not known exactly what proportion of digital trade is attributable to cross-border data flows.

The EU is the U.S.' largest digital trade partner. Between 2003 and 2017, total EU-U.S. trade increased from $594 billion to $1.2 trillion. In 2017, ICT and potentially ICT-enabled services accounted for approximately $190 billion of U.S. exports to the EU.[58] Furthermore, the U.S. and EU account for nearly half of each other's 'digitally deliverable service exports' (e.g. business, professional and technical services).[59] Finally, in 2016, it was estimated that the EU-U.S. economic relationship involves $260 billion digital services trade per annum.[60]

All of the technology companies and business representatives we interviewed stressed the importance of Privacy Shield and maintaining the status quo. Some examples of how Privacy Shield is used by businesses are:

- Just under 1600 companies (30% of the total) use Privacy Shield to transfer their HR data back to the U.S.[61]
- A software company uses Privacy Shield to transfer crash report data from EU customers to servers in the U.S., where it can be analysed by technicians and customer service agents.
- A B2B company which uses an AI system and data centre in the EU to undertake business analytics for a U.S. client uses Privacy Shield to transfer the data and analytics results to the client's servers in the U.S.
- A major HR and payroll company has clients all over the world, including in the EU, but its operations and data centres are based in the U.S. It uses Privacy Shield so that its clients can transfer HR data for processing in the U.S.
- A scientific research organisation uses Privacy Shield to participate in an EU-based clinical trial.
- ***Video conferencing tools like Zoom, Skype, Google Hangouts and Cisco Webex routinely transfer EU customer data to U.S. servers for processing and analysis using***

57 Congressional Research Service, 'Digital Trade and U.S. Trade Policy' (2017), p. 20.
58 Ibid.
59 Ibid, p. 21.
60 Penny Pritzker and Andrus Ansip 'Making a Difference to the World's Digital Economy: The Transatlantic Partnership' (2016) International Trade Administration Blog.
61 Jeremy Greenberg and Daniel Neally, 'More Than 200 European Companies are Participating in Key EU-US Data Transfer Mechanism' (2019) Future of Privacy Forum.

Privacy Shield. This potentially includes personal data generated by European government and EU officials, who have increasingly used such tools since COVID-19, which has prompted privacy concerns and even calls to use European-headquartered video conferencing companies. [62]

Privacy Shield is beneficial for SMEs and startups, who may lack sufficient resources to set up SCCs or BCRs. Approximately 65% of Privacy Shield certified firms are SMEs. Also, 41% of certified firms have a revenue of below $5 million.[63] They span all economic sectors, including travel, retail, finance and manufacturing.

It is plausible that large companies could manage without Privacy Shield as they have the resources to set up alternative legal arrangements. However, its invalidation would be difficult for SMEs and firms with tighter resources. One startup policy advocate argued that Privacy Shield is a "tool to level the playing field", as it enables startups to benefit from free data flows with the U.S. without significant additional cost, which could be easily absorbed by the larger companies.[64]

The U.S. is generally against restricting data flows and it pushes for unrestricted data flows when negotiating trade agreements. According to its objectives for the UK trade negotiations, the U.S. will seek to 'establish state-of-the-art rules to ensure that the UK does not impose measures that restrict cross-border data flows'.[65] This demonstrates how economically important the U.S. government views the issue, and, as discussed below, has significant implications for the UK in its quest for an EU adequacy decision post-Brexit.

The European Commission also agrees that EU-U.S. data flows are important, which is why it worked hard after Safe Harbour's invalidation to ensure a new arrangement was quickly put in place. Also, the Commission's Digital Single Market strategy emphasises the importance of free data flows for trade.[66] Furthermore, the pursuit of harmonised data protection standards via the 1995 Data Protection Directive was in part driven by the Commission's desire to facilitate free flow of data between member states and strengthen the single market.[67]

Over 200 European headquartered companies also benefit from Privacy Shield and are active participants, including major corporations like Aldi, Louis Vuitton and Dr. August Oetker KG.[68] However, some EU officials are sceptical about just how important Privacy Shield really is. Our interviews revealed a lack of trust between EU officials and U.S. technology companies. U.S. technology companies emphasise the value of Privacy Shield when lobbying the EU, but they do not always have robust economic data to support their claims. They also have a somewhat strained relationship with the EU, where trust is in short supply due to previous developments.

For example, in 2017, Facebook was fined €110 million by the Commission for providing 'incorrect or misleading information' during its acquisition of WhatsApp, which was approved in 2014.[69] There was additional concern when Facebook announced plans to merge all Facebook and WhatsApp user data.[70] Also, in the 2014 Google Spain case on the right to be forgotten, Google argued that obliging search engines to delist entries would be costly and undermine its business model.[71] However, since then, Google has received requests to delist over 3.6 million URLs and it has delisted over 46% of them, reviewing each on a case-by-case basis.[72] It does not appear to have negatively impacted Google's business, with global revenues increasing from $65.6 billion in 2014 to $160.7 billion in 2019.[73]

Such examples demonstrate why the EU does not always trust what the technology giants tell them. Concerted lobbying on the importance of the Privacy Shield is no exception. One senior EU official we interviewed remarked that, ***"Privacy Shield is a big issue, but it's not as important as technology companies make out. There is a mismatch between the rhetoric and the reality".***[74]

62 Vincent Manancourt, 'EU Zooms ahead, despite worries over app' (2020) Politico.
63 James Sullivan, 'The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks: Why They Matter' (2019) International Trade Administration Blog.
64 Research interview with business representative (2019).
65 Office of the United States Trade Representative, 'United States-United Kingdom Negotiations' (2019), p. 6.
66 European Commission, 'A Digital Single Market Strategy for Europe' (2015).
67 Lee Bygrave, 'Transatlantic Tensions on Data Privacy' (2013) Transworld Working Paper, p. 5.
68 Jeremy Greenberg and Daniel Neally, 'More Than 200 European Companies are Participating in Key EU-US Data Transfer Mechanism' (2019) Future of Privacy Forum.
69 European Commission, 'Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover' (2017).
70 Chloe Taylor, 'Facebook's plan to merge messaging services could be barred in the EU' (2019) CNBC.
71 Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
72 Google, 'Requests to delist content under European privacy law' (2020).
73 Statista, 'Annual revenue of Google from 2002 to 2019' (2020).
74 Interview with EU official (2019).

What is the current status of Privacy Shield?

Privacy Shield's future is uncertain. There are ongoing Court cases which threaten its survival and fundamental problems which may never be solved. It is highly plausible that Privacy Shield will be invalidated by the CJEU in the coming months or years.

After the 2015 Schrems judgement, Max Schrems reformulated his complaint to the Irish DPC, which duly investigated. In the new complaint, Schrems argued that the DPC should suspend the SCCs which Facebook uses to transfer data to the U.S. SCCs are an alternative legal mechanism which companies use to transfer data from the EU, often used as alternative or backup to Privacy Shield, in part due to the latter's legal instability. The DPC referred the case to the Irish High Court, taking the position that the entire EU system of SCCs should be invalidated; this goes much further than what Schrems called for.

In its October 2017 judgement, the Irish High Court referred the case, known as 'Schrems II', to the CJEU for a preliminary ruling. In a strongly worded judgement, it argued that the U.S. carries out mass and indiscriminate surveillance which puts EU data subjects at risk of violations to Articles 7 and 8 of the Charter. It also criticised the Privacy Shield Ombudsperson as an ineffective mechanism, claiming that EU citizens do not have access to appropriate legal remedies when their data is transferred to the U.S.[75] Although the case is about the validity of SCCs, it also relates to Privacy Shield, as it concerns personal data that is transferred to the U.S.

The CJEU hearing for the Schrems II case occurred in July 2019, with the U.S. government, Facebook, the European Commission, the Irish DPC, Schrems, several member states, activists and lobby groups all involved. In December 2019, Advocate General Saugmandsgaard Øe issued his formal opinion.

In CJEU cases, Advocate General opinions are advisory, not binding. They precede the final judgement (usually by several months) and the judges can either follow the opinion fully, partially or not at all. CJEU cases are not binary and ascertaining the influence of Advocate General opinions is a difficult endeavour. However, one study found that when the Advocate General proposes the annulment of an act in its opinion, the CJEU is around 67 per cent more likely to decide to annul the act or part of it.[76] This suggests a relatively high degree of influence.

In this instance, the opinion of Advocate General Saugmandsgaard Øe presents us with an insight into the most recent legal thinking from the CJEU on EU-U.S. data flows and Privacy Shield.[77] In the opinion he argued that:

- The EU system of SCCs should not be invalidated. It would be inappropriate to invalidate a global system due to problems with specific third countries or organisations.
- However, EU data exporters or, failing this, member state DPAs, should use their powers to investigate problems and complaints relating to SCCs. If they find that specific SCCs do not adequately protect EU citizens' data, they should suspend the SCCs on a case-by-case basis.
- The CJEU should not use this case to rule on the validity of Privacy Shield. This should wait for the pending case currently before the EU's General Court.

Interestingly, despite arguing that the judges should not rule on Privacy Shield's validity, the Advocate General's opinion contains a wide-ranging and lengthy critique of Privacy Shield, in which he casts serious doubt over its validity and conformity with EU law.

The CJEU judgement will be delivered on 16th July 2020. It is impossible to predict whether the judges, whose decision cannot be appealed, will agree with the Advocate General. If they do agree on the validity of SCCs, this will throw the gauntlet back to the Irish DPC, which will be under pressure to investigate, and potentially invalidate, SCCs used by technology giants like Facebook to transfer data to the U.S. In theory, DPAs have the power to suspend SCCs to an entire jurisdiction, like the U.S. As will be elaborated below, this has significant implications for the UK post-Brexit.

Max Schrems and several EU officials we interviewed suspect that the judges may come down harder on the U.S. than the Advocate General, due to their more critical line of questioning on Privacy Shield during the hearing.[78] If this is correct, then it is plausible that the CJEU could draw on the arguments put forward by the Advocate General and choose to invalidate Privacy Shield. Indeed, in the Irish High Court's 2014 judgement, the CJEU was not explicitly asked to rule on the validity of Safe Harbour, which is what ultimately happened.[79] However, it is equally possible that the CJEU will defer judgement on Privacy Shield until it is explicitly presented to them in a dedicated case.

French digital rights group La Quadrature du Net is pursuing a case (T-738/16) which explicitly concerns the validity of Privacy Shield. It is currently pending in the General Court (the CJEU's lower court). Their complaint is that Privacy Shield violates Article 7 of the Charter and also fails to provide an effective remedy against U.S. wrongdoing, rendering its protection as not 'essentially equivalent' to EU law.

The hearing of the La Quadrature du Net case was originally scheduled for July 2019, but it was postponed pending the conclusion of the Schrems II case. When it resumes, the General Court will have to follow precedents set by the CJEU. Depending on the outcome of the Schrems II case, Privacy Shield could thus potentially be invalidated in the next few months, in the La Quadrature du Net case, in a future CJEU case or perhaps never. Either way, the arguments put forward by Advocate General Saugmandsgaard Øe cast serious doubt over its future.

75 The High Court Commercial, 'The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems. Judgement of Ms. Justice Costello delivered on the 3rd data of October, 2017.'
76 Caros Arrebola et al., 'An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union' (2016) Cambridge Journal of Comparative and International Law.
77 'Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019' (Case C-311/18).
78 NOYB, 'Prep – Background on tomorrow's AG Opinion' (2019).
79 The High Court of Ireland, 'Schrems -v- Data Protection Commissioner' (2014).

Possible scenarios for standard contractual clauses (SCCs) in the CJEU's Schrems II judgement (16th July 2020)

Future of SCCs	Implications
SCCs are invalidated globally *rejection of Advocate General opinion*	This would cause major disruption to EU-third country data flows worldwide and would require the Commission to produce new template contracts, leading to large-scale compliance burdens for firms.
SCCs are upheld, but the CJEU requests amendments or annulments to specific provisions *rejection of Advocate General opinion*	Although the SCC system would be protected, the European Commission would have to amend SCCs, leading to large-scale compliance burdens for firms.
SCCs are upheld, but DPAs are instructed to investigate and suspend them on a case-by-case basis *reflection of Advocate General opinion*	Although the SCC system would be protected, the pressure would be on data exporters, the Irish DPC and other DPAs to investigate U.S. SCCs.
SCCs are upheld with no further comment *partial reflection of Advocate General opinion*	The SCC system is protected and there would be less pressure on data exporters and DPAs to review U.S. SCCs.

Possible scenarios for Privacy Shield in the CJEU's Schrems II judgement (16th July 2020)

Future of Privacy Shield	Implications
Privacy Shield is invalidated *rejection of Advocate General opinion*	This would cause major disruption to EU-U.S. data flows as it is uncertain whether a new agreement could be reached.
Privacy Shield is upheld, with judgement 'deferred' to a later date and concerns on its validity expressed *reflection of Advocate General Opinion*	This would provide stability in the short-term, but other CJEU cases could threaten Privacy Shield's survival. Not ruling on the validity of Privacy Shield could just mean a delay to its invalidation.
Privacy Shield is upheld, but the CJEU requests amendments or annulments to specific provisions *rejection of Advocate General opinion*	EU and U.S. negotiations would ensue, with no certainty of agreement.
Privacy Shield is upheld, with no further comment *partial reflection of Advocate General opinion*	This would be the most stable outcome for EU-U.S. data flows.

What could be the implications of the upcoming Schrems II judgement?

It is unlikely that the CJEU will invalidate both the global system of SCCs and Privacy Shield in its upcoming Schrems II judgement. Both could survive for now, meaning no disruption to EU-U.S. data flows in the short-term.

However, it is not so difficult to map out a path to severe disruption to EU-U.S. data flows in the medium or long-term. Privacy Shield may be invalidated by the CJEU, either in the Schrems II case or the La Quadrature du Net case. Also, the Irish DPC, following an investigation, could suspend all SCCs which facilitate data transfers from Ireland to the U.S., or at least those used by major technology companies like Facebook and Google, which are more susceptible to the security services accessing their data. Furthermore, in an extreme scenario, the European Data Protection Board (EDPB) could review SCCs en masse, and decide to suspend all SCCs used to transfer data from the EU to the U.S.

The original European Commission decision (2001/497/EC) which established SCCs states that DPAs have the power to prohibit or suspend a data transfer or set of transfers based on SCCs where the transfer is likely to have a substantial adverse effect on the data subject's level of protection.[80] The 2004 amendment to this decision (2004/915/EC) stipulates that data exporters must conduct due diligence on data importers when signing SCCs, to ensure that an adequate level of protection exists post-transfer.[81] In essence, the Advocate General's opinion clarified and elaborated on this legal position, thereby encouraging data exporters and DPAs to fulfil their responsibilities and make greater use of their powers, which have thus far been used sparingly. This opinion, especially if followed by the judges, could embolden data subjects and activists, leading to a flurry of complaints to DPAs relating to data transfers based on SCCs. The CJEU could also amend SCCs in a manner which renders complaints and investigations more likely, perhaps by enhancing the due diligence obligations of data exporters.

Some think that the notion of DPAs and data exporters (i.e. companies) being able to robustly assess and determine the level of data protection and fundamental rights of third countries (e.g. the U.S., Russia and China), including their national security systems, is fanciful.[82] Indeed, there has historically been very little DPA enforcement linked to data transfer violations.[83] Nonetheless, this is ostensibly the position in EU law, elaborated by the Advocate General.

The European Commission and their U.S. counterparts have conducted official annual reviews of Privacy Shield in parallel to the legal challenges. Each review has shown a steady increase in Commission satisfaction with Privacy Shield. The appointment of the Privacy Shield Ombudsperson in January 2019 significantly addressed the Commission's outstanding concerns. Following the third annual review in October 2019, the Commission heralded Privacy Shield as a successful framework in ensuring that EU citizens have adequate data protection whilst also facilitating transatlantic data flows.[84]

However, the business community remains very concerned about Privacy Shield's survival.[85] In some of the scenarios, severe disruption to EU-U.S. data flows and digital trade would ensue. In future, without Privacy Shield or SCCs, firms might be left with very few legal mechanisms to transfer data from the EU to the U.S. This would present major headaches and there would be a big push from industry, with lots of pressure on the European Commission, for a solution. Business leaders argue that, ***"there is no Plan B without Privacy Shield or SCCs"***.[86]

If Privacy Shield is invalidated, the political fallout could be great. It is already a rocky period for the transatlantic relationship, with very strong headwinds over issues like Iran, NATO, trade, digital taxation and climate change. A mini crisis over Privacy Shield and data flows would add to these tensions. Various U.S. experts we interviewed predicted that the response from President Trump could be ugly and could even include sanctions or tariffs. One analyst said that there would be "an angry response from the administration", with another claiming that "Trump will be furious".[87]

Crucially, it is unclear whether there would be scope for agreement on a new deal. One U.S. official noted that it would be extremely difficult for the administration to engage in a new negotiation process, as the U.S. has already engaged constructively and made several concessions.[88] As such, further negotiations may not be in its interests. Also, the details of the judgement may restrict the scope for a future deal. However, European Commission officials remain confident they could reach a new deal with the U.S., even in the event of Privacy Shield invalidation.[89]

80 European Commission, 'Commission decision on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC' (2001/497/EC).
81 European Commission, 'Commission decision amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries' (2004/915/EC).
82 W. Scott Blackmer, 'Model Contracts and Privacy Shield: Why the AG Opinion in Schrems II Suggests that Belt and Braces Is a Good Strategy for Data Transfers from the EU' (2019) InfoLawGroup.
83 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal, p. 885.
84 European Commission, 'Report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield' (2019).
85 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. 154.
86 Research interviews with business representatives (2019).
87 Research interviews with U.S. privacy experts.
88 Research interview with U.S. government official (2019).
89 Research interviews with EU officials (2019).

Timeline of EU-U.S. data flows relationship

Date	Event
October 1995	EU adopts the Data Protection Directive (95/46/EC). Imposed restrictions on the transfer of personal data from EU to third countries.
1998 – 2000	EU and U.S. conduct Safe Harbour negotiations.
July 2000	EU-U.S. Safe Harbour framework is adopted.
September 2001	9/11 terrorist attacks reorient U.S. lawmakers away from privacy and towards security.
January 2009	Entry into force of the Lisbon Treaty, which elevates the EU's Charter of Fundamental Rights to Treaty status.
June 2013	NSA whistleblower Edward Snowden releases details of U.S. mass surveillance programmes to the international media.
June 2013	Activist Max Schrems submits a complaint regarding Safe Harbour to the Irish DPC, citing U.S. mass surveillance revealed by Snowden.
June 2014	Irish High Court refers the Schrems case to the CJEU for a preliminary ruling.
October 2015	CJEU invalidates Safe Harbour, in its landmark judgement in the Schrems case.
October 2015	Schrems reformulates his complaint to the Irish DPC, focusing on Facebook's use of SCCs. This begins the Schrems II case.
October 2015 – February 2016	EU and U.S. negotiations on Safe Harbour replacement (Privacy Shield).
July 2016	EU-U.S. Privacy Shield is adopted.
October 2016	French NGO La Quadrature du Net brings a case to the CJEU, claiming that Privacy Shield breaches the EU Charter of Fundamental Rights.
October 2017	Irish High Court refers the Schrems II case to the CJEU for a preliminary ruling.

Timeline of EU-U.S. data flows relationship

Date	Event
October 2017	Privacy Shield passes its first annual review.
November 2017	Digital Rights Ireland Privacy Shield case ruled inadmissible by the CJEU.
May 2018	The GDPR enters into force, strengthening and harmonising EU data protection standards.
July 2018	European Parliament votes to suspend Privacy Shield (in a non-binding resolution).
December 2018	Privacy Shield passes its second annual review.
January 2019	Keith Krach is appointed as Privacy Shield Ombudsperson.
July 2019	La Quadrature du Net Privacy Shield case suspended to allow resolution of Schrems II case.
July 2019	CJEU hearing in the Schrems II case.
October 2019	Privacy Shield passes its third annual review.
December 2019	CJEU Advocate General issues opinion in Schrems II case, upholding validity of SCCs but casting doubt over validity of Privacy Shield.
January 2020	The California Consumer Privacy Act enters into force.
16 July 2020	Final CJEU judgement in the Schrems II case.
Unknown	Hearing and final CJEU judgement in the La Quadrature du Net case.
Uncertain	Irish DPC and other DPA investigations into SCCs used by U.S. firms (e.g. Facebook)?
Uncertain	Congress one day adopts comprehensive, federal U.S. privacy law?

Penny Pritzker (Former United States Secretary of Commerce) and Věra Jourová (Vice President of the European Commission for Values and Transparency) joint press conference following the adoption of Privacy Shield (July 2016). mage credit: epa-efe / Olivier Hoslet

Věra Jourová and Dimitris Avramopoulos press conference following Privacy Shield annual review (2018). Image credit: epa-efe / Stephanie Lecocq

What is the fundamental problem for EU-U.S. data flows?

Although the scenarios of disruption and political fallout outlined above sound extreme, they are plausible because of the fundamental problem which permeates this issue: ***a clash between U.S. national security and surveillance laws and practices on the one hand, and EU data protection standards and fundamental rights on the other.*** This problem contributed to the invalidation of Safe Harbour. It is also the reason for the Advocate General's strong critique of Privacy Shield and why it could be invalidated by the CJEU in future.

The importance of the Snowden revelations cannot be overstated. In highlighting how Safe Harbour enabled mass surveillance of EU citizens, it exposed this fundamental problem and brought it to the fore of the EU's thinking.[90] The information was also used by Schrems and La Quadrature du Net to pursue strategic litigation. One U.S. government official described Snowden as "a bombshell moment […] we had to explain to the EU the rigorous and multi-layered oversight framework that protects the privacy of U.S. and non-U.S. persons information under national security authorities. It was a steep learning curve for the European Commission, who were understandably not experts on these protections."[91]

Privacy Shield does contain compromises and concessions from the U.S., such as the Ombudsperson, which go some way towards defending EU principles. Law firm Hogan Lovells argue that the 'significant' changes means that the Privacy Shield framework does provide 'essentially equivalent' protection of personal data when transferred to the U.S.[92] And it is certainly impressive that the EU was able to persuade the U.S. to publicly commit to limit mass surveillance (in the Privacy Shield letters).

However, the Privacy Shield framework did not entail or require any changes to U.S. national security, surveillance or data privacy legislation, and the U.S. government is not subject to the Privacy Shield framework. Although it strengthens the data protection principles which certified U.S. firms have to adhere to and provides for stronger oversight and enforcement of this compliance, it does not stop the NSA or other U.S. intelligence agencies from conducting surveillance on EU citizens in a way which violates EU law. The fundamental problem of U.S. government access to EU citizens' data has thus not been fully resolved – indeed, the positions may remain irreconcilable.

This is why various key actors, like the European Parliament, its Civil Liberties (LIBE) Committee, the EDPB,[93] European Data Protection Supervisor (EDPS) and prominent digital rights groups and privacy activists are against, or highly critical of, Privacy Shield. In July 2018, the European Parliament voted (in a non-binding vote) to suspend Privacy Shield, citing concerns with U.S. mass surveillance and the lack of effective remedies for EU citizens.[94] LIBE Committee MEPs recently reiterated these concerns after a 'fact-finding' mission to the US.[95]

The same problem applies if personal data is transferred to the U.S. via SCCs or BCRs. These mechanisms all impose obligations on data processors and controllers, but they cannot prevent the U.S. government from accessing this data. As one lawyer put it, ***"neither SCCs nor BCRs were designed to stop third country law enforcement from accessing data […] U.S. companies cannot provide protection from state power"***.[96]

Indeed, many experts agreed that it would not make sense to invalidate Privacy Shield while permitting data transfers via SCCs. The fundamental problem remains; once the data is in U.S. the firms must comply with U.S. national security laws. Transferred data is not protected from state mass surveillance, irrespective of the legal transfer mechanism. Kuner agrees, arguing that it is a legal fiction to imagine that procedural mechanisms, like Privacy Shield, other adequacy decisions or SCCs, can actually protect data and fundamental rights in practice, as they cannot provide protection against foreign governments' surveillance and intelligence gathering activities.[97]

On this note, it is reasonable to argue that companies which are most affected by U.S. mass surveillance law and intelligence gathering – 'electronic communications service providers' like Google, Facebook, Microsoft and Yahoo, as well as major ISPs – are more likely to have their SCCs investigated and suspended, as it may be considered more likely that US government agencies will access personal communications data they hold on EU citizens.[98]

This is why it is plausible that severe disruption to EU-U.S. data flows could ensue in future. The CJEU, national DPAs and the EDPB may take measures to invalidate both Privacy Shield and SCCs used for EU-U.S. transfers, if it is concluded that EU citizens' data is insufficiently protected in the U.S. This is not what the European Commission, EU member states or U.S. government want, but it could be out of their hands.

The CJEU is the ultimate arbiter of all EU data transfer decisions. The available evidence, including the relevant case law (outlined below), as well as Advocate General Saugmandsgaard Øe's opinion in Schrems II, suggests that the Court takes a dimmer view of the U.S. national security system than does the European Commission. And the U.S. is not going to amend and weaken its national security laws in order to preserve data flows and digital trade with the EU.

The big picture is that the GDPR, which outlines the data transfer mechanisms, is superseded by the Charter, and the CJEU has consistently prioritised the rights to privacy and data protection over the economic value of data flows. As one EU official argued "depending on how deep the judges want to go, there is a risk that their concerns with U.S. mass surveillance may lead to significant disruption to EU-U.S. data flows".[99]

90 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. 142.
91 Research interview with U.S. government official (2019).
92 Hogan Lovells, 'Legal Analysis of the EU-U.S. Privacy Shield' (2016), p. 3.
93 EDPB, 'EU-U.S. Privacy Shield – Third Annual Joint Review' (2019).
94 European Parliament, 'European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield' (2018/2645(RSP)).
95 Elena Sanchez Nicolas, 'MEPs: 'Mass surveillance' still possible under US privacy deal' (2019) EU Observer.
96 Research interview with European privacy lawyer (2019).
97 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal, p. 885.
98 NOYB, 'CJEU – AG Opinion, First Statement' (2019).
99 Research interview with EU official (2019).

How does EU data protection and fundamental rights law clash with U.S. national security and mass surveillance?

EU fundamental rights and data protection: relevant legal instruments and cases

These legal instruments and cases should be carefully considered by anyone seeking to understand what factors are at play when the European Commission assesses a country for adequacy (including the UK) or when adequacy decisions are reviewed by the CJEU (e.g. Privacy Shield or a future UK adequacy decision).

Legal instrument	Key aspects	Significance
Charter of Fundamental Rights of the European Union (the Charter)	Article 7: Respect for private and family life Article 8: Protection of personal data Article 52: Scope and interpretation (i.e. interpreting limitations on the Charter's rights and freedoms).	The Charter has the same legal status as EU treaties (i.e. the highest under EU law). Privacy and data protection are fundamental rights, but they are not absolute rights. Rather, they are balanced against other fundamental rights, with the CJEU using Article 52 to undertake 'proportionality tests' in its judgements. For example, Article 6 of the Charter establishes a right to 'security', which can override a right to privacy.
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679	Chapter 5, Articles 44-50: Transfers of personal data to third countries or international organisations	The GDPR is the comprehensive legislation which harmonises data protection standards across the EU. However, personal data processed for the purposes of law enforcement and safeguarding national security is outside the GDPR's scope.
European Convention on Human Rights (ECHR)	Article 8: Right to respect for private and family life	Article 6(3) of the Treaty on European Union stipulates that fundamental rights recognised by the ECHR constitute general principles of EU law. The Convention is upheld by the European Court of Human Rights (EctHR), which is not an EU institution. However, the CJEU draws on the Convention in its rulings. The EctHR also applies a proportionality test and has been more lenient than the CJEU when ruling on mass surveillance.
e-Privacy Directive Directive 2002/58/EC	Article 15(1): Member States may restrict the scope of the rights and obligations provided for in the Directive (Articles 5-9) when such restriction constitutes a necessary, appropriate and proportionate measure to safeguard national security and the fighting of criminal offences.	The 2002 Directive, which was amended in 2009, complements the GDPR with specific rights and rules for electronic communications. In 2017, the Commission published its proposal for an e-Privacy Regulation, to replace the Directive. Its progress is currently stalled due to member state disagreement.

Case (past / ongoing)	Key aspects	Significance
Digital Rights Ireland, 2014 Joined cases C-293/12 and C-594/12	CJEU judgement invalidating the EU's Data Retention Directive 2006 and establishing which safeguards and limitations are required for data retention (i.e. mass surveillance) legislation.	CJEU invalidated the Data Retention Directive due to 'wide-ranging' and 'particularly serious' interferences with Articles 7 and 8 of the Charter. The CJEU argued that the generalised manner of data retention, and lack of procedural safeguards, exceeded the limits of proportionality and what is strictly necessary for fighting serious crime.
Schrems, 2015 Case C-362/14	CJEU judgement invalidating Safe Harbour decision and establishing CJEU as ultimate arbiter of EU data transfer decisions.	Safe Harbour was invalidated in part because the Commission adequacy decision specified that U.S. law enforcement and national security requirements have primacy over the Safe Harbour principles, which could lead to fundamental rights violations.
Tele2 Sverige/Watson, 2016 Joined Cases C-203/15 and C-698/15	CJEU judgement which interpreted the e-Privacy Directive, outlawed blanket data retention legislation and deemed the UK's 2014 Data Retention and Investigatory Powers Act (DRIPA) as unlawful.[100]	Building on the Digital Rights Ireland judgement, the CJEU ruled that national legislation establishing general and indiscriminate retention of personal data, for the purpose of fighting crime, violates Articles 7 and 8 of the Charter. It also specified which minimum safeguards and procedural conditions need to accompany such legislation, noting that the objective must be to fight 'serious crime' and prior review by an independent authority (e.g. court) is required.
Ministerio Fiscal, 2018 Case C-207/16	Very narrow case in scope, which established CJEU case law on when specific retained data can be accessed by law enforcement authorities.	CJEU ruled that the access of law enforcement authorities to personal data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone is permissible for the objective of fighting crime. This was criticised as potentially weakening the Tele2/ Watson judgement conditions.[101]
Schrems II, 2020 Case C-311/18	CJEU case on the validity of SCCs, which is also linked to Privacy Shield. Awaiting final judgement following Advocate General Saugmandsgaard Øe's opinion in December 2019.	The CJEU may invalidate Privacy Shield in its final judgement in July 2020. The Advocate General expressed severe doubts about the validity of Privacy Shield in his opinion.
Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others Case C-623/17	CJEU case on the UK security and intelligence agencies acquisition and use of bulk communications data. Awaiting final judgement following Advocate General Campos Sánchez-Bordona's opinion in January 2020.[102]	In his opinion, the Advocate General expressed doubts as to whether UK legislation is lawful and argues that the UK should comply with the conditions established in the Tele2 Sverige/Watson judgement.
La Quadrature du Net Case T-738/16	CJEU (General Court) case on the validity of Privacy Shield. The hearing has yet to occur.	Privacy Shield could be invalidated by the CJEU in this case.

100 Orla Lynskey, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change' (2017) European Law Blog.
101 EDRi, 'CJEU introduces new criteria for law enforcement to access to data' (2018).
102 CJEU, 'Opinion of Advocate General Campos Sanchez-Bordona delivered on 15 January 2020' (Case C623/17).

In the case law, the CJEU has maintained a consistent position on the retention of and government access to personal data (i.e. mass surveillance). Below are the key principles which will be taken into account when the CJEU assesses Privacy Shield and when the Commission (and potentially the CJEU) assesses the UK for data adequacy.

- Legislation authorising the collection and retention of personal data, for the purposes of combating serious crime and protecting national security, is not necessarily unlawful.
- However, legislation which permits the public authorities to collect, and have access to, in a 'generalised and indiscriminate' manner, the content of electronic communications, violates Article 7 of the EU Charter.
- For there to be an interference with this fundamental right, it does not matter whether the personal data in question is sensitive. It also does not matter whether the affected individuals were inconvenienced, harmed or suffered any other adverse consequences.[103]
- EU legislation which interferes with Articles 7 and 8 of the Charter must be limited to what is 'strictly necessary' for the legitimate objective at hand (e.g. fighting terrorism), which should be specified using objective criteria. It must stipulate clear and precise rules governing its scope and application (e.g. under what circumstances can personal data be collected, what can it be used for, who can access it and when must it be deleted).[104]
- The need for these minimum safeguards is greater where personal data is automatically processed and where there is a significant risk of unlawful access to that data.[105]
- Such legislation must give individuals the possibility to pursue effective legal remedies before an independent and impartial tribunal, for example to request access to their personal data, or to secure the rectification or erasure of this data.
- There must also be robust and independent oversight mechanisms.

Court of Justice of the European Union

103 'Judgment of the Court (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.' (Joined Cases C293/12 and C594/12.)

104 Ibid.
105 Ibid.

U.S. National Security: relevant legal instruments, intelligence programmes and oversight mechanisms

Legal instrument, programme or oversight mechanism	Purpose and significance
Foreign Intelligence Surveillance Act 1978 (FISA)	Federal law which establishes procedures for the physical and electronic surveillance and collection of 'foreign intelligence information' (i.e. not just for national security purposes). Under **Section 702 of FISA**, the intelligence community can conduct mass surveillance, including foreign intelligence from non-Americans located outside the U.S.[106] Provides the legal basis for PRISM and Upstream programmes and compels U.S. internet and technology companies to assist law enforcement and intelligence agencies. A six-year extension to Section 702 was approved in January 2018 and its current authorisation expires in December 2023.[107]
Executive Order 12333 (EO 12333)	The primary authority under which the NSA gathers foreign intelligence.[108] Signed by President Regan in 1981, it 'established broad new surveillance authorities for the intelligence community, outside the scope of public law'.[109] EO 12333 is the legal basis of NSA surveillance for a wide range of purposes.
Patriot Act (2001)	Federal law, passed in response to the 9/11 terrorist attacks, which enhances the powers and investigatory tools of law enforcement agencies. Reformed by the **USA Freedom Act 2015**. **Section 215**, which provides a lawful basis for some forms of mass surveillance, is currently up for 'renewal'. The House and Senate have both recently voted for an extension, albeit with amendments which are now being reviewed.[110]
CLOUD Act (2018)	Federal law which allows law enforcement agencies to obtain data from U.S. technology companies, regardless of where the data is stored globally. Amends the Stored Communications Act (SCA, 1986).
PRISM	Secret NSA surveillance programme, revealed by Edward Snowden, which collects communications data (content and metadata) from U.S. internet companies. Operated under Section 702 of FISA.
Upstream collection	NSA programme for intercepting telephone and internet traffic from the 'internet backbone' (i.e. major domestic and foreign internet cables and switches), with the help of telecommunications companies.
Five Eyes (FVEY)	Intelligence sharing alliance between Australia, Canada, New Zealand, U.S. and UK.

106 EFF, 'Decoding 702: What is Section 702?' (2019).
107 Andrew Liptak, 'President Donald Trump has signed the FISA reauthorization bill' (2018) The Verge.
108 Ashley Gorski, 'Summary of U.S. Foreign Intelligence Surveillance Law, Practice, Remedies, and Oversight' (2018) ACLU, p. 19.
109 Electronic Privacy Information Center, 'Executive Order 12333' (2019).
110 Martin Matishak, 'Senate passes FISA renewal bill, sends it back to the House' (2020) Politico.

Legal instrument, programme or oversight mechanism	Purpose and significance
Presidential Policy Directive 28 (PPD28)	Post-Snowden, President Obama extended certain privacy protections to non-U.S. citizens when subject to foreign intelligence surveillance. PPD28 therefore imposes some constraints on surveillance and the intelligence community, noting that collection of signals intelligence must be authorised by statute or Presidential authorisation.[111]
Foreign Intelligence Surveillance Court (FISA Court)	Court which oversees requests for surveillance warrants by federal law enforcement and intelligence agencies (e.g. NSA and FBI).
Privacy and Civil Liberties Oversight Board (PCLOB)	Independent agency which reviews and analyses U.S. national security programmes, laws and policies to ensure that privacy and civil liberties are considered and protected.[112]

111 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. 144.
112 The Privacy and Civil Liberties Oversight Board (2020).

Various influential EU actors cast doubt as to whether the U.S. national security and mass surveillance system is compatible with the principles of EU law outlined above. The core concern is on government (i.e. security services) access to EU citizens' personal data and a lack of effective legal remedies. Specifically, both the European Parliament and the EDPB have raised concerns that the mass surveillance conducted under both Section 702 of FISA and EO 12333 is indiscriminate and generalised, which is incompatible with EU law.[113] The American Civil Liberties Union (ACLU) also claims that under Section 702 and EO 12333, 'the U.S. obtains generalized access to the content of E.U.–U.S. communications.'[114]

Although Section 702 surveillance is based on 'minimisation' and targeting procedures, whereby the NSA only conducts surveillance on specific targets filtered via 'selectors' (e.g. email addresses), the ACLU argues that this safeguard is insufficient to prevent abuse of fundamental rights. For example, it notes that the 'selectors' are designed to prevent US citizens' communication from being unjustifiably monitored, not to protect non-US citizens' communication. Also, the personal data of individuals who are not being specifically targeted is incidentally captured. As such, Section 702 permits the targeting of any non-US person – with a very low threshold – according to the ACLU. [115] The European Parliament and the EDPB raise similar concerns.

The European Parliament and the EDPB also argue that the legal remedies which EU citizens have to seek redress for any violations relating to U.S. mass surveillance remain inadequate, despite the Ombudsperson. The Parliament's resolution states that non-US citizens face 'persistent obstacles' in seeking legal redress.[116] The EDPB notes that the U.S. constitutional requirements for 'standing' means redress is 'yet to be effectively guaranteed'.[117]

The European Commission does not share these concerns. It believes that the use of 'selectors' for targeted surveillance is sufficient to protect fundamental rights. A senior Commission official noted that 'FISA explicitly excludes bulk collection' and defended the 'selector' filtering system.[118] The Commission also did not highlight any major issues with U.S. mass surveillance in the 2019 Privacy Shield Annual Review and praised oversight mechanisms like the PCLOB.[119] It is fair to say that on the matter of Privacy Shield and the 'essential equivalence' of the U.S. national security system with EU law, there is major disagreement between the European Parliament and the European Commission.

The Advocate General's December 2019 opinion in Schrems II offered a comprehensive assessment of Privacy Shield and the conformity of the U.S. national security system with EU law. He also raised serious concerns, arguing that surveillance conducted

113 European Parliament, 'European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield' (2018/2645(RSP)).
114 Ashley Gorski, 'Summary of U.S. Foreign Intelligence Surveillance Law, Practice, Remedies, and Oversight' (2018) ACLU, p. 3.
115 Ashley Gorski, 'Summary of U.S. Foreign Intelligence Surveillance Law, Practice, Remedies, and Oversight' (2018) ACLU, pp. 12-17.
116 European Parliament, 'European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield' (2018/2645(RSP)).
117 EDPB, 'EU-U.S. Privacy Shield – Third Annual Joint Review' (2019), p. 20.
118 Jennifer Baker, 'EU Parliament debates: Could California be considered 'adequate' on its own?' (2020) IAPP.
119 European Commission, 'Report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield' (2019), p. 6.

under Section 702 of FISA and EO 12333 violates both the Charter and the ECHR. Specifically, he criticised the 'selector' filtering system, arguing that the safeguards in U.S. law are not 'essentially equivalent' to the requirements of EU law, as their imprecise nature gives rise to risk for government abuse. He also argued that the available legal remedies, for EU citizens' whose data is transferred to the US, are ineffective and not 'essentially equivalent' to those provided under EU law, which also violates the Charter.

The Advocate General concluded by stating that he entertained doubts as to the conformity of Privacy Shield with EU law and the ECHR.[120] Although the U.S. could revoke Section 702 of FISA when it is up for re-authorisation in 2023, this seems unlikely. If, as seems highly likely, the CJEU continues to uphold fundamental rights and 'unilaterally assert EU values',[121] while the U.S. is unwilling to substantively reform its national security and surveillance laws, this could prove to be an intractable problem for EU-U.S. data flows, with considerable economic consequences. In 2012, Kuner argued that there is 'no clear solution' to such conflicts; this remains true today.[122]

This could also become an intractable and serious problem for the UK post-Brexit.

Headquarters of the NSA at Fort Meade, Maryland.

Image credit: Wikimedia

120 It is beyond the scope of this report to assess whether an invalidation of Privacy Shield would be legitimate, only to highlight the serious prospect of Privacy Shield invalidation.
121 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal, p. 917.
122 Christopher Kuner, 'Transborder Data Flows and Data Privacy Law' (2013) Oxford University Press, p. 138.

Are there any alternative solutions for EU-U.S. data flows?

If this fundamental problem cannot be resolved, then there are few good options. For example, there are several derogations in the GDPR (Article 49) which can be used if there is no adequacy decision or alternative safeguards like SCCs or BCRs. These include provisions such as obtaining the consent of data subjects for data transfers, transfers for important public interest reasons (e.g. developing a COVID-19 vaccine) and transfers to protect the vital interests of data subjects. These narrow derogations, which must be interpreted restrictively and mainly relate to 'occasional and non-repetitive' data transfers, are no replacement for the large-scale and systematic data flows facilitated by adequacy decisions like Privacy Shield and SCCs – which are built into the core functioning of the modern transatlantic economy.[123]

The last resort is probably increased data localisation. This simply means that data is processed and stored in the EU, instead of being transferred to the U.S. This is technically possible, but would impose additional costs and burdens on businesses, who prefer to streamline data processing in fewer data centres and locations (as evidenced by the 5300+ Privacy Shield certified firms). It will also make it harder for SMEs and startups to conduct transatlantic digital trade and could discourage U.S. companies from investing and operating in the EU.

Nonetheless, there is already evidence that U.S. technology firms are preparing for this. U.S. firms have been investing heavily in European data centres for several years[124] and this has continued unabated, with Google announcing plans in 2019 to invest $3.3 billion in European data centres.[125] As discussed above, we do not know exactly how costly disruption to EU-U.S. data flows and a shift to data localisation would be, but it would certainly have significant economic consequences. Although it is rather unrealistic to imagine a halt to transatlantic data flows and a major shift to data localisation, not least given the popularity of U.S. internet services.[126] One has to consider the possibility that data transfers would merely continue – even without appropriate legal mechanisms – with firms opting to take the risk of GDPR enforcement action. Minimal empirical research has been done on this point.

Furthermore, not even EU-based data localisation ensures that the U.S. government cannot access data, as the CLOUD Act 2018 gives US law enforcement agencies extra-territorial powers, enabling them to access 'electronically-stored communications data located outside the U.S. provided that the information sought is relevant and material to an ongoing criminal investigation'.[127]

The CLOUD Act applies to any 'service provider' subject to U.S. jurisdiction, although the scope of its applicability remains unclear. The EDPB has acknowledged that the CLOUD Act will result in a 'conflict of laws' for organisations processing EU citizens' data and also subject to U.S. jurisdiction, unless there is a legal basis under EU law for the requested data transfer to the U.S. authorities (e.g. a GDPR Article 49 derogation).[128] Christakis argues that this conflict of U.S. and EU laws places internet and telecommunications companies in a 'particularly uncomfortable position',[129] with the International Chamber of Commerce echoing similar sentiments.[130] In the coming years we will see how this issue plays out; it may yet be partially solved by an EU-U.S. agreement on law enforcement data transfers.[131]

Finally, a relevant question is whether a U.S. state, like California, could be granted EU adequacy status. This is legally possible, as the GDPR (Article 45) states that adequacy decisions can be granted to third countries, territories, specified sectors within third countries and international organisations. The European Commission also confirmed that this is theoretically possible.[132] However, it is highly unlikely that California will be granted adequacy status. Not least because the state has no data privacy authority, remains subject to U.S. federal law and could not prevent onward transfer of data to other U.S. states.[133] Nonetheless, this question is clearly of interest, as demonstrated by a report from South Carolina's Deputy Chief Privacy Officer which analyses whether the state could attain EU adequacy.[134]

Will California be granted EU adequacy status?

Image credit: Photo by Maarten van den Heuvel on Unsplash

123 DLA Piper, 'Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield?' (2019).
124 Sam Schechner, 'EU Sees U.S. Firms Building More Data Centers in Europe' (2014) The Wall Street Journal.
125 Ron Miller, 'Google is investing $3.3B to build clean data centers in Europe' (2019) TechCrunch.
126 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal, p. 914.
127 Caitlin Potratz Metcalf and Peter Church, 'U.S. CLOUD Act and GDPR – Is the cloud still safe?' (2019) Linklaters.
128 EDPS and EDPB, 'ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence' (2019).
129 Theodore Christakis, 'Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?' (2019), p. 15.
130 International Chamber of Commerce, 'Cross-border law enforcement access to company data – current issues under data protection and privacy law' (2012).
131 European Commission, 'Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence' (2019).
132 Jennifer Baker, 'EU Parliament debates: Could California be considered 'adequate' on its own?' (2020) IAPP.
133 Jennifer Baker, 'California Dreamin': Is a Single State EU Data Protection Deal on the Cards?' (2020).
134 Alexander McD. White, 'South Carolina 'Adequacy' with the European Union' (2019).

SECTION 3
EU-UK Data Flows post-Brexit: Lessons and implications

When Brexit happened on 31 January 2020 the UK became a third country under EU law. However, during the transition period, the UK continues to follow EU law and EU-UK cooperation remains unchanged. As such, personal data continues to flow freely between the EU and the UK. This will change as soon as the transition period ends on 31 December 2020. An extension to the transition period for up to two years is possible, but at the time of writing the UK government insists that it will neither request nor accept an extension.[135]

Both sides have committed to pursuing an adequacy decision for the UK. The European Commission will conduct the adequacy assessments during the transition period, but there is no guarantee of a positive decision. Whether or not the UK is granted adequacy will have a significant impact on the UK (and European) economy, especially the services sector (e.g. digital technology and finance).[136]

The negotiations on data adequacy have begun in earnest. In March 2020, the UK government published a series of policy documents, setting out its case for EU data adequacy. This pack of documents, titled the 'Explanatory Framework for Adequacy Discussions', covers a wide range of topics, from the role and effectiveness of the ICO, to the ways in which the UK meets the criteria of the EDPB's 'adequacy referential'. The European Commission's slide deck on 'Personal data protection (adequacy decisions)', published in January 2020, is not as detailed.

The long and unresolved struggle over EU-U.S. data flows is an instructive case study when considering EU-UK data flows post-Brexit. There are many lessons to be learnt, as well as important direct implications for the UK in its quest for adequacy. The key point is that the EU-UK data flows relationship will be complex, messy and could remain unresolved even many years from now, due to similar issues which permeate the EU-U.S. relationship. Policy makers, businesses and data protection practitioners should expect a rocky few years ahead.

8 Key Lessons

1. The European Commission is likely to grant the UK an adequacy decision

Although data has always flowed freely between the EU and the UK, the UK follows the GDPR and the ICO is a respected and leading European DPA, there are several reasons why an adequacy decision may not be granted. Detailed elaboration of these arguments can be found elsewhere.[137] However the main points concern the:

- Potential incompatibility of the UK's Investigatory Powers Act 2016 with EU fundamental rights law;
- derogations from the GDPR in the UK's Data Protection Act 2018 (i.e. on processing data for immigration control);
- onward data transfers to the U.S. and countries without EU adequacy decisions;
- no fundamental right to data protection in the UK post-Brexit, as the UK is not retaining the EU Charter and may pull out of the European Convention on Human Rights (ECHR).

Despite this, and contrary to much commentary, it is highly plausible that the Commission will grant the UK an adequacy decision. The EU-U.S. data flows dispute has demonstrated that the Commission acts in a flexible and pragmatic way in order to preserve unrestricted data flows with an important economic partner, even if its data protection and security landscape is dubious.[138] It also takes a more positive view of the U.S. national security and mass surveillance system than other EU actors such as the Parliament, the EDPB and potentially the CJEU. Analysis of the Commission's stance in the conflict over passenger name records (PNR), which resulted in the controversial U.S.-EU PNR agreement, further highlights this point.[139]

Furthermore, the haste at which Privacy Shield negotiations were concluded following the invalidation of Safe Harbour shows how quickly the Commission can move on this issue. In January 2020, the Commission committed to endeavouring to finalise the adequacy assessment by the end of 2020.[140] As such, despite the time constraints and well documented concerns with the UK, it is highly plausible that it will receive an adequacy decision from the Commission before the end of the transition period (or perhaps shortly after). This then needs to be approved by member state representatives (by qualified majority vote) in the relevant Standing Committee and the EDPB issues a formal opinion. As with other aspects of the Brexit process, it is likely that the Commission will remain in step with the member states.[141]

It is possible, however, that the UK will receive a partial adequacy decision, similar to Privacy Shield. This would be a downgrade from the current situation and would negatively impact the UK economy, as it would only cover certified firms and would entail increased compliance burdens and business costs.

135 BBC News, 'Brexit: UK will refuse any transition extension request' (2020).
136 techUK 'No Interruptions: Options for the Future UK EU data-sharing relationship' (2017).
137 Oliver Patel and Nathan Lea 'EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?' (2019) UCL European Institute, pp. 9-11; and Andrew D. Murray, 'Data transfers between the EU and UK post Brexit?' (2017) International Data Privacy Law.

138 Paul Schwartz, 'Global Data Privacy: The EU Way' (2019) NYU Law Review, p. 786.
139 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, pp. 69-94.
140 European Commission, 'Internal EU27 preparatory discussions on the future relationship: Personal data protection (adequacy decisions); Cooperation and equivalence in financial services' (2020), p. 17.
141 Oliver Patel, 'The EU and the Brexit Negotiations: Institutions, Strategies and Objectives' (2018) UCL European Institute, pp. 7-8.

Also, while adequacy decisions must be periodically reviewed once every four years, Privacy Shield must be reviewed annually. Both timelines are plausible for any UK adequacy decision, but an annual review would be more likely if it is a partial (and hence more controversial) decision.

There are two caveats to this analysis. Firstly, the judgement in the Schrems II case or the La Quadrature du Net case could tie the Commission's hands, making it virtually impossible for the UK to receive an adequacy decision without making significant reforms. Secondly, if there is a breakdown in the EU-UK negotiations, the relationship turns sour and no-deal is pursued, then the Commission will not grant the UK an adequacy decision.

2. Any UK adequacy decision will face significant and multiple legal challenges

Both Safe Harbour and Privacy Shield have been challenged on multiple legal fronts. The 2015 Schrems case brought down Safe Harbour and the 2020 Schrems II case could yet bring down Privacy Shield. Even if the UK attains an adequacy decision from the Commission, it will also be very likely to face extensive legal challenges.

One implication of the Schrems judgement is that EU DPAs are obliged to investigate cases relating to jurisdictions covered by adequacy decisions. A member state DPA can then refer the case to a national court, which in turn can refer the case to the CJEU.

There are various organisations which pursue strategic litigation to uphold data protection standards, and many of these have challenged both the U.S. adequacy decisions and UK mass surveillance laws. These organisations include NOYB (led by Max Schrems), La Quadrature du Net, Privacy International, Big Brother Watch and Digital Rights Ireland, to name but a few.

These actors will view any UK adequacy decision as a weakening of EU data protection and fundamental rights standards and will immediately seek to invalidate it. Any legal challenge could take many years to conclude. In that time, EU-UK data flows would remain unrestricted but would be shrouded over clouds of uncertainty, just as EU-U.S. data flows currently are.

3. The CJEU could invalidate a UK adequacy decision

Given the likelihood of legal challenges should the Commission grant the UK an adequacy decision, it is plausible that at least one case will end up being referred to the CJEU by a member state court.

Unlike the Commission, the CJEU has not thus far prioritised the economic importance of unrestricted data flows in its rulings. It will primarily assess whether there is a risk of EU citizens' fundamental rights to privacy and data protection being violated when their personal data is transferred to the UK under any adequacy decision.

The established CJEU case law in Schrems and Schrems II, and other cases like Tele2 Sverige/Watson, will inform any future judgement. As elaborated above, the case law is consistent and well established in this domain and the CJEU will not diverge from its core tenets. This does not bode particularly well for the UK.[142] As one EU official told us, ***"for the UK the big question is not whether it will get adequacy, but whether any adequacy decision would stand up in Court"***.[143]

It is beyond the scope of this report to fully assess whether or not the UK's national security and surveillance legislation is in conformity with EU law. However, only a cursory analysis of the EU-U.S. data flows dispute illustrates that CJEU invalidation is a serious possibility. Virtually all lawyers, business leaders and policy makers we interviewed agreed on this point.

4. A UK adequacy decision would be an unstable arrangement and organisations would use backup options

Because of this legal uncertainty – which could last for years – any UK adequacy decision would be a relatively unstable arrangement, just like Privacy Shield.

The permanent threat of invalidation will encourage many organisations which engage in EU-UK data transfers to take a different approach and use SCCs or BCRs, even if there is an adequacy decision. Some large organisations which engage in EU-U.S. data transfers do not actually use Privacy Shield as it is viewed as too unstable. Indeed, many organisations set up SCCs or BCRs to cover EU-U.S. data transfers after Safe Harbour was invalidated, as there was uncertainty about what would replace it.

One IT firm, for example, does not use Privacy Shield to transfer data from the EU to the U.S., as many European corporate customers "do not like or trust Privacy Shield".[144] Instead, it opts to use SCCs, even though this is more burdensome and expensive, and requires a specific SCC to be drafted for each point-to-point data transfer (of which there are many). It also prefers SCCs because complaints can be more effectively raised with European DPAs, instead of relying on U.S. Privacy Shield enforcement.

Similarly, even if there is a UK adequacy decision, many organisations would opt to use backup options such as SCCs or BCRs, even if they are more burdensome, as this might be considered more stable and reliable.

142 Oliver Patel and Nathan Lea 'EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?' (2019) UCL European Institute, pp. 9-11.
143 Research interview with EU official (2019).
144 Research interview with business representative (2019).

5. SCCs and BCRs are also unstable

If the EU does not grant the UK an adequacy decision, or if the UK's future adequacy decision is subsequently invalidated by the CJEU, organisations will have no option but to use alternative, ad hoc legal safeguards to transfer data. At present, SCCs and BCRs are the only viable mechanisms.

This report's preceding analysis explained why these mechanisms are also unstable. Put simply, SCCs and BCRs cannot provide protection against foreign governments' surveillance and intelligence gathering activities.[145] In the December 2019 opinion, the Advocate General clarified and elaborated on the legal position, arguing that SCCs should be investigated and reviewed on a case-by-case basis. Data exporters using SCCs should conduct due diligence and always review whether the data is sufficiently protected after it is transferred. If they cannot do this, or they suspect the data is not protected, then the relevant DPA should investigate and potentially prohibit or suspend transfers based on SCCs. DPAs should also investigate complaints raised about specific SCCs. Max Schrems' analysis of this opinion was that instead of invalidating the global system of SCCs, the Advocate General was "telling the Irish Data Protection Authority to just do its job".[146]

It is possible that the CJEU will follow the Advocate General's opinion on this matter. This would entail instructing DPAs to investigate and potentially suspend SCCs on a case-by-case basis. However, it is also possible, though less likely, that the global system of SCCs will be invalidated or amended. Both outcomes have implications for the UK, especially if it fails to secure an adequacy decision. Either way, the Advocate General's opinion encourages and emboldens data subjects and activists to challenge SCCs.

If SCCs cannot be used, this is a dire situation for organisations seeking to transfer data from the EU to the UK. However, even in the less extreme and more likely scenario, there could be a flurry of complaints to EU DPAs regarding SCCs used to transfer data to the UK, which may result in investigations and suspensions of SCCs. This could particularly implicate 'telecommunications operators' which are most affected by Investigatory Powers Act notices (e.g. ISPs, social media websites, email and cloud service providers),[147] as the personal data they retain is more likely to be accessed by UK government agencies.

Consider this situation: the CJEU invalidates a UK adequacy decision on the grounds that the Investigatory Powers Act is incompatible with the EU Charter. As such, companies transferring data from the EU to the UK use SCCs instead. Privacy activists then file complaints regarding the use of SCCs by major internet companies, noting that the UK's surveillance law means that personal data is still not protected, even when transferred via an SCC. The relevant DPA, following the CJEU's logic, suspends a specific SCC or an entire organisation's SCCs. In the most extreme scenario, it is theoretically possible for the DPA or even the EDPB to suspend all SCCs used to transfer data to a specific jurisdiction, like the UK, from either one EU member state or the entire EU.

For these reasons, SCCs and BCRs may yet prove to be unstable and unreliable. Just as with EU-U.S. data flows, it is possible to map out a path to severely restricted EU-UK data flows, i.e. no adequacy decision and the suspension of critical or even all SCCs used to facilitate lawful EU-UK data transfers. Businesses and data protection officers need to be aware of this risk.

6. The EU will expect dynamic alignment with its data protection standards over time

The threshold for adequacy is that the level of data protection in the third country must be 'essentially equivalent' to the level of protection in the EU. The Commission periodically reviews adequacy decisions to ensure that this remains the case. The annual reviews of Privacy Shield have not produced any major flashpoints and the Commission has become increasingly satisfied with the framework over the years. If the U.S. ever adopts a comprehensive, federal privacy law this would be viewed very positively by the EU.

Post-Brexit, if the UK is granted an adequacy decision, it will be because the Commission deems that the UK's level of data protection is 'essentially equivalent' to the EU's. This would be unsurprising given the UK's implementation of the GDPR. However, this could change over time, especially if the UK were to diverge from EU data protection standards, which the UK government has hinted at. In a written statement to Parliament, Boris Johnson stated that 'the UK will in future develop separate and independent policies in areas such as […] data protection'.[148] In response, the EDPS stated that 'any substantial deviation from the EU data protection acquis that would result in lowering the level of protection would constitute an important obstacle to the adequacy findings'.[149]

A third country does not need to follow identical data protection standards to the EU's to attain adequacy status, but it certainly helps. If future UK divergence is substantive, or if the EU substantively reformed the GDPR – or passed the e-Privacy Regulation – and the UK's data protection standards did not follow suit, then any UK adequacy decision could be revoked. Although this is not an issue for the near future, divergence in one direction will happen at some point, and the UK must continue to meet the 'essentially equivalent' threshold to retain any adequacy decision. As such, the EU will expect dynamic alignment with its data protection standards over time.

145 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) German Law Journal, p. 885.
146 NOYB, 'CJEU – AG Opinion, First Statement' (2019).
147 Graham Smith, 'The UK Investigatory Powers Act 2016 – what it will mean for your business' (2016) Bird & Bird.
148 Boris Johnson, 'UK/EU relations: Written Statement' (2020) House of Commons.
149 EDPS, 'EDPS Opinion on the opening of negotiations for a new partnership with the UK' (Opinion 2/2020), p. 4.

7. UK government and business will feel aggrieved should an adequacy decision not be granted

As previously mentioned, when undertaking adequacy assessments, the Commission considers aspects of the third country linked to defence and national security, despite the fact that these competences have not been conferred to the EU by the member states. Indeed, law enforcement and data protection are treated as separate domains in EU law, and the CJEU has conceded that member state national security laws fall outside the scope of EU law, meaning the CJEU has no jurisdiction over them.[150]

This has led to claims of unfairness, due to a perception that the EU is holding third countries to a higher standard than its own member states, some of which are suspected to have national security architectures which contravene EU fundamental rights law.[151]

It is beyond the scope of this report to assess whether the U.S. or UK national security systems protect fundamental rights to a greater degree than EU member states do. However, our interviews with data privacy stakeholders in the U.S., including government officials, lawyers and academic experts, revealed a prevailing perception of unfairness and dismay at the way the U.S. had been treated by the EU with regard to commercial data flows.

Their core argument is as follows: by invalidating Safe Harbour and now considering to invalidate Privacy Shield, the EU is penalising the U.S. for its national security system. However, this is deemed to be unfair, because, those stakeholders argue, U.S. intelligence gathering systems benefit European countries, as the U.S. 'exports' a significant amount of intelligence to its European allies to enable them to fight security threats.[152] Furthermore, it is perceived as hypocritical, because several EU member states have national security and mass surveillance systems which undermine civil liberties like privacy to a greater extent than the U.S. system, with less transparency, oversight and accountability, so the argument goes.[153]

Jim Halpert of DLA Piper argued that ***"EU member state concerns regarding US surveillance laws are somewhat hypocritical. Several major EU member states have similar surveillance laws to the U.S. For example, France is more of a wild west than is the US in terms of controls on government surveillance."***[154] Virtually everyone we interviewed in the U.S. expressed sentiments of this nature. These claims are difficult to prove, due to a lack of transparency in the surveillance domain.[155]

However, a group of leading scholars argue that the U.S. and UK surveillance revealed by Snowden is in fact 'much more widespread' and that 'the U.S. is the only country to terminate a bulk collection programme in recent years […] meanwhile the UK, France and Germany have expanded collection programmes'.[156] Also, Privacy International argued that 21 EU member states' surveillance legislation do not meet the standards of EU fundamental rights law (as outlined in the judgements in Tele2 Sverige/Watson and Digital Rights Ireland).[157] France, for example, which significantly increased its intelligence gathering activities after the 2015 terrorist attacks, is thought by academics and activists to have data retention laws which violate CJEU case law.[158]

It is fair to argue that EU member states benefit from U.S. intelligence gathering and rely upon intelligence sharing with the U.S. for protecting national security. It is also empirically true that there has been greater transparency and public debate regarding mass surveillance in the U.S., but this was largely provoked by the extraordinary Snowden revelations.

However, it could be a stretch to label the EU as hypocritical, as the CJEU does review member state intelligence gathering and national security-related activities, as although these are not conferred competences, the Charter still applies when member states implement EU law such as the e-Privacy Directive. Indeed, in January 2020, Advocate General Campos Sánchez-Bordona issued opinions on four similar cases (concerning France, Belgium and the UK), in which he clarified that EU law applies when member state governments compel private companies to retain data, even for national security purposes.[159] He also argued that the e-Privacy Directive precludes the collection of and access to 'bulk communications data' – enshrined in the UK's Investigatory Powers Act. The CJEU ruling will follow later this year.[160]

This U.S. perception of unfairness is a sneak preview of the relatively peculiar situation which awaits the UK. Post-Brexit, the UK's national security system will be under the microscope, as Commission officials assess the UK for data adequacy. The prospect that the EU may not permit data to flow freely to the UK, because of aspects of its national security system which have been in place for several years, and despite the fact that EU-UK data flows have been unrestricted since the emergence of the modern internet in the 1990s, is bound to provoke dismay.

UK officials might ask why this is 'suddenly' a problem, if it was not an issue when the UK was a member state. The answer is that it has always been a problem, as evidenced by the Tele2/Watson case and the January 2020 Advocate General opinion. Also, although such contested issues with UK surveillance legislation have never led to a halt of EU-UK data flows – and it is not always apparent which aspects of EU law apply to member states with regards to their national security activities – the EU is not obliged to grant any third country an adequacy decision.

The difficulties around EU-U.S. data flows highlight how the EU is perceived as applying more rigorous national security standards for third countries than EU member states, at least with regards to its threshold for permitting unrestricted commercial data flows.

One U.S. official we interviewed claimed that 'the Commission knows about the situation in France and the UK, but it cannot do anything'.[161] Similarly, an EU official stated that 'of course the

150 Paul Schwartz and Karl-Nikoloaus Peifer, 'Transatlantic Data Privacy' (2017) The Georgetown Law Journal, p. 168.
151 Privacy International, 'New Privacy International report shows that 21 European countries are unlawfully retaining personal data' (2017).
152 Henry Farrell and Abraham Newman, 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security' (2019) Princeton University Press, p. 141
153 David Bender, 'Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective' (2016) International Data Privacy Law.
154 Research interview with U.S. privacy lawyer Jim Halpert (2019).
155 Ira Rubenstein et al., 'Systematic Government Access to Private-Sector Data: A Comparative Analysis', in Fred Cate and James Dempsey (eds.), 'Bulk Collection: Systematic Government Access to Private-Sector Data' (2017) Oxford University Press, p.17.
156 Ibid, p. xxviii.
157 Privacy International, 'New Privacy International report shows that 21 European countries are unlawfully retaining personal data' (2017).
158 Winston Maxwell, 'Systematic Government Access to Private-Sector Data in France', in Fred Cate and James Dempsey (eds.), 'Bulk Collection: Systematic Government Access to Private-Sector Data' (2017) Oxford University Press, pp. 56-57
159 CJEU, 'Advocate General Campos Sánchez-Bordona : the means and methods of combating terrorism must be compatible with the requirements of the rule of law' (2020).
160 CJEU, 'Opinion of Advocate General Campos Sanchez-Bordona delivered on 15 January 2020' (Case C623/17).
161 Research interview with U.S. official (2019).

Commission knows about the situation in the member states. It is not in denial.'[162]

Put simply, the EU would not restrict commercial data transfers between its member states, even if a member state's legislation was found to be incompatible with EU fundamental rights law. This peculiar dynamic is why UK officials and businesses may respond ungenerously if the UK fails to attain an adequacy decision, especially if they have full knowledge of the national security systems of other EU member states (e.g. France).

The prevailing sense of anger and injustice we documented among U.S. stakeholders may be a sign of things to come for the UK, not least because one leading lawyer, Eduardo Ustaran of Hogan Lovells, argued that to question the UK's adequacy is "nonsensical – the UK is 97% there",[163] with another calling UK adequacy a "no brainer".[164]

8. Ultimately, the UK will probably face the same problems as the U.S.

The fundamental problem for the U.S. in preserving unrestricted data flows with the EU is a clash between U.S. national security and surveillance laws and programmes on the one hand, and EU data protection standards and fundamental rights on the other.

Although the clash for the UK may not be as stark, given that it follows the GDPR and has relatively robust data protection enforcement, fundamental tensions between UK national security, mass surveillance and human rights on the one hand, and EU fundamental rights on the other, could prove problematic for the UK in its quest for a continuation of unrestricted EU-UK data flows. This will be an issue both for attaining and retaining an adequacy decision and, failing that, the reliable use of SCCs and BCRs.

This fundamental problem underpins this section's entire analysis; various scholars argue that there is no clear solution.[165] It is therefore highly likely that the EU-UK data flows relationship will be complex, messy and could remain unresolved even many years from now.

What about UK-U.S. data flows?

The future UK-U.S. relationship is significant, given the extent of digital trade and data flows across the Atlantic. It is estimated that more than 72% of UK services exports to the U.S. (totalling £46 billion) were delivered remotely in 2018, the majority of which were due to cross-border data flows.[166] The U.S. and UK governments have confirmed that, post-Brexit, Privacy Shield will continue to enable UK-U.S. data flows, so long as certified U.S. organisations update their public commitments to include UK-U.S. transfers.[167] This would represent a continuation of the status quo, as organisations would be able to transfer data from the UK to the U.S. in the same way that they currently do. This is similar to the Switzerland-U.S. Privacy Shield, which largely replicates the EU-U.S. Privacy Shield.

As noted above, the U.S. pushes for unrestricted data flows when negotiating trade agreements, and its objectives for the UK negotiations emphasise this. In future, if Privacy Shield is invalidated by the CJEU, this would leave the UK in a difficult situation, as the U.S. would continue to insist on unrestricted UK-U.S. data flows, but the EU may be concerned about unprotected onward transfers from the UK to the U.S. If the UK grants the U.S. a separate adequacy decision in this scenario, thereby diverging from Privacy Shield and the CJEU judgement, this has the potential to complicate the adequacy assessments and potentially derail a future adequacy decision. This is also true if Privacy Shield is not invalidated, but the future UK-U.S. trade agreement entails far greater liberalisation of UK-U.S. data flows than does EU-U.S. Privacy Shield.[168]

162 Research interview with EU official (2019).
163 Research interview with privacy lawyer Eduardo Ustaran (2019).
164 Research interview with European privacy lawyer (2019).
165 Christopher Kuner, 'Transborder Data Flows and Data Privacy Law' (2013) Oxford University Press, p. 138.
166 Department for International Trade, 'UK-US Free Trade Agreement' (2020), p. 19.
167 'Privacy Shield and the UK FAQs' (2020).
168 Javier Ruiz, 'UK publishes trade objectives for deal with the US: What you need to know' (2020) Open Rights Group.

Conclusion

Cross-border data transfers underpin the modern, digital economy, and their preservation is of vital importance to business. Despite this, the topic receives minimal attention in academic, policy and political debates.

On this issue, there are long-standing tensions between the EU institutions, as well as the EU's policy objective and core values. The European Commission and most member states have been keen to preserve relatively unhindered data flows with the U.S., in recognition of the associated economic benefits. The European Parliament, European Court of Justice and EDPB have been more sceptical. The problem arises when economically beneficial data transfers threaten or weaken EU citizens' fundamental rights to privacy and data protection – as is most likely the case with EU-U.S. data transfers.

The coming months will be fascinating, and perhaps decisive, for the future of EU-third country data transfers. The outcome of the Schrems II case is key, as this could lead to significant changes (and suspensions) to SCCs, and even invalidation of Privacy Shield. The negotiations on the future EU-UK relationship – and crucially, whether the Commission grants the UK an adequacy decision – will also be highly informative as to where the EU stands on this matter.

There is minimal precedent for significant disruption to previously unrestricted commercial data flows between two jurisdictions; no one knows exactly what this would entail. However, this is precisely what could happen to both EU-U.S. and EU-UK transfers in the near future.

Irrespective of the legal and regulatory situation, the EU – which is already struggling to enforce the GDPR – cannot simply switch off the internet. As such, large-scale data transfers will likely continue in any scenario, with the biggest loser perhaps being data protection compliance levels and the rule of law.

Oliver Patel
Research Associate & Manager
UCL European Institute
Email: oliver.patel@ucl.ac.uk
www.ucl.ac.uk/european-institute/people/oliver-patel

Oliver is an expert on the legal, political and constitutional aspects of the Brexit negotiations and withdrawal process. He is also an expert in EU data protection law and policy, cross-border data flows and the regulation of digital technologies and the internet more broadly.

Dr Nathan Lea
Senior Research Associate
UCL Institute of Health Informatics
Email: n.lea@ucl.ac.uk
www.ucl.ac.uk/health-informatics/people/nathan-lea-0

Nathan's areas of expertise include information governance and regulatory oversight in healthcare and medical research. His research focus is on the role of information systems in supporting healthcare delivery and empowering patients. He is also an expert on GDPR.

UCL European Institute
16 Taviton Street
London WC1H 0BW
Email: european.institute@ucl.ac.uk
www.ucl.ac.uk/european-institute

The UCL European Institute is UCL's hub for research, collaboration and engagement on Europe.

Co-funded by the European Union

UCL EUROPEAN INSTITUTE

POLICY PAPER

Design: davidlovelock.com