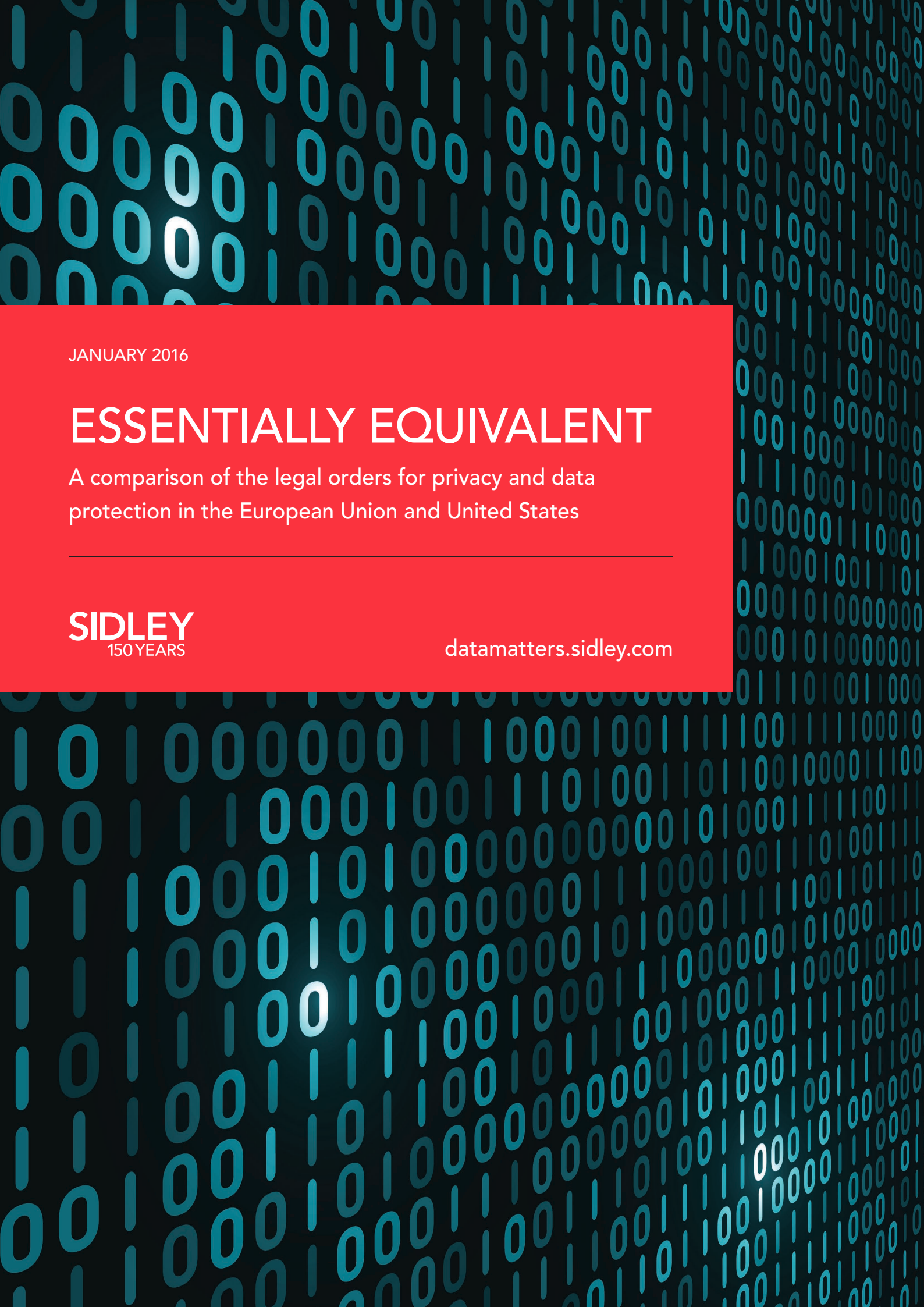

JANUARY 2016

ESSENTIALLY EQUIVALENT

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

SIDLEY
150 YEARS

datamatters.sidley.com

SIDLEY
150 YEARS

25 January 2016

A report for:

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

Respectfully submitted,

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

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

SIDLEY
150 YEARS

Essentially Equivalent

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

Jacques Bourgeois

Cameron F. Kerry

William R. M. Long

Maarten Meulenbelt

Alan Charles Raul

January 2016

datamatters.sidley.com

Preface

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

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

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

SIDLEY AUSTIN LLP

CONTENTS

EXECUTIVE SUMMARY

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

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

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

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

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

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

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

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

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

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

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

PART ONE:

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

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

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

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

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

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

PART TWO:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PART THREE:

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

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

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

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

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

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

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

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

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

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

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

ABOUT THE AUTHORS

Sidley Austin LLP is a premier global law firm celebrating its 150th anniversary in 2016. With 1,900 lawyers and 19 offices worldwide, the firm provides a broad range of services to meet the needs of large and small businesses and other organizations across a multitude of industries, forums and governments. Sidley has a broad transactional practice and consistently ranks among the top global capital markets firms. Sidley also has an extensive litigation and arbitration practice, spanning nearly every area of substantive law. The firm also provides regulatory counseling and advocacy regarding communications, energy, environmental, food, drug and device, healthcare, insurance, Internet, life sciences, financial and securities law, and represents clients in virtually every major industry. Sidley is rated among the top law firms, recognized in the United States and globally for service and responsiveness, and widely recognized for its pro bono and diversity programs.

Sidley's Privacy, Data Security and Information Law practice group is a global and interdisciplinary team of lawyers focused on a broad range of emerging issues, including privacy and data protection; cybersecurity and data breach preparedness and response; Big Data; government surveillance; data localization; Internet law; cross-border data flows; and e-Commerce. The group handles litigation and investigations, cybersecurity compliance and regulatory counseling, data breach incident response, legislative and policy developments and sector-specific counseling internationally. Clients cover a broad range of industries. The practice and its lawyers consistently rank in the top tiers of *Chambers USA, Chambers Global*, and *The Legal 500*.

Jacques Bourgeois
Senior Advisor
Brussels
jbourgeois@sidley.com
+32 2 504 6490

Jacques Bourgeois is senior adviser in Sidley's Brussels office. He is a recognized authority on European Union (EU) law, with over four decades of experience in private practice and public service. Prior to joining Sidley, Jacques served for over 25 years as a senior official with the European Commission, where he was the principal legal adviser of the Commission in charge of foreign trade policy and, later, antitrust policy. Previously, he served for several years as head of the Trade Policy Instruments Division in the Directorate-General for External Relations. Since 2006, he has served as Chairman of the Competition Commission advising the Belgian government. He advises Sidley lawyers and clients around the globe on all aspects of EU law. He is also a professor at the College of Europe in Bruges and a guest professor at the University of Ghent.

Cameron F. Kerry
Senior Counsel
Boston
ckerry@sidley.com
+1 617 223 0305

Cameron F. Kerry is senior counsel in Sidley's Boston and Washington, D.C. offices. He is former General Counsel and Acting Secretary of the United States Department of Commerce, where he played a leadership role in consumer privacy issues and the flow of information and technology across international borders, including on the EU-U.S. Safe Harbour Framework. Cam is also a visiting scholar with the MIT Media Lab and a frequent speaker and writer on privacy and the digital economy. At Sidley, his broad practice operates at the intersection of law, technology and public policy, and is informed by his years of government service and more than three decades in private practice.

William Long
Partner
London
wlong@sidley.com
+44 20 7360 2061

William Long is a partner in Sidley's London office. He advises international clients on a wide variety of data protection, privacy, information security, social media, e-Commerce and other regulatory matters. William is on the DataGuidance panel of data protection lawyers and is a contributing author on a number of books, including leading legal text books published by BNA in the areas of privacy, cloud computing and the use of health data. He also co-authored a major global survey of Privacy, Data Protection and Cybersecurity law covering 62 international jurisdictions published by Law Business Research. William has been interviewed widely for his thought leadership and writes for a number of publications, including *Data Protection Law & Policy*, *Computer Weekly* and *CIO Today*.

Maarten Meulenbelt
Partner
Brussels
mmeulenbelt@sidley.com
+32 2 504 6467

Maarten Meulenbelt is a partner in Sidley's Brussels office. He has extensive litigation experience before the EU Courts, national courts and competition authorities, the European Commission and national regulatory authorities in several EU Member States with a specific focus on the life sciences sector. He is a member of Sidley's Privacy, Data Protection and Information Law, Global Life Sciences and Antitrust practices focusing on EU regulatory affairs, litigation and competition law issues affecting clients in Europe.

Alan Charles Raul
Partner
Washington, D.C.
araul@sidley.com
+1 202 736 8477

Alan Charles Raul is a partner in Sidley's Washington, D.C. office and the founder and leader of Sidley's Privacy, Data Security and Information Law practice. While practicing law at Sidley, Alan served as Vice Chairman of the Privacy and Civil Liberties Oversight Board and, prior to joining Sidley, he served as Associate Counsel to the President, General Counsel of the Office of Management and Budget and General Counsel of the U.S. Department of Agriculture. He represents a wide range of companies on federal, state and international privacy issues and litigation. He is a prolific writer and speaker on privacy, cybersecurity and related issues.

SIDLEY
150 YEARS

sidley.com

AMERICA • ASIA PACIFIC • EUROPE

MN-2984-01/16