Cross-Border Data Flows, the GDPR, and Data Governance (29 Wash. Int'l L.J. 485 (2020)

W. Gregory Voss

CROSS-BORDER DATA FLOWS, THE GDPR, AND DATA GOVERNANCE

W. Gregory Voss[†]

Abstract: Today, cross-border data flows are an important component of international trade and an element of digital service models. However, they are impeded by restrictions on cross-border personal data transfers and data localization legislation. This Article focuses primarily on these complexities and on the impact of the new European Union ("EU") legislation on personal data protection—the GDPR. First, this Article introduces its discussion of these flows by placing them in their economic and geopolitical setting, including a discussion of the results of a lack of international harmonization of law in the area. In this framework, rule overlap and rival standards are relevant. Once this situation is established, this Article turns to an analysis of the legal measures that have filled the gap left by the lack of international regulation and the failure to harmonize law: extraterritorial laws in the European Union (regional legislation) and the United States (state legislation); and data localization laws in China and Russia. Specific provisions restricting cross-border personal data transfers are detailed under EU legislation, as are the international agreements that have been invaluable in allowing flows between the United States and the European Union to continue—first the Safe Harbor, and now the Privacy Shield. Finally, in this context, the role of data governance is investigated, both in the context of data controllers' accountability for the actions of other actors in global supply chains under EU law and under the Privacy Shield. Thus, this Article goes beyond the law itself, to place requirements in the context of the globalized business world of data flows, and to suggest ways that companies may improve their compliance position worldwide.

Cite as: W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485 (2020).

I. INTRODUCTION: THE ECONOMIC AND GEOPOLITICAL SETTING

"So, when we start talking about regulation and we start talking about GDPR, and we start talking about this extra territorial reach where the Europeans are going to find American

[†] Associate Professor of Business Law, TBS Business School, Toulouse, France. The author would like to thank the dedicated editors and staff of the Washington International Law Journal for their helpful suggestions and their diligent editing work on this Article, amid a worldwide pandemic, which made a discussion of global data supply chains ever more poignant. The author may be contacted at g.voss@tbs-education.fr.

> companies and California is going to find Alabama companies. The IT folks are recognizing, 'boy we've got some debt.' I don't know where the data is."[1]

Kris Torgerson, Chief Information Officer at Oak Ridge National Laboratory.

This Article is about cross-border data flows, the impact of EU data protection regulation on them, the role of international agreements in this context, and resulting requirements for data governance. The structure of this Article is as follows: after this introduction, cross-border personal data transfer restrictions in EU legislation are discussed, followed by the role of international agreements—both in terms of regulating cross-border data flows and in allowing an EU "adequacy" determination. This leads to an analysis of data governance requirements under the GDPR. Naturally, the relevant environment is an international one, with economics[2] and geopolitics each playing a role; including, issues of "rival standards"[3] or, as one academic has put it, "transnational regulatory conflict and interdependence"[4] and "rule overlap" of extraterritorial laws,[5] notably between the United States and the

---

[1] Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent, Jennifer Boling, and Amanda Sweenty, *Law and Business Technology: Cyber Security & Data Privacy Update*, 20 TENN. J. BUS. L. 1065, 1071 (2019), https://trace.tennessee.edu/transactions/vol20/iss4/3.

[2] Julie E. Cohen refers to the economic actors who profit from services provided "via digital information and communications networks" having an interest in cross-border data flows:

> The new information-economy actors that profit from those services—including global platform companies and financial services firms but also any firm that engages in offshoring of functions such as customer support and human resources—have interests in defining and controlling their own global operations in ways that may include transfers of data for processing, cloud storage spanning multiple jurisdictions, and cross-border provision of services to end users. Data flows between networked devices—ranging from personal communications devices to industrial sensors—are central concerns of internet governance processes. JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 214–15 (2019).

[3] For a discussion of the "rival standards" aspect of international data privacy legislation, *see* DANIEL W. DREZNER, ALL POLITICS IS GLOBAL: EXPLAINING INTERNATIONAL REGULATORY REGIMES 79, 103–06 (2007) (discussing rival standards as "[d]ifferent groups of countries will generate alternative sets of regulatory standards, while trying to weaken the legitimacy of competing standards.").

[4] Gregory Shaffer speaks of "transnational regulatory conflict and interdependence," where the battlefield is not exclusively international. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 4 (2000) ("The war over privacy standards is fought not just between Europe and the United States. It is a civil war as well, fought within the United States itself, with European law changing the balance of power on the fields where U.S. interest groups clash.").

[5] Political scientists Henry Farrell and Abraham L. Newman summarize salient aspects of "rule overlap," in a book that analyzes the local and global political actions of various actors, such as multinational

European Union. Authors Farrell and Newman apply their New Interdependence Approach ("NIA") analytic framework "to explain the dynamics of world politics in an age of globalization," focusing on process and dynamics in world politics,[6] much as Shaffer discusses the process of trading up in data privacy standards through the actions of various actors.[7] While these analyses are not at the heart of the Article, they provide background and show the dynamic effect of actions of various stakeholders, such as governments, trade associations, data privacy advocates, and others, which helps explain why international data trade finds itself in the position described in this Article, and the implications for data-driven supply chains worldwide. First, this introduction will show the growing importance of cross-border data flows, then discuss the lack of harmonization of data privacy law and various divergent regulatory models with strategic effect, and finish discussing the Article's aims.

A. The Growing Importance of Cross-Border Data Flows

Cross-border data flows have been described as commerce-enabling "hallmarks of 21st century globalization"[8] and "the connective tissue holding the global economy together."[9] One estimate shows cross-border data flows added $2.8 trillion to world GDP in 2014.[10] They include personal and professional information flows alike, along with flows of digital media

---

firms, in this context: "Globalization is not characterized primarily by an absence of rules or norms. Rather, the process of creating openness—in trade, finance, production and information—creates a series of overlapping authority claims made by domestic and international actors. The importance of rule overlap is demonstrated by continuing global controversies in policy areas as diverse as antitrust, taxation, bank supervision, and data privacy." *See* HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 27–28 (2019).

[6] *Id*. at 26 (especially relevant for the reader is Farrell and Newman's discussion of political action in connection with various issues of data privacy and security rule overlap).

[7] *See* Shaffer, *supra* note 4, at 4 (stating that: [I]n order to avoid a trade conflict, U.S. regulators promote enhanced data privacy "self-regulation" by businesses. In order to avoid EU data transfer restrictions, U.S. businesses implement new internal data privacy practices with an eye on the EU criteria. Through the publicity given to the EU Directive, U.S. privacy advocates press for businesses to adopt more stringent internal practices and for legislators to enact additional legislation).

[8] MCKINSEY GLOBAL INSTITUTE, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS 30 (March 2016), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx.

[9] MCKINSEY GLOBAL INSTITUTE, GLOBALIZATION IN TRANSITION: THE FUTURE OF TRADE AND VALUE CHAINS 25 (January 2019), https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/Globalization%20in%20transition%20The%20future%20of%20trade%20and%20value%20chains/MGI-Globalization%20in%20transition-The-future-of-trade-and-value-chains-Full-report.ashx.

[10] *Id*. at 74.

content.[11] Two U.S. government agencies within the U.S. Department of Commerce—the Economics and Statistics Administration and the National Telecommunications and Information Administration—place such flows in four categories. Thus, providing more detail although, not specifically referring to the personal data that is furnished in order to obtain what they describe as a "$0 market price." These categories are:

1) *Purely non-commercial data traffic*, including government and military communications;
2) *Transaction data flows between buyers and sellers at a market price*, including direct purchases between buyers and sellers, such as in online banking or advertising, and services transactions that involve digital platforms acting as intermediaries between buyers and sellers;
3) *Commercial data and services exchanged between or within businesses or other related parties at $0 market price*, including supply chain, personnel, or design information;
4) *Digital data and services delivered to and from end-users at $0 market price*, including free email, search engine results, maps and directions, and information via social media.[12]

Moreover, internet intermediaries, who have "captured much of the value from the collection of personal data while the data subjects have received access"[13] to them, provide cross-border "free" digital services, such as those within the fourth category above. These services have been estimated to have added between $240 billion and $3.2 trillion to trade in services in 2017.[14] Such flows are ubiquitous, and with the Internet of Things ("IoT") there will be huge volumes of international data transfers without human

---

[11] MCKINSEY GLOBAL INSTITUTE, DIGITAL GLOBALIZATION, *supra* note 8, at 32.

[12] *See* ECON. & STAT. ADMIN. & NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, MEASURING THE VALUE OF CROSS-BORDER DATA FLOWS 3 (2016).

[13] W. Gregory Voss, *Internet, New Technologies, and Value: Taking Share of Economic Surveillance*, 2017 U. ILL. J.L. TECH. & POL'Y 469, 472 (2017).

[14] The difference between the two figures has been explained as follows: "The lower estimate is based on substitute prices, while the higher estimate is based on consumer willingness-to-accept measures. This very broad range reflects uncertainty surrounding what consumers would pay for the suite of free digital services they consume, and about the business models and bundled services that might emerge if companies charged for these services. The reality is likely somewhere between these two figures. Either case, however, would represent a sizable addition to global services trade flows." *See* MCKINSEY GLOBAL INSTITUTE, GLOBALIZATION IN TRANSITION, *supra* note 9, at 51.

intervention.[15] They allow small and medium size enterprises ("SMEs") to expand their businesses worldwide and access online digital services that can help them increase their productivity.[16] However, national (and regional) actors have not provided harmonious regulation for these increasing flows, or for data privacy, more generally.

B. Lack of International Legal Harmonization and Divergent Regulatory Models with Strategic Effect

Globalized trade in digital data and services has neither been accompanied by a general harmonization of internet law,[17] nor true data protection and data privacy law convergence, exemplified by the divergence between the two large Western blocs: the United States and the European Union.[18] This divergence exists despite the growing influence of the EU data protection model worldwide,[19] with its recently applied General Data Protection Regulation ("GDPR").[20] Furthermore, in the transatlantic context, certain obstacles to data privacy law harmonization exist between the European Union, on the regional level, and the United States, on the federal level.[21]

Transatlantic divergence exists; but, on the international scale there are also various legal standards used in Internet governance, arguably for strategic ends. China uses regulation, innovation, and foreign policy to gain greater power in Internet governance, among other goals. At the same time its citizens expect little from the government in terms of privacy; although, perhaps more

---

[15] CHRISTOPER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 3 (2013).

[16] *See* JOSHUA P. MELTZER, THE IMPORTANCE OF THE INTERNET AND TRANSATLANTIC DATA FLOWS FOR U.S. AND EU TRADE AND INVESTMENT 3, (The Brookings Institution, Global Econ. & Dev. Working Paper No. 79, 2014), https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf.

[17] W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 403, 408 (2019).

[18] *Id*. at 408.

[19] *Id*. at 458.

[20] Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

[21] These obstacles have been described as U.S. neoliberalism and laissez-faire policy, lobbying, and differing constitutional provisions on one side and the other of the Atlantic. *See* Voss, *Obstacles*, *supra* note 17, at 431–52.

from businesses.[22] China seeks the goal of "cyber-sovereignty," and has adopted an Internet regulation model that places an emphasis on national interests instead of corporate ones.[23] Thus, regulation of the Internet holds strategic value.

Europe, through the adoption of the GDPR, has also taken a strategic aim—creating the online trust in digital services necessary to strengthen the EU economies[24]—with legislation that almost seems to take on an evangelistic air, as described by Helen Dixon, head of the supervisory authority of Ireland,[25] where many U.S. Internet giants have their main European Union establishment:[26]

> The EU has opened a new chapter in the history of the Internet, creating a blueprint that other states and organizations will study closely as they, too, seek to properly balance individuals' rights to data protection with their other rights and with the legitimate interests of business and government. The world's governments must start to converge on laws regarding data protection, ideally

---

[22] Adam Segal, *When China Rules the Web: Technology in Service of the State*, FOREIGN AFF., Sept.-Oct. 2018, at 10.

[23] *Id*. at 11–12.

[24] Helen Dixon, *Regulate to Liberate: Can Europe Save the Internet?*, FOREIGN AFF., Sept.-Oct. 2018, at 28, 30.

[25] *Background*, DATA PROT. COMM'N, https://www.dataprotection.ie/en/about/background (last visited Feb. 20, 2020). The Data Protection Commission (DPC) is Ireland's supervisory authority, defined as "an independent public authority which is established by a Member State pursuant to Article 51" of the GDPR. GDPR, *supra* note 20, art. 4(21). In common parlance, supervisory authorities are sometimes known as "data protection authorities" or "DPAs." The DPC's structure, with Helen Dixon at its head (as Data Protection Commissioner), may be viewed on their website. *See Senior Management Committee & Organisational Structure*, DATA PROT. COMM'N, https://www.dataprotection.ie/en/about/senior-management-committee-organisational-structure (last visited on Feb. 20, 2020).

[26] Ireland "is the European headquarters for data-hungry companies including Airbnb, Apple, Facebook, Google, Twitter and Microsoft, which owns LinkedIn." Adam Satariano, *New Privacy Rules Could Make This Woman One of Tech's Most Important Regulators*, N.Y. TIMES (May 16, 2018), https://nyti.ms/2GjRTaN. It is the supervisory authority of the Member State of the main establishment of the controller of data processing activities in the European Union that acts as the lead supervisory authority for that company. GDPR, *supra* note 20, art. 56(1). A "controller" is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data . . . ." GDPR, *supra* note 20, art. 4(7). A controller's "main establishment" is, for these controllers with establishments in more than one EU Member State, "the place of its central administration in the [European] Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment." GDPR, *supra* note 20, art. 4(16)(a). Thus, for each of the large companies listed in this footnote, the Irish DPC would likely be the lead supervisory authority.

> taking inspiration from the GDPR. Otherwise, authoritarians and unscrupulous tech giants will stand to gain, and democratic states and ordinary people will lose out.[27]

Furthermore, Khorana and Voss describe Europe's Digital Single Market strategy, of which the GDPR is an important element, as being able to be "perceived as an integral part of Europe's ability to exert its market power. By externalizing market-related social and economic policies and regulatory measures, the EU is inherently competing with other trade partners in exporting its standards internationally and in defining international standards."[28]

Under the moniker of the "Brussels effect," Anu Bradford describes the European Union as establishing global rules in a range of areas of regulation: antitrust, privacy, health protection (with the regulation of chemicals), environmental protection, and food safety.[29] The area of privacy protection,[30] where Bradford says Europe sets the tone,[31] is central for this Article. Bradford sees EU law in this area influencing the laws of areas outside its borders, except the United States.[32] Moreover, despite its differences with U.S. law, EU law in the area of privacy impacts U.S. firms' business practices, through lawsuits against them in EU courts,[33] or through firms adopting privacy policies compliant with EU law,[34] or they're voluntarily signing on to principles from international agreements between the EU and the United States, such as those of the Safe Harbor Framework for cross-border data transfers.[35]

In the United States, the early Internet gained substantially—both financially and in terms of its regulatory framework—from the U.S. government, in particular through government grants and a policy of

---

[27] Dixon, *supra* note 24, at 28–29.

[28] Sangeeta Khorana & W. Gregory Voss, *The Digital Single Market: Move from Traditional to Digital?*, *in* HANDBOOK ON THE EU AND INTERNATIONAL TRADE 384, 389 (Sangeeta Khorana & María García, eds., 2018).

[29] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 19–35 (2012).

[30] *Id*. at 22–26.

[31] *Id*. at 22.

[32] *Id*.

[33] *Id*. at 23. This reach was noted years earlier by Gregory Shaffer, who described the fact that "in a globalizing economy, European regulation casts a net wider than Europe." Shaffer, *supra* note 4, at 4.

[34] Bradford, s*upra* note 29, at 24.

[35] *Id*. at 24–25.

"openness" for an "open and free Internet."[36] U.S. public policy choices in telecommunications regulation and the Section 230 (Communications Decency Act) exclusion of internet intermediary liability for third party content also helped create the environment for the development of the U.S. Internet companies.[37] These substantially lowered risk for Silicon Valley in terms of possible torts and copyright liability related to such content.[38] More to the point, historically there has been little regulation of Silicon Valley insofar as data privacy is concerned, and privacy torts are of little help in protecting personal information.[39] Thus, there are considerable differences between this *laissez-faire* approach, the European Union's emphasis on individual rights, and China's national interest focus.

While some have seen that there may be regulatory competition causing regulation to rise to global standards,[40] there has been no harmonization between the national law of China, the regional law of the European Union,

---

[36] *See* Karen Kornbluh, *The Internet's Lost Promise: And How America Can Restore It*, FOREIGN AFF., Sept./Oct. 2018, at 33. *See also* ROXANA RADU, NEGOTIATING INTERNET GOVERNANCE 61 (2019) ("In addition to sustained funding from DoD and NSF, the development of the Internet in the American context was facilitated by the minimal state ideology, dominant at the time. In 1988, the Federal Communications Commission (FCC) created the special category of 'value-added' services, which left computer-mediated information virtually unregulated by the government.").

[37] The Communications Decency Act (CDA) was initially subject to court review, with the most restrictive CDA provisions invalidated, but Section 230 remained, allowing the CDA to have "an immense impact . . . [b]y freeing Web platforms from liability for content on their sites uploaded by third parties, the Supreme Court ruling not only was a major victory for the tech companies of the dot-com era, but it was a massive win for the giant social media platforms yet to come." MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA 330 (2019). *See* Kornbluh, *supra* note 36, at 34. *See also* RADU, *supra* note 36, at 84 ("Being the first country to introduce protections against liability for online platforms, the United States established itself as a safe haven for Internet services, attracting the majority of providers. An outcome of this favourable legal environment was the growth of Silicon Valley into a prominent hub for high-tech innovation.").

[38] Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 642 (2014).

[39] According to Professor Chander: "U.S. privacy law offers limited constraints for American Internet entrepreneurs. The vaunted common law privacy torts are each quite narrow in scope and mostly unavailing to web users concerned about protecting personal information. The torts are not well-suited to the typical privacy concern with respect to social media, doing little to bar the use of personal information for marketing or the onward sharing of personal information in unexpected ways. Statutory protections remain quite narrow." *Id.* at 664–65.

[40] *See* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD TOGETHER IN COMMERCE 167 (2013). Several years earlier, Gregory Shaffer predicted a ratcheting up of U.S. standards as a result of EU legislation. *See* Shaffer, *supra* note 4, at 80. ("Yet the U.S.-EU conflict over data privacy protection demonstrates that in a globalizing economy, social protection levels are not necessarily driven downward in the United States.")

and the federal law of the United States.[41] Furthermore, the United States views certain types of foreign laws, such as the kinds mentioned above in connection with China and the European Union, as barriers or impediments to digital trade.[42] This might be expected given its *laissez-faire* policy perspective.[43]

C. Aims

International trade in data has grown rapidly in importance—both in terms of the amount of data flows and their financial value. As this element of globalization has developed, nations have not harmonized their data privacy laws, and various divergent models of governance have been adopted with strategic effect. The scope of this Article aims to inform companies not only of the complexities they will face in the context of cross-border data flows, but how data governance requirements and good practices are limited to the impact of EU data protection laws and their related international agreements. This Article also seeks to encourage companies to see cross-border data flows as part of an international personal data supply chain and help them realize the importance of managing such supply chain in compliance with data protection law.

---

[41] On the lack of harmonization between the United States federal law and that of the European Union, *see* Voss, *supra* note 17, at 417–27. An earlier study comparing the Chinese regime to that in Europe found that, "An assessment of the data protection regime in China would be an impossible task because . . . there is none to be found." Paul de Hert & Vagelis Papakonstantinou, *The Data Protection Regime in China*, DIRECTORATE GEN. FOR INTERNAL POL. 24 (2015) https://europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf. *But see* Louise Lucas, *China Emerges as Asia's Surprise Leader on Data Protection*, FIN. TIMES (May 29, 2018), https://www.ft.com/content/e07849b6-59b3-11e8-b8b2-d6ceb45fa9d0 (reporting the words of lawyer Richard Bird, saying that China "in some respects is the country that has embraced GDPR most directly—but in a very Chinese way," including requiring data localization and having a social credit system based on personal data).

[42] These barriers or impediments were classified into the following categories: localization barriers, data privacy and protection, intellectual property-related concerns, online censorship, and traditional impediments. The European Union is specifically cited under the category of data privacy and protection. *See Digital Trade in the U.S. and Global Economies, Part 1*, U.S. INT'L TRADE COMM'N xxi (July 2013), https://www.usitc.gov/publications/332/pub4415.pdf.

[43] For a discussion of U.S. *laissez-faire* policy and neoliberalism, *see* Voss, *Obstacles*, *supra* note 17, at 432–36.

II. LEGISLATIVE RESPONSES: DATA PRIVACY LAWS WITH EXTRATERRITORIAL EFFECT; DATA LOCALIZATION LAWS

Nation states and regions have not taken action to create international harmonization of data privacy law but have adopted divergent regulatory models with strategic effect. The EU and several states have adopted legislation that impacts international business and data flows beyond their borders.

A. Data Privacy Laws with Extraterritorial Effect: The GDPR and Company

Data privacy law with extraterritorial application exists and is being adopted in different areas of the world. This is the case in Europe with its GDPR,[44] and in the United States through state legislation.

1. The Extraterritorial Effect of the GDPR

In Europe, the EU's GDPR applies when personal data[45] is processed[46] and the material and territorial scope provisions of the GDPR are met. The material scope of the GDPR includes the processing of personal data, at least in part by automated means or as part of (or intended to form part of) a filing

---

[44] Regarding the GDPR's extraterritorial effect, *see* Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICHMOND. J.L. & TECH. no. 1, [60]-[63] (2018).

[45] Personal data is defined broadly under the GDPR, as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, and identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, *supra* note 20, art. 4(1). Salient is the fact that the data subject need not be identified by the data, only identifiable. An example is that of dynamic internet protocol (IP) addresses, which may in certain circumstances be considered personal data in the European Union, even though they do not directly identify the data subject, but when he or she is identifiable through the help of an ISP or a competent authority, for example. *See* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 318–20 (2019).

[46] "Processing" is defined broadly, as well, under the GDPR, as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, *supra* note 20, art. 4(2).

system.[47] However, it excludes such processing in the course of activities falling outside the scope of EU law,[48] such as activities concerning national security.[49] Nor does it include activities by Member States "when carrying out activities in relation to the common foreign and security policy" of the European Union.[50] In addition, it excludes processing of personal data "by a natural person in the course of a purely personal or household activity."[51] Processing by the competent authorities for the "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" is covered by a different legal instrument, and is therefore excluded from the scope of the GDPR.[52] Furthermore, personal data processing by EU institutions is covered by a different legislative act and also excluded.[53] The GDPR affords protection to natural persons "whatever their nationality or place of residence" regarding the processing of their personal data. However, the processing of personal data concerning legal persons "including the name and the form of the legal person and the contact details of the legal person" is not covered by the GDPR,[54] nor is the personal data of deceased persons.[55]

Perhaps more strikingly, the territorial scope of the GDPR reaches outward. First, the GDPR applies to the processing of personal data "in the context of the activities of an establishment of a controller or a processor in the [European Union], regardless of whether the processing takes place in the [European Union] or not."[56] While the GDPR does define the term "main

---

[47] *Id*. art. 2(1). A "filing system" is "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." *Id*. art. 4(6). However, "Files or sets of files, as well as their cover pages, which are not structured according to specific criteria" fall out of the GDPR's scope. *Id*. recital (15).

[48] *Id*. art. 2(2)(a).

[49] *Id*. recital (16).

[50] *Id*. art. 2(2)(b), recital (16).

[51] *Id*. art. 2(2)(c). This is the case for processing which is not connected to a professional or commercial activity and such processing could include "correspondence and the holding of addresses, or social networking and online activity undertaken within the content of such activities." However, the professional or commercial organizations providing the means for such processing would be covered by the GDPR. *Id*. recital (18).

[52] *Id*. art. 2(2)(d). That legislative instrument is Directive (EU) 2016/680 of the European Parliament and of the Council. *Id*. recital (19).

[53] Such other legislative act is Regulation (EC) No. 45/2001. *Id*. art. 2(3).

[54] *Id*. recital (14).

[55] *Id*. recital (27) ("This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.").

[56] *Id*. art. 3(1).

establishment,"[57] it does not define the term "establishment" itself, although the recitals give some help. There, an establishment is described as implying "the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."[58] Taking a key from the recitals, Voss and Woodcock describe the term "establishment" as referring "to place where a controller conducts the 'effective and real exercise of activities,' and has 'human and technical resources necessary' in order to achieve certain services through 'stable arrangements.'"[59] Furthermore, case law from the Court of Justice of the European Union ("CJEU") may prove instructive to interpret the part of this provision requiring a determination of whether or not an establishment in the EU is involved, even when the caselaw was rendered under the GDPR's predecessor, the 1995 Directive. However, to determine whether the processing is done in connection with the activities of such an establishment or not, a case-by-case analysis is necessary.[60]

As an example, one case rendered under the 1995 Directive provides a sense of the direction of decisions on this concept of an establishment. In the now-famous *Google Spain* case,[61] a complaint was brought by Mario Costeja González before the Spanish supervisory authority in order to obtain the removal of web pages by the Spanish newspaper *La Vanguardia* related to the forced sale of real estate to satisfy social security debts some years prior to the case. In addition, he sought delisting of search engine results including

---

[57] *Id*. art. 4(16) (for a controller with establishments in more than one EU Member State, "the place of its central administration in the [European] Union, unless the decisions and the purposes and means of the processing of personal data are taken in another establishment of the controller in the [European] Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment").

[58] *Id*. recital (22) ("Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.").

[59] *See* W. GREGORY VOSS & KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS 224 (2016) (while Voss and Woodcock were referring to the 1995 Directive, the same meaning would apply to term "establishment" as used in the GDPR).

[60] *See* Dan Jerker B. Svantesson, *Article 3. Territorial scope*, *in* THE EU GENERAL DATA PROTECTION REGULATION(GDPR): A COMMENTARY 74, 87 (Christopher Kuner et al. eds., 2020). The EPDB has also provided examples analyzing different cases under Article 3(1). *See Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, EUR. DATA PROT. BD. 5-13 (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/Files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [hereinafter *Guidelines 3/2018*].

[61] Case C-131/12, Google Spain SL v. Agencía Española de Protección de Datos (AEPD), 2014 E.C.R. 317.

such pages from the Google search engine.[62] In that case, the CJEU determined that Google Spain SL was the establishment of Google Inc. in Spain. The court also found that the U.S. company was subject to the 1995 Directive because the activities of its Spanish establishment—including the advertising—helped finance the U.S. company's search engine.[63] Referring to the later *Weltimmo* case,[64] the European Data Protection Board ("EDPB") summarized the CJEU's ruling "that the notion of establishment extends to any real and effective activity—even a minimal one—exercised through stable arrangements" where the threshold for "stable arrangements" is quite low.[65]

Next, and perhaps even more remarkably, the GDPR applies to certain companies, even if they do not have an establishment in the European Union. Article 3(2) provides as follows:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behavior as far as their behavior takes place within the Union.[66]

Furthermore, if the controller is established in the European Union, but an EU Member State's law applies through public international law, the GDPR will apply as well.[67] Where a controller or a processor does not have an

---

[62] *See* W. Gregory Voss, *The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation*, 18(1) J. INTERNET L. 3, 3–4 (2014).

[63] *Id.* at 4. Note that the "SL" in the name of Google's establishment Google Spain SL refers to its corporate form—*sociedad limitada*. *See* Mercantile Registry Regulations art. 177(1) (B.O.E. 1996, 184) (Spain). The *sociedad limitada* is one of the two most popular forms of commercial companies in Spain for business ventures, together with the *sociedad anónima*. TERESA RODRÍGUEZ DE LAS HERAS BALLELL, INTRODUCTION TO SPANISH PRIVATE LAW: FACING THE SOCIAL AND ECONOMIC CHALLENGES 106 (2010).

[64] Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, 2015 E.C.R. 639

[65] *Guidelines 3/2018, supra* note 60, at 6.

[66] GDPR, *supra* note 20, art. 3(2).

[67] *Id.* art. 3(3).

establishment in the European Union, but is subject to the GDPR by virtue of Article 3(2), the controller or processor must designate in writing a representative in the European Union,[68] unless an exception applies.[69] This representative must be established in one of the Member States where the data subjects whose data are processed are located.[70] Data subjects and supervisory authorities may address this representative either in addition to, or in the place of, the controller or processor.[71]

Exceptions are provided where processing is occasional and does not include large-scale processing of sensitive data (i.e., special categories of data) or data relating to criminal offenses, and "is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing,"[72] or where the controller or processor is a public authority or body.[73]

However, the European Union is not the only jurisdiction with data protection law that has an extraterritorial effect. This Article next looks at current and proposed U.S. state legislation with extraterritorial effect.

2. The Extraterritorial Effect of New and Proposed U.S. State Legislation

This Articles examines new and proposed U.S. state legislation with extraterritorial effect, by looking at the California Consumer Privacy Act and the proposed Washington Privacy Act.

a. California Consumer Privacy Act

In 2018, California adopted its California Consumer Privacy Act ("CCPA").[74] The law has been described as a first step to giving California

---

[68] *Id.* art. 27(1).

[69] *Id.* art. 27(2) (this would be the case where processing is only occasional and does not include large scale processing of sensitive data or data concerning criminal convictions and offenses, and "is unlikely to result in a risk to the rights and freedoms of natural persons . . . ," or where the controller or processor is a public authority or body).

[70] *Id*. art. 27(3) ("The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.").

[71] *Id*. art. 27(4).

[72] *Id*. art. 27(2)(a).

[73] *Id*. art. 27(2)(b).

[74] CAL. CIV. CODE § 1798.100–.199 (2020).

consumers rights similar to those of Europeans.[75] CCPA applies to many businesses without a California physical presence, so long as they meet certain thresholds and are doing business in that state (which can include businesses that only transact business by Internet), and may be said to have extraterritorial effect.[76] The definition of "business" includes legal entities that operate "for profit" and that either collect consumers' personal information (as broadly defined under the CCPA), or have such information collected on their behalf where they alone or jointly determine the purposes and means of the processing of such information.[77] Businesses must meet one or more of the following thresholds for the CCPA to apply:

> a) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>
> b) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

---

[75] *See* Stéphanie Le Stujon, *Le California Privacy Act : premier pas vers un RGPD américain?*, 2020 REVUE DE L'UNION EUROPÉEN 41, no. 634 (Jan. 6, 2020) ("The Californian text represents the beginning of a widespread awareness in the United States of the need to protect individuals' personal data in the digital age. This is a first step in the continuity of the GDPR.").

[76] *See* Erin Illman & Paul Temple, *California Consumer Privacy Act: What Companies Need to Know*, 75 BUS. LAW. 1637, 1640 (2019/2020). While extraterritorial reach is not a new concept in privacy, the CCPA is less explicit about its geographic scope than some other privacy regulations are. For example, the GDPR explicitly applies to the processing of personal data in the context of the activities in the European Union, whether the processing takes place in the European Union. On the other hand, while the CCPA's broad definition of "business" does not limit a business to its place of incorporation or physical presence, it also does not explicitly apply to companies outside California. However, given the definition of "doing business" referenced above, the result is that the CCPA will have an extraterritorial impact on companies that have no physical presence in California. *Id.* at 1640-41. One law firm warns its U.K. clients that, "The reach of the CCPA extends beyond California and the US; it may apply to businesses based in the UK depending on the level of interaction with California residents and their personal information." John Timmons et al., *UK Business Exposure to the California Consumer Privacy Act 2018 ("CCPA")*, WHITE & CASE (Jan. 31, 2020), https://www.whitecase.com/publications/alert/uk-business-exposure-california-consumer-privacy-act-2018-ccpa; *see also* Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, INT'L ASS'N OF PRIVACY PROF. (Jul. 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/ ("As of January 1, 2020, companies around the world will have to comply with additional regulations related to processing of personal data of California residents.").

[77] *See* Illman & Temple, *supra* note 76, at 1638–39. The requirement that companies determine the purposes and means of the processing nearly tracks the definition of "controller" in the GDPR, replacing "personal data" by "consumers' personal information," instead. GDPR, *supra* note 20, art. 4(7).

c) Derives 50 percent or more of its annual revenues from selling consumers' personal information.[78]

Thus, if at least one of the above thresholds is met, the CCPA will apply to the businesses described in this paragraph even if they do not have a physical presence in California.

b. Proposed Washington Privacy Act

While it is only a bill at this stage, the State of Washington also has a proposal for a data privacy law with extraterritorial scope—Second Substitute Senate Bill 6281,[79] with the short title "Washington Privacy Act."[80] The proposed Washington Privacy Act would apply to legal entities that conduct business in the State of Washington or that "produce products or services that are targeted to residents of Washington"[81] provided one or more of the following thresholds is met:

a) During a calendar year, controls or processes personal data of one hundred thousand consumers or more; or

b) Derives over fifty percent of gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand consumers or more.[82]

It is interesting to note that the GDPR's influence is cited in the legislative findings of the Washington Privacy Act:

> [T]he European Union's general data protection regulation has continued to influence data privacy policies and practices of those businesses competing in global markets. In the absence of federal standards, Washington and other states across the United States are analyzing elements of the European Union's general data protection regulation to enact state-based data privacy regulatory protections.[83]

---

78 CAL. CIV. CODE § 1798.140(c)(1) (2020).
79 Second Substitute S. B. 6281, 66th Leg., 2020 Reg. Sess. (Wash. 2020).
80 *Id.* § 1.
81 *Id.* § 4(1).
82 *Id.* § 4(1)(a)–(b).
83 *Id.* § 2(3).

Thus, European and certain U.S. states have adopted or are adopting data privacy law with extraterritorial effect, expanding the reach of their laws beyond their shores. U.S. states are being influenced by the GDPR. However, further complexity is added by other nations, which have adopted data localization laws.

B. Data Localization Laws

Taking a different approach, certain other nations are dealing with the question of data flows by imposing data localization requirements. This has notably been the case with China and Russia.

1. China's Cybersecurity Law

China has imposed a requirement of data storage within its borders on companies.[84] Reflecting the priority given to data localization in Beijing, China's Cybersecurity Law took effect on June 1, 2017,[85] and its Article 37 provides as follows:

> Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.[86]

---

[84] *See* Segal, *supra* note 22, at 12.

[85] Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[86] Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, NEW AMERICA (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (This text is from unofficial translation of the Chinese Cybersecurity Law, provided by the New America think-tank).

Yuxi Wei argues that the adoption of this data localization regulation should be taken as an indication that "all foreign companies are required to cooperate with Chinese data centers for data storage."[87]

China's law was proceeded by that of its large Eurasian neighbor—Russia.

a. Russia's Data Localization Law

Countries other than China have adopted data localization requirements for personal data, as well. Notably, Russia has adopted a law requiring that all databases storing personal data of Russian citizens be physically situated in Russia.[88] It provides:

> During personal data collection, inter alia, through the Internet, the operator shall ensure that databases located within the Russian Federation are used to record, systematize, accumulate, store, clarify (update or modify) and retrieve personal data of citizens of the Russian Federation, except for cases specified in clauses 2, 3, 4, 8 of part 1 of Article 6 of this Federal Law.[89]

To a certain extent, the revelations by Edward Snowden of the U.S. National Security Agency's mass surveillance programs motivated calls for such requirements,[90] in addition to advancing work on the GDPR prior to its

---

[87] *See* Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, HENRY M. JACKSON SCH. OF INT'L STUD., U. WASH. (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

[88] *Id*.

[89] Federal'nyy zakon No. 242-FZ ot 21 iyulya 2014 g. O vnesenii izmeneniy v nekotoryye zakonodatel'nyye akty Rossiyskoy Federatsii v chasti, kasayushcheysya obnovleniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh [Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks], FEDERAL'NYY ZAKON [FZ] [Federal Law] 2014, No. 242-FZ art. 2 (Rus.).

[90] *See* W. KUAN HON, DATA LOCALIZATION LAWS AND POLICY: THE EU DATA PROTECTION INTERNATIONAL TRANSFERS RESTRICTION THROUGH A CLOUD COMPUTING LENS xii (2017) ("Calls for further and tighter data localization laws were spurred particularly by contractor Edward Snowden's revelations in 2013 ('Snowden's revelations') of mass collection and interception, by the US National Security Agency (NSA), the UK intelligence agency (GCHQ) and other authorities, of the digital data of many countries' citizens.").

adoption.[91] Moreover, W. Kuan Hon refers to the EU personal data transfer restriction (in its 1995 Directive version) as being "invoked to regulate personal data's physical location as such rather than to ensure that transferred personal data are processed in compliance with substantive [1995 Directive] Principles."[92]

C. Conclusion Regarding Legislative Responses

Legislative responses to the lack of internationally-harmonized data privacy law have resulted in differing laws with extraterritorial effect—notably those of the European Union and California—in addition to data localization laws such as those of China and Russia. These legislative developments have led to what has been called "the splinternet," describing the trend towards the fragmentation of the internet, and cautioning of the risk of economic damage, the hampering of digital innovation, and the restriction of free speech.[93] This context necessitates a study of recent concerns and risks and an analysis of their lessons for business. Foreign regulation and geopolitical considerations, sometimes reflecting foreign strategic aims, are elements of the geopolitical environment of international cross-border data flows. Companies must understand these complexities in order to comply with data privacy laws that apply up and down the data flow supply chain. Importantly, they must also understand and comply with the EU's cross-border personal data transfer restriction and any relevant international agreements intended to allow for cross-border data flows.

III. THE EU'S CROSS-BORDER PERSONAL DATA TRANSFER RESTRICTION AND INTERNATIONAL AGREEMENTS RELATED TO IT

Both current and prior EU data protection legislation include a cross-border restriction to personal data transfer in certain circumstances, although the Commission has negotiated international agreements in order to allow data to continue to flow. This Section analyzes the restriction on cross-border

---

[91] See W. Gregory Voss, *Looking at European Union Data Protection Law Reform through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17(9) J. INTERNET L. 1, 20 (2014) ("The Snowden disclosures likely had a role in obtaining the LIBE Committee vote in Parliament and moving the GDPR forward.").

[92] *Id*. at 318.

[93] *Lost in the Splinternet*, ECONOMIST (Nov. 5, 2016), https://www.economist.com/international/2016/11/05/lost-in-the-splinternet.

personal data transfer in the EU legislation and international agreements. prior.

A. The Restriction on Cross-Border Transfers of Personal Data in EU Legislation

The precursor EU data protection legislation to the GDPR, EU Directive 95/46/EC (the "1995 Directive"),[94] sets out dual objectives in its first Article:

> 1) In accordance with this Directive, Member States shall protect the fundamental rights and freedom of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.[95]

While the fundamental right focus is listed first, the second objective is equally important as targeting the development of the single market in the European Union. A new fifth freedom—the free movement of personal data[96]—was set to join the existing four freedoms: the free movement of goods, services, capital, and persons.[97] The idea was to further increase integration of what was the previously known as the common market, allowing transfers personal data within that economic space by businesses in

---

[94] 1995 O.J. (L 281) 31 [hereinafter 1995 Directive].

[95] *Id*. art. 1. The corresponding provisions in the GDPR parallel those of the 1995 Directive, with an introductory phrase on the subject matter of the GDPR having been added. They are as follows: "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data." GDPR, *supra* note 20, art. 1.

[96] *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 50 (2015) ("the EU chose to ensure the free flow of data via positive integration by creating a harmonized legal environment, via the [1995] Directive, in order to eliminate all disparities which would create obstacles to the free flow of personal data").

[97] *See* GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 134 (2014) ("The principles of the free movement of goods, persons, services and capital have always been contemplated as of crucial importance for Community law"). Fuster describes the link between the free flow of personal data and these four freedoms, while commenting that, "It remains nevertheless unclear whether the free flow (or movement) of data serves the free movement of goods, persons, services or capital." *Id*. at 135 (citation omitted).

connection with activities conducted across national borders, and for scientific and other purposes, while harmonizing Member State data protection law,[98] as the 1995 Directive had to be implemented by national legislation. Orla Lynskey explains that there was no basis for removing obstacles to the free flow of such data in the European treaties, so the European Union chose instead to use the basis of improvement of the functioning of the internal market for the EU data protection legislation.[99]

While the 1995 Directive aimed at allowing personal data to flow freely within the boundaries of the European Union, it introduced a cross-border personal data transfer restriction on certain transfers to countries outside the European Union. It required that the receiving country (called a "third country") ensure "an adequate level of protection" for such personal data.[100] That adequacy of the protection was to be "assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations," including "the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."[101]

The transfer restriction was intended to ensure that companies not try to avoid the 1995 Directive by engaging in processing operations outside of the European Union.[102] It had an impact, as several countries modified their legislation to attempt to comply with adequacy requirements. But the United States encouraged self-regulatory measures instead,[103] as is consistent with the self-regulatory nature of U.S. federal data privacy policy.[104]

---

[98] *See* ORLA LYNSKEY, *supra* note 96, at 49 (2015) (citation omitted).

[99] *Id*. at 50. Indeed, Lynskey comments that, "as a result of the EU's lack of competence to enact fundamental rights legislation" the Court of Justice of the European Union (CJEU) "initially emphasized data protection's market integration objective while treating its fundamental rights dimension with caution." *Id*. at 47.

[100] 1995 Directive, *supra* note 94, art. 25(1).

[101] *Id*. art. 25(2).

[102] *See* DREZNER, *supra* note 3, at 104.

[103] "This threat was proved sufficiently potent for Australia, Canada, and Eastern European countries to revise their own laws in an attempt to comply with EU preferences. However, the U.S. response was to encourage American multinationals to establish self-regulatory mechanisms that would meet EU standards. Sets of voluntary principles, such as those provided by TRUSTe and BBBOnline, were developed." *Id.*

[104] *See* Voss, *supra* note 17, at 435.

The United States was not considered to be ensuring an adequate level of protection,[105] and the data transfer restriction's "potentially detrimental impact on [U.S.] business interests" was feared. With up to $120 billion in trade under threat,[106] the European Union and the United States negotiated an international agreement, known as the "Safe Harbor" scheme.[107] This agreement and its successor, the Privacy Shield, are discussed below. However, prior to the finalization of the Privacy Shield, the European Union adopted the GDPR, which repealed and replaced the 1995 Directive on May 25, 2018.[108]

While the GDPR contains changes from the 1995 Directive, it is more an evolution of the law rather than a "radical departure" from the prior approach, specifically in the area of transfers of personal data to third countries.[109] The GDPR sets out the general principle that transfers of personal data undergoing processing (or to be processed after transfer), either outside of the European Union or to an international organization, comply with the GDPR's Chapter V. The GDPR requires such compliance in order "to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined."[110] Onward transfers are also subject to this requirement.[111] Although the term "onward transfers" is not defined, it refers to further transfers to another country outside of the European Union (or European Economic Area), or to another international organization, which are common in practice.[112]

---

[105] *See* Randi Bessette & Virgina Haufler, *Against All Odds: Why There Is No International Information Regime*, 2 INT'L STUD. PERSP. 69, 81 (2001) ("the United States steadfastly argued that personal information transferred to the United States would be adequately protected by industry self-regulation. The European Union consistently refused to accept the U.S. system as providing adequate privacy protections under the Data Directive. The U.S. negotiators went back to the drawing board a number of times to try to modify their proposals while still clinging to self-regulation as the underlying principle for protecting privacy.").

[106] *See* Lee A. Bygrave, Data Privacy Law: An International Perspective 194 (2014).

[107] *Id*. at 195.

[108] GDPR, *supra* note 20, arts. 94 and 99.

[109] *See* CHRISTOPHER KUNER, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 755 (Christopher Kuner et al., eds., 2020).

[110] GDPR, *supra* note 20, art. 44. This obligation applies to both controllers and processors. It should be noted that, unlike the GDPR, the CCPA contains no cross-border transfer restriction. *See* Illman & Temple, *supra* note 76, at 1646.

[111] GDPR, *supra* note 20, art. 44 (". . . including for onward transfers of personal data from the third country or international organization to another third country or to another international organization.").

[112] Kuner, *supra* note 109, at 763 ("Onward transfers are common in practice, since data are often re-exported to third parties by a data importer." An example is the outsourcing of a data base to a data importer in a third-party country who then outsources the data base maintenance to another third-party company.").

Transfers may be made on the basis of a European Commission adequacy decision, where the Commission has "decided that the third country, a territory or one or more specified sectors with that third country, or the international organization in question ensures an adequate level of protection."[113] Commission adequacy decisions exist for Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States (but solely under the Privacy Shield framework), and adequacy discussions are ongoing with South Korea.[114] This is a far cry from a majority of the total 194 countries of the world, or of the remaining number when deduction is made for the Member States of the European Union.[115]

For those remaining nations not benefitting from a Commission adequacy decision, other grounds must exist for cross-border personal data transfers to be made—what the GDPR refers to as "appropriate safeguards."[116] These appropriate safeguards are intended to "compensate for the lack of data protection" in the destination country,[117] and may include "a legally binding and enforceable instrument between public authorities or bodies,"[118] binding

---

[113] GDPR, *supra* note 20, art. 45(1). An "international organisation" is defined as "an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries." *Id.* art. 4(26). The GDPR sets out criteria to be taken into account when assessing the adequacy of the level of protection, such as the rule of law, respect for human rights, relevant legislation, "including rules for the onward transfer of personal data to another third country . . . ." *Id*. art. 45(2)(a). Furthermore, the existence and functioning of an independent supervisory authority and the international commitments in relation to the protection of personal data figure among the criteria. *Id*. art. 45(2)(b)-(c). However, in order to be considered adequate, the level of protection need not be identical to that of the European Union, but "essentially equivalent," instead. *See* Voss, *Obstacles*, *supra* note 17, at 459.

[114] *Adequacy Decisions*, EUROPEAN COMMISSION (last visited Feb. 25, 2020), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[115] *See How Many Countries Are In The World?*, WORLDATLAS, https://www.worldatlas.com/nations.htm (last visited on Feb. 25, 2020) (There are approximately 194 countries in existence in the world, although measures vary); *see also Countries*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/countries_en (last visited on Feb. 25, 2020) (Out of this total, the total Member States of the European Union—27 after Brexit—must be deducted); *Adequacy Decisions*, *supra* note 114 (out of approximately 167 nations that would need an adequacy decision in order to allow the free flow of personal data of individuals in the European Union to such countries, only those listed above have received such a decision).

[116] GDPR, *supra* note 20, art. 46(1).

[117] *Id*. recital 108.

[118] *Id*. art. 46(2)(a).

corporate rules ("BCRs"),[119] standard data protection clauses adopted by the Commission[120] or by a supervisory authority and approved by the Commission,[121] an approved code of conduct[122] or an approved certification mechanism[123] together with "binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights."

Furthermore, there exist certain "derogations"[124] to the cross-border personal data transfer restriction contained in the GDPR, when a transfer may be made without an adequacy decision or appropriate safeguards. First, a derogation is available where the data subject has given explicit informed consent to the transfer.[125] Alternatively, a derogation may apply when the transfer is necessary for one of the following five reasons: (1) "the performance of a controller-data subject contract;[126] (2) the conclusion or performance of a contract "concluded in the interest of the data subject;"[127] (3) "important reasons of public interest;"[128] (4) "the establishment, exercise or defense of legal claims;"[129] or (5) "in order to protect the vital interests of

---

[119] *Id*. art. 46(2)(b). Binding corporate rules are defined as "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity." *Id*. art. 4(20). An enterprise is defined as "a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity." *Id*. art. 4(18). Finally, a "group of undertakings" means "a controlling undertaking and its controlled undertakings." *Id*. art. 4(19).

[120] *Id*. art. 46(2)(c). These are contractual clauses are entered into by the European Union-located data exporter and the data importer in a third country and set out obligations to provide certain personal data protections. The text of the clauses is standardized and adopted by the European Commission. *See* Kuner, *supra* note 109, at 799.

[121] GDPR, *supra* note 20*,* art. 46(2)(d). These are similar to the contractual clauses mentioned *supra* note 109. The difference is that they are adopted by a supervisory authority (instead of the Commission), followed by an approval of the Commission.

[122] *Id*. art. 46(2)(e).

[123] *Id*. art. 46(2)(f).

[124] *See* F.H.S. BRIDGE, THE COUNCIL OF EUROPE FRENCH-ENGLISH LEGAL DICTIONARY 78 (1994) ("Derogation" is a term used in the European Union—even in English—which may be translated from the French "*dérogation*" as ". . . exclusion from the effect of a provision; exemption; . . . exception.").

[125] The data subject must be informed "of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards." GDPR, *supra* note 20, art. 49(1)(a).

[126] This derogation also includes where the transfer is necessary for "the implementation of pre-contractual measures taken at the data subject's request." *Id*. art. 49(1)(b).

[127] This derogation reads as follows: "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person." *Id*. art. 49(1)(c).

[128] *Id*. art. 49(1)(d).

[129] *Id*. art. 49(1)(e).

the data subject or other persons, where the data subject is physically or legally incapable of giving consent."[130] Finally, a derogation is available where the personal data transfer is from a public register open for consultation, where EU or Member State law conditions for consultation are met in the specific case.[131] There is a final, limited basis for derogation: if no other derogation applies and no other basis for transfer (such as an adequacy decision or appropriate safeguards) exists. This involves a transfer that is "not repetitive, concerns only a limited number of data subjects," and is necessary for the controller's legitimate interests, "which are not overridden by the interests or rights and freedoms of the data subjects."[132] In such case, the controller must, *inter alia*, provide suitable safeguards for the protection of the personal data and inform both the supervisory authority and the data subject of the transfer, and also inform the data subject as to the legitimate interests in question.[133]

The concept of cross-border personal data transfer restrictions is not unique to the European Union. For example, the Organization for Economic Co-operation and Development ("OECD"), an organization that today includes most of the EU Member States, the United States, Canada, and other advanced and emerging countries[134] established the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines").[135] These are nonbinding, but influential guidelines that permit legitimate restrictions to the free flow of personal data, as shown in the table in this Article's Annex. Legitimate restrictions were also allowed in the 2013 modernization text of the OECD Guidelines,[136] although these have been

---

[130] *Id*. art. 49(1)(f).

[131] "[T]he transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case." *Id*. art. 49(1)(g). However, the transfer under this derogation shall not involve "the entirety of the personal data or entire categories of the personal data contained in the register," and if the consultation is done by persons "having a legitimate interest," such persons must either request the transfer or be the recipients of the data. *Id*. art. 49(2).

[132] *Id*. art. 49(1).

[133] *Id*.

[134] *See Where: Global Reach*, OECD, http://www.oecd.org/about/membersandpartners/ (last visited on Feb. 24, 2020).

[135] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)*, ORG. FOR ECON. COOPERATION & DEV., http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[136] The OECD Privacy Framework (2013): Annex: Guidelines governing the protection of privacy and transborder flows of personal data, ORG. FOR ECON. COOPERATION & DEV. (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

modified from the earlier version of the OECD Guidelines, as also shown in the Annex.

Furthermore, both the Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("Convention 108")[137] and the Modernized Convention 108 ("Convention 108+")[138] permit restrictions on the cross-border transfer of personal data under certain circumstances. The Council of Europe has prepared a comparative table on the corresponding texts of Convention 108, with amendments, and those of Convention 108+.[139] However, the United States is a party to neither of these two versions of Convention 108,[140] although the European Commission has encouraged it to become one.[141]

Moreover, the Commission negotiated an exemption for data protection from the General Agreement on Trade in Services ("GATS"), intended to protect it against possible challenges by the United States.[142] The relevant general exemption of the GATS is as follows:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services,

---

[137] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108.

[138] Convention 108+, Convention for the protection of individuals with regard to the processing of personal data, COUNCIL OF EUR., https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (last visited on May 6, 2020).

[139] *Modernisation of Convention 108: Comparative table: Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS 108)*, COUNCIL OF EUR., https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (last visited on Mar. 4, 2020).

[140] *See Chart of Signatures and Ratifications of Treaty 108: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, COUNCIL OF EUR. (status as of Feb. 25, 2020), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=2ZBNRLeZ; *Chart of Signatures and ratifications of Treaty 223: Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, COUNCIL OF EUR. (status as of Feb. 25, 2020), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.

[141] *See* EUR. COMM'N, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND TO THE COUNCIL ON THE SECOND ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD, at 6 (2018).

[142] *See* FARRELL & NEWMAN, *supra* note 5, at 32 ("In order to prevent the trade regime from affecting European privacy rules, the European Commission negotiated a privacy exemption from the General Agreement on Trade in Services, which entered into force in the mid-1990s. This exemption, in turn, stymied future U.S. efforts to challenge EU privacy rules as a protectionist barrier to services trade." (citation omitted)).

> nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: . . . (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: . . . (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;[143]

Various commentators have noted that no case has yet been brought where the exemption for data protection has been used as a defense.[144] Furthermore, when the European Union and the United States were negotiating the Transatlantic Trade and Investment Partnership Agreement ("TTIP"), data protection was seen as a blocking issue, given transatlantic divergence on the issue.[145] Some may argue that "contrary to popular perception, internet security and privacy can promote free flow of data and trade in digital services, provided they are consistent and reasonable and promote global, interoperable standards."[146] However, the GATS and the proposed TTIP are not the only international agreements germane to our discussion of cross-border data flows.

B. The Role of International Agreements

International agreements help ensure the cross-border transfer of personal data, as will be shown in this Section. One past international agreement affecting transatlantic data flows has already been mentioned in this Article: the U.S.-EU Safe Harbor Framework. The Safe Harbor Framework, which one U.S. congresswoman referred to as "a little-known

---

[143] General Agreement on Trade in Services, art. XIV (c)(ii), https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

[144] *See*, *e.g.*, Diane A. MacDonald & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUS. J. INT'L L. 625, 638 (2014) ("The GATS exception for the protection of the privacy of personal data has neither been tested by a disputed resolution panel nor attracted much interest in the otherwise lively GATS negotiations." (citation omitted)). *See also* Joshua D. Blume, *Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy, Localization and Cybersecurity Laws*, 49 GEO. J. INT'L L. 801, 819 (2018).

[145] *See* Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEO. J. INT'L L. 407, 438 (2017) ("[T]he approaches of the U.S. and EU towards the protection of privacy are at this stage hardly reconcilable" (citation omitted)).

[146] Neha Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, 52 VAND. J. TRANSNAT'L L. 463, 501 (2019).

trade agreement between the United States and the European Union,"[147] resulted from negotiations between the U.S. Department of Commerce and the European Commission in 2000, shortly after the 1995 Directive and its cross-border personal data transfer restriction were to be transposed into EU Member State national law in 1998.[148]

The Safe Harbor involved companies self-certifying to comply with the Safe Harbor Framework principles, which would result in their being considered to be in compliance with the substance of the 1995 Directive, especially insofar as data subject rights are concerned.[149] In turn, the companies were able to transfer personal data across the Atlantic to the United States, which was a country that did not otherwise benefit from an adequacy determination. Companies were also subject to the jurisdiction of U.S. entities, principally the Federal Trade Commission, in case of violation of the company's undertakings.[150]

However, U.S. compliance with the 1995 Directive and the Safe Harbor has been described as "uncertain."[151] The FTC failed to be proactive in monitoring Safe Harbor compliance prior to 2009, and to enforce it prior to 2011.[152] Early EU reviews of the Safe Harbor raised concerns about non-compliance and lack of enforcement on the U.S. side, but the FTC and the U.S. Department of Commerce did not take any action as a result.[153]

In 2013, following the Edward Snowden revelations, which showed that several Safe Harbor-certified companies where transferring personal data to U.S. authorities, the Commission issued documents aimed at restoring trust in EU-U.S. data flows, including certain calls for action targeting both the

---

[147] Anna G. Eshoo, *Safe Harbor 2.0*, CONGRESSWOMAN ANNA G. ESHOO (Nov. 18, 2015), https://eshoo.house.gov/media/op-eds/safe-harbor-20.

[148] *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19(11) J. INTERNET L. 8, 9 (May 2016). *See also* DREZNER, *supra* note 3, at 104-105.

[149] *See* Voss, *The Future*, supra note 148, at 9.

[150] *Id.*

[151] *See* DREZNER, *supra* note 3, at 105.

[152] *See* Voss, *The Future*, *supra* note 148, at 11. *See also* Chris Connolly & Peter van Dijk, *Enforcement and Reform of the EU-US Safe Harbor Agreement*, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 261, 277, 278–81 (David Wright & Paul De Hert, eds., 2016) (the authors speak of "long periods (2000–2008, 2010–2011 and 2012–2013) with absolutely no enforcement activity).

[153] *Id.* at 263.

United States and the European Union.[154] The Snowden revelations in turn informed an important case before the CJEU, *Schrems I*, that would ultimately invalidate the Safe Harbor Framework.[155]

In *Schrems I*, Schrems—an Austrian national[156]—brought a complaint against the supervisory authority of Ireland for having rejected a complaint against Facebook.[157] He based his claim mainly on the Safe Harbor, the mechanism under which Facebook's Irish subsidiary (Facebook Ireland Ltd.) would transfer his personal data to the United States.[158] There, the U.S. authorities would be able to access the data, he claimed, and there would not be adequate protection against mass surveillance.[159] Facebook Ireland Ltd. was the data controller under the 1995 Directive, which gave the Irish supervisory authority jurisdiction.[160] The case went up to the CJEU, which invalidated the Safe Harbor Framework.[161]

Now that the Safe Harbor could no longer be used, a new international agreement was needed in order to ensure transatlantic cross-border data flows. Thousands of companies had to find another basis for adequacy in order to ship personal data to the United States.[162] Following intense negotiations (and re-negotiations)[163] the Privacy Shield Framework—a new international

---

[154] Examples of these calls for action include, but are not limited to, quickly adopting the GDPR, strengthening the Safe Harbor and having U.S. legislation protect the personal data of those in the European Union, and not just U.S. citizens. *See* VOSS & WOODCOCK, *supra* note 59, at 70; Eur. Comm'n, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM (2013) 847 final (Nov. 27, 2013), https://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_en.pdf.

[155] Case C-362/14, Schrems v. Data prot. Comm'r (Oct. 6, 2015), http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en.

[156] *Id*. ¶ 26.

[157] *Id*. ¶ 2.

[158] *Id*. ¶ 67 (in the case, the Safe Harbor is referred to by the number of the Commission's Safe Harbor adequacy decision: Decision 2000/520).

[159] *Id*. ¶ 28

[160] *See* Voss, *The Future*, *supra* note 148, at 10.

[161] *See id.*

[162] *See id*. at 10–11.

[163] *See id*. at 11–12 (providing a feel for some of this procedure).

agreement—was adopted, and an adequacy decision was issued by the Commission.[164]

Broadly speaking, the Privacy Shield provided additional protections to data subjects. These included commitments from U.S. government entities buttressing protections such as those of the data protection principles (for example, purpose limitation). In addition, the Privacy Shield included recourse mechanisms for data subjects, such as arbitration and an Ombudsperson, and certain limitations on data retention and onward transfers of personal data.[165] However, the Privacy Shield is not a compliance mechanism for the GDPR, as such. It merely serves as the basis for meeting the requirements of the GDPR's cross-border transfer provisions. It does so by providing grounds for considering that Privacy Shield-certified U.S. organizations ensure adequate protection to personal data.[166]

While the Privacy Shield is one form of appropriate safeguard to the cross-border transfer of personal data, it is also subject to control in the form of an annual review by the Commission[167] and through the courts when challenges are made under the fundamental rights to privacy and data protection (such as the *Schrems I* case involving its predecessor, the Safe Harbor, discussed above). The Privacy Shield passed its first two annual reviews, with certain improvements made to its operations, as noted by the

---

[164] *See* Commission Implementing Decision of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield and Annexes 1–7, 2016 O.J. (L 207) 1, 1–112, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

[165] W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221, 231–32 (2016).

[166] *FAQs – General*, PRIVACY SHIELD FRAMEWORK (last visited on Mar. 5, 2020), https://www.privacyshield.gov/article?id=General-FAQs ("Q. Will the Privacy Shield continue to serve as a data transfer mechanism under the EU General Data Protection Regulation (GDPR)? . . . It is important to note that Privacy Shield is not a GDPR compliance mechanism, but rather is a mechanism that enables participating companies to meet the EU requirements for transferring personal data to third countries, discussed in Chapter V of the GDPR.").

[167] The annual review of Privacy Shield Framework takes the form of a "Joint Review Mechanism of the Functioning of the Privacy Shield," described as follows: "The Department of Commerce, the FTC, and other agencies, as appropriate, will hold annual meetings with the Commission, interested DPAs, and appropriate representatives from the Article 29 Working Party, where the Department will provide updates on the Privacy Shield program. The annual meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield, including referrals received by the Department from DPAs, the results of ex officio compliance reviews, and may also include discussion of relevant changes of law." *Annex 1 - Letter from Acting Under Secretary for International Trade Ken Hyatt*, https://seersco.com/law/letter-from-acting-under-secretary-for-international-trade-ken-hyatt/#%20https://seersco.com/law/category/eu-us-privacy-shield/intro/.

Commission, and remaining points open.[168] It also made it through its third annual review, although the Commission noted several points for improvement, including a point regarding onward transfers:

> In the context of its spot-check procedure, the Department of Commerce should assess companies' compliance with the Accountability for Onward Transfers Principle, including by making use of the possibility provided by the Privacy Shield to request a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company for the purposes of onward transfer.[169]

The Commission requested that the Department of Commerce use its powers to obtain information about contracts for the purposes of onward transfer. The EDPB followed this up with a call for greater enforcement of the Privacy Shield. The EDPB referred to "lack of substantial checks," specifically in the area of onward transfers, in which it seconded the Commission's request and gave background for why it was important:

> Since onward transfers possibly lead to transfers of data outside of the jurisdiction of the U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance that the competent U.S. authorities closely monitor the practical implementation of the Privacy Shield's "Accountability for the Onward Transfers Principle".[170]

Thus, there is a push for greater monitoring of onward data transfers, including those from the United States to potentially other countries.

Furthermore, although appropriate safeguards have received an adequacy decision by the Commission, this does not guarantee that they will

---

[168] *See* Kimberly A. Houser & W. Gregory Voss, *The European Commission on the Privacy Shield: All Bark and No Bite?*, U. ILL. J.L. TECH. & POL'Y: TIMELY TECH (Dec. 20, 2018), http://illinoisjltp.com/timelytech/the-european-commission-on-the-privacy-shield-all-bark-and-no-bite/.

[169] Eur. Comm'n, *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*, COM (2019) 495 final, Oct. 23, 2019, at 8, https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.

[170] EUR. DATA PROT. BD., *EU - U.S. Privacy Shield – Third Annual Joint Review*, Nov. 12, 2019, at 5, https://edpb.europa.eu/sites/edpb/files/files/file1/edpbprivacyshield3rdannualreport.pdf_en.pdf.

be upheld in the courts. This could fragilize certain companies' bases for cross-border personal data transfers to countries not having otherwise received an adequacy decision, much in the way the *Schrems I* case was decided. From the start, the Privacy Shield has risked facing challenge,[171] and in the more recent *Schrems II* case, the use of standard contract clauses as an appropriate safeguard has also come under attack.[172] Although the Advocate General in that case has weighed in on confirming the validity of standard contract clauses,[173] his comment is no guarantee that the CJEU will follow.

Finally, the European Union is seeking to obtain other international agreements in the context of the negotiation of trade deals. In January 2019, the European Commission issued an adequacy decision for Japan,[174] allowing transfers of personal data in both directions between the trading partners subject to "Supplementary Rules providing for a higher level of protection of an individual's rights and interests regarding the handling of personal data received from the EU based on an adequacy decision," that are "binding on a personal information handling business operator that receives personal data transferred from the EU."[175] The negotiation of the adequacy decision was

---

[171] *See* Voss, *The Future*, *supra* note 148, at 16.

[172] *See* Houser & Voss, *supra* note 168 ("Following the invalidation of the Safe Harbor, Schrems reformulated his lawsuit (Schrems II) to object to Facebook's use of SCCs to transfer personal data to the U.S. for reasons similar to those of Schrems I. In April 2018, the Irish High Court transferred the case to the ECJ for consideration of eleven questions. The underlying substantive issue is whether the U.S. government's surveillance program violates the right to data protection under the European Charter of Fundamental Human Rights." (citations omitted)).

[173] The Advocate General stated: "I propose that the Court answer the questions for a preliminary ruling referred by the High Court, Ireland, as follows: Analysis of the questions for a preliminary ruling has disclosed nothing to affect the validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016." *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximilian Schrems, 2019 EUR-Lex CELEX LEXIS 1145, ¶ 343 (Dec. 19, 2019), http://curia.europa.eu/juris/celex.jsf?celex=62018CC0311&lang1=en&type=TXT&ancre=. *Id.* ¶ 7 (Interestingly, in a preface seemingly acknowledging the importance of the future court decision on cross-border data flows and trade, while also recognizing fundamental rights, the Advocate General prefaced the discussion by saying that the analysis would be, "guided by the desire to strike a balance between, on the one hand, the need to show a 'reasonable degree of pragmatism in order to allow interaction with other parts of the world', and, on the other hand, the need to assert the fundamental values recognised in the legal orders of the Union and its Member States, and in particular in the Charter.").

[174] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, 2019 O.J. (L 76) 1, (Mar. 19, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=EN.

[175] *Id.* at 38 (Annex 1 - Supplementary Rules Under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU Based on an Adequacy Decision).

linked to trade talks leading to an EU-Japan trade agreement.[176] Because of the importance of cross-border data flows to the international economy, the European Union is extending the reach of its data privacy standards in parallel with international trade agreement negotiations. As it earlier indicated was its intent "[h]aving completed the EU's data protection rules, the Commission is now setting out a strategy on promoting international data protection standards."[177]

In deciding which nations to target, the Commission looks at the actual or potential commercial relations with the country. This includes: whether a free trade agreement exists or is being negotiated with such country, the data flows between the European Union and such country, the role the country might serve as a model for its region in privacy and data protection, and the political relationship with such country.[178] In early 2017, the Commission indicated its targets for future adequacy agreements were the following:

> The Commission will actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea, and, depending on progress towards the modernization of its data protection laws, with India, and also with countries in Latin America and the European neighborhood which have expressed an interest in obtaining an "adequacy finding."[179]

Thus, consistent with the concept of rival standards,[180] the European Union is actively promoting its concept of data protection—including its data protection principles for data governance—around the world through international trade ties.

---

[176] The European Commission stated, in discussing the adequacy decision: "This arrangement will also complement the EU-Japan Economic Partnership Agreement as European companies will benefit from free data flows with this key commercial partner, as well as from privileged access to the 127 million Japanese consumers. The EU and Japan affirm that, in the digital era, promoting high privacy and personal data protection standards and facilitating international trade must and can go hand in hand." *See* European Commission Press Release IP/18/5433, International data flows: Commission launches the adoption of its adequacy decision on Japan (Sept. 5, 2018), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433.

[177] European Commission Memoranda MEMO/17/15, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers (Jan. 10, 2017), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15.

[178] *Id.*

[179] *Id.*

[180] *See* Drezner, *supra* note 3.

C. Conclusion Regarding the EU Cross-Border Transfer Restriction and International Agreements

In summary, the European Union has continued the cross-border personal data transfer restriction introduced in the 1995 Directive, into the GDPR. This provision, without something more, would have braked international personal data transfers to the United States and to other nations not considered to provide adequate protection for personal data. International agreements such as the Privacy Shield and the agreement on an adequacy decision (and Supplementary Rules) with Japan permit the Commission to establish an adequacy finding. In the cases of the United States and Japan, the finding was given in consideration of for guarantees provided by such countries (and by companies, under the Privacy Shield) that allow the countries to be considered to provide an adequate level of data protection. This in turn permits personal data transfers to such countries from the European Union under the GDPR. Other agreements and elements of agreements, such as BCRs and standard contractual clauses provide the same function. Prudence must be exercised in connection with the use of such instruments, due to challenges against the Privacy Shield and standard contractual clauses in the courts and monitoring of court proceedings must be done. In addition, another form of international agreement—contracts—are essential in managing the personal data global supply chain, especially in the context of onward transfers under the Privacy Shield. We will discuss contracts further in our analysis of data governance under the GDPR and the Privacy Shield in Part IV.

IV. DATA GOVERNANCE UNDER THE GDPR AND THE PRIVACY SHIELD

One definition of "data governance," described by its author as a narrow one, is "a framework which formalizes the roles, functions, and procedures within which an organization's data is well managed and enabled as a strategic asset."[181] It is based on processes and requires a thorough understanding of a company's business, the data it holds, and the relationships between such data.[182] Data governance processes and policies manage data

---

[181] *See* Barbara L. Cohn, *Data Governance: A Quality Imperative in the Era of Big Data, Open Data, and Beyond*, 10 ISJLP 811, 813 (2015).

[182] *Id*. at 814.

storage, data flows, and erasure of data.[183] Sensitive data must be clearly identified within the organization and control of their flows ensured.[184] Data governance involves protecting data, complying with legislation, and "leveraging of data protection and legal compliance in order to establish rights to data," according to one lawyer,[185] echoing other contributions. Its key function is ensuring data availability and data quality.[186] Data governance regimes may help companies comply with different data privacy law regimes.[187] This Article begins its discussion of data governance with an analysis of requirements under the GDPR, before discussing the situation under the Privacy Shield, and then concluding.

A. Data Governance Under the GDPR

Under the GDPR, these data governance regimes must provide for controls along the data flow supply chain.

A first step in GDPR compliance may involve mapping personal data being processed, establishing processing records, and identifying the types of data being processed.[188] The GDPR establishes several rules for data

---

[183] *See* Roland L. Trope & E. Michael Power, *Lessons in Data Governance: A Survey of Legal Developments in Data Management, Privacy and Security*, 61 BUS. LAW. 471, 472 (2005) (calling on corporate Directors and Officers to "focus on the 'data governance' policies and procedures that manage the long-term storage, routine information flows and ultimate disposal" of information assets, and describing such data governance as a comprehensive process to keep pace with security and privacy developments, to "ensure compliance with statutes, regulations, rules and court orders.").

[184] *See* E. Michael Power & Roland L. Trope, *The 2006 Survey of Legal Developments in Data Management, Privacy, and Information Security: The Continuing Evolution of Data Governance*, 62 BUS. LAW. 251 (2006) (the authors, writing in an American publication, use the term "sensitive information" generally, not as it is defined under either the 1995 Directive or the GDPR, where "special categories of data" is the term used, instead. They see the need for identification of such data "to ensure corresponding legal obligations to control and protect such information are respected.").

[185] *The Private-Sector Ecosystem of User Data in the Digital Age*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1099, 1104 (2019) (the lawyer whose 26th Annual IPLJ Symposium Data Governance Regimes panel contributions are reported in this part of the article, is Boris Segalis, Partner and Global Vice Chair, Cyber/Data/Privacy at Cooley LLP).

[186] *See* Barbara Engels, *Data Governance as the Enabler of the Data Economy*, 54 INTERECONOMICS 216, 217 (2019), https://www.researchgate.net/publication/334742032_Data_Governance_as_the_Enabler_of_the_Data_Economy.

[187] *Id*. at 1105 (relating the contributions of Anthony Ford, Senior Data Privacy Counsel at Medidata Solutions, on the same panel: "data governance regimes help to keep companies disciplined and accountable by monitoring where data is stored; what the data is being used for; who has access to the data; how many copies of the data are kept: and what level of security different data require." According to Ford, the result of this "fastidiousness" is that organizations obtain "the ability to comply with the multitude of different legal regimes governing data privacy.").

[188] *See* Voss & Houser, *supra* note 45, at 289.

governance, many of which have their origins in the fair information practice principles ("FIPPs")[189] that were distilled in a report made by a committee of the U.S. Department of Health, Education, and Welfare in 1973.[190] They were later incorporated in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines").[191] The importance of the foundational FIPPs cannot be overstated,[192] as is the case for their the OECD Guidelines variants, which served to influence the development of data protection principles incorporated in the 1995 Directive and later the GDPR.[193] Although the latter instruments add certain data subject rights, such as the right to data portability,[194] the right to erasure (right to be forgotten),[195] and assigns a greater role to accountability. Globally, these data protection principles include the following: data quality, purpose limitation, integrity and confidentiality, transparency, rights of the data subject, accountability, and lawfulness of processing.[196]

The controller has most responsibilities for data protection compliance under the GDPR, although that regulation has imposed certain obligations on the processor as well. Under the concept of accountability, the controller is to "implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with" the GDPR.[197] Approved codes of conduct may be adhered to and used as an

---

[189] *See* Voss, *Obstacles*, *supra* note 17, at 421.

[190] U.S. Dep't of Health, Education & Welfare, No. (OS) 73-94, Records Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, (July 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[191] *OECD Privacy Framework (2013)*, *supra,* note 136.

[192] The role of the FIPPs is recognized in the technology sector, as evidenced by the words of Intel Corporation staff:

> Paula Bruening at Intel succinctly captured the importance of the FIPPs when she described them as a global "common language of privacy." The eight OECD FIPPs have been the foundation of privacy law for more than forty years, and they lay out a model to think about privacy that is much greater than just minimizing the collection and use of data. The FIPPs have proven to be flexible enough to apply to decades of technology innovation and are still adaptable to our current environment.

See David A. Hoffman & Patricia A. Rimo, *It Takes Data to Protect Data*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 546, 555 (Evan Selinger et al., eds., 2018) (citation omitted) (co-author David A. Hoffman is Associate General Counsel and Global Privacy Officer at Intel Corporation).

[193] *See* Voss, *Obstacles*, *supra* note 17, at 415.

[194] GDPR, *supra* note 20, art. 20.

[195] *Id*. art. 17.

[196] *See* Voss, *Obstacles*, *supra* note 17, at 421-422.

[197] GDPR, *supra* note 20, art. 24(1). The "appropriate technical and organizational measures" called for "should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons." *Id*. recital (74). Further guidance is given as to the kind and the

element of evidence of compliance.[198] Where a controller uses a processor to carry on processing on its behalf, it "shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of [the GDPR] and ensure the protection of the rights of the data subject."[199] Furthermore, a contract (or "other legal act") is to govern the processing, specifying, inter alia, that the processor "processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization . . . ."[200] If the processor engages another processor for carrying out specific processing for the controller, it is to enter into a contract containing the same data protection obligations as the controller—processor contract.[201] Either sort of contract may be basis in whole or in part on standard contractual clauses,[202] and must be in writing (including electronic form).[203] In the contract, the processor should also be required to comply with security and confidentiality requirements under data protection law[204] ("integrity and confidentiality" is the term for the data protection principle under the GDPR[205]).

As part of the transparency obligations of the controller, it must inform the data subject, among other obligations: (1) of the recipients or categories of recipients of the personal data being processed;[206] (2) of whether or not it intends to transfer the data to a third country or international organization; and (3) whether an adequacy decision applies to allow such transfer or subject to which appropriate or suitable safeguards they are being transferred and how and where to obtain a copy of such safeguards.[207] Where personal data is

---

severity of the risk concerned in recitals (75) and (76), and as to the implementation of the measures, in recital (77).

[198] *Id*. art. 24(3).

[199] *Id*. art. 28(1).

[200] *Id*. art. 28(3).

[201] *Id*. art. 28(4).

[202] *Id*. art. 28(6) (Commission standard contractual clauses are provided for in art. 28(7); supervisory authority standard contractual clauses in art. 28(8)).

[203] *Id*. art. 28(9).

[204] *See* VOSS & WOODCOCK, *supra* note 59, at 89 (the authors, who discuss this in the context of a controller-processor contract, also recommend that the contract allow for auditing of the processor's security arrangements).

[205] GDPR, *supra* note 20, art. 5(1)(f) ("Personal data shall be: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')").

[206] *Id*. art. 13(1)(e).

[207] *Id*. art. 13(1)(f).

obtained by the controller from a third party, the controller must obtain information in order to allow it to provide the information required to be provided to the data subject.[208] This information includes, as an example, the source from which the personal data come and whether or not they were derived from publicly accessible sources.[209]

Importantly, a controller is responsible for responding to a data subject's request to exercise his or her rights under the GDPR, facilitating such exercise,[210] and providing information regarding action taken in response to the data subject request "without undue delay and in any event within one month of receipt of the request."[211] If the controller does not take the requested action it must inform the data subject of the reasons for this within at the latest one month of the request, and provide information about the possibility of filing a complaint.[212] So long as it is not "manifestly unfounded or excessive," the actions taken following a subject right exercise request should be free of charge.[213]

In addition to the rights already mentioned in Section IV, these data subject rights under the GDPR include: (1) a right of access to the personal data;[214] (2) a right to rectification of inaccurate personal data and completion of incomplete personal data, without undue delay;[215] (3) a right to restriction of processing in certain circumstances (such as where the accuracy of the data is contested or where the processing is unlawful);[216] (4) a right to object to data processing in certain circumstances (such as at any time, where the data are being processed for direct marketing purposes); and, (5) subject to certain exceptions, a "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects his or her."[217]

---

[208] *Id*. art. 14.
[209] *Id*. art. 14(2)(f).
[210] *Id*. art. 12(2).
[211] The GDPR provides that such period may be extended where necessary an additional two months, "taking into account the complexity and the number of requests." In such case, the data subject must be informed of the additional time required and the reasons for the delay. *Id*. art. 12(3).
[212] Such a complaint could be filed with a supervisory authority. *Id*. art. 12(4).
[213] *Id*. art. 12(5).
[214] *Id*. art. 15.
[215] *Id*. art. 16.
[216] *Id*. art. 18.
[217] *Id*. art. 22(1).

An important tool for ensuring interoperability of data—and therefore data governance—is metadata, which allows for discovery and reuse.[218] Security expert Bruce Schneier describes metadata as "data about data—information a computer system uses to operate or data that's a by-product of that operation."[219] In responding to data subject requests, and in ensuring compliance with data subject requests to exercise their rights, such as the "right to be forgotten,"[220] metadata helps.[221] As discussed by the U.K. supervisory authority, in connection with big data where anonymization of data is important in order that it no longer be considered personal data, and thus no longer covered by the GDPR,[222] metadata is a tool to help with data subject requests to exercise their rights under that legislation, such as the right to access their personal data:

> The existence of the right of access compels organizations to practice good data management. They need adequate metadata, the ability to query their data to find all the information they have on an individual, and knowledge of whether the data they are processing has been truly anonymized or whether it can still be linked to an individual.[223]

---

[218] *See* Barbara L. Cohn, *supra* note 181, at 821.

[219] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 17 (2015). Mayer-Schönberger and Ramge describe the use of metadata to "have an efficient way to label and categorize information," through the use of categories that are "data about data." *See* VIKTOR MAYER-SCHÖNBERGER & THOMAS RAMGE, REINVENTING CAPITALISM IN THE AGE OF BIG DATA 66 (2018).

[220] GDPR, *supra* note 20, art. 17(1) ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies . . . .").

[221] *See* Eugenia Politou et al., *Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions*, 4(1) J. CYBERSECURITY 1, 15 (2018) (". . . metadata-based architecture is considered as a useful building block for enabling and supporting the RtbF . . . , metadata alone cannot guarantee that entities will abide by specified policies. Nevertheless, it can facilitate their enforcement by making them readily accessible . . . ." RtbF is an abbreviation for "Right to be Forgotten."), https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056.

[222] GDPR, *supra* note 20, recital (26) ("The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.").

[223] INFO. COMM'R'S OFF. (ICO), BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION 46 (2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

While metadata is one way to help ensure good data governance, technologies used by businesses today, such as cloud computing, create certain difficulties for compliance. Where cloud providers move data around "in response to load and other factors," the location of data at any specific time may not be known.[224] This may involve concerns with the cross-border transfer restriction if the location is in a country that has not received an adequacy decision.[225]

The French data protection authority—the CNIL—offered recommendations in connection with cloud computing prior to the adoption of the GDPR (although these points are still valid today): "Clearly identify the data and processing operations that will be passed to Cloud;" "Define your own requirements for technical and legal security;" "Carry out a risk analysis to identify the security measures essential for the company;" "Identify the relevant type of Cloud for the planned processing;" and "Choose a service provider offering sufficient guarantees."[226]

Furthermore, the Article 29 Data Protection Working Party, an influential advisory group created under Article 29 of the 1995 Directive[227] (which was replaced by the EDPB under the GDPR[228]), opined that cloud service agreements should indicate where the data is to be processed and by whom, in addition to ensuring "effective control over and allocate clear responsibility for processing activities."[229] Careful thought must be made

---

[224] *See* CHRISTOPHER S. YOO & JEAN-FRANÇOIS BLANCHETTE, REGULATING THE CLOUD: POLICY FOR COMPUTING INFRASTRUCTURE 186 (2015).

[225] *Id*. at 155.

[226] *Cloud computing: CNIL's recommendations for companies using these new services*, CNIL (June 25, 2012), https://www.cnil.fr/en/cloud-computing-cnils-recommendations-companies-using-these-new-services. The recommendations may be downloaded directly. *See Recommendations for Companies Planning to Use Cloud Computing Services*, CNIL, https://www.cnil.fr/sites/default/files/typo/documentRecommendations_for_companies_planning_to_use_Cloud_computing_services.pdf (last visited on Mar. 20, 2020). Similarly, the United Kingdom's data protection authority—the ICO—published guidance for cloud computing prior to the adoption of the GDPR. *See Guidance on the Use of Cloud Computing*, ICO, https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations. pdf.

[227] 1995 Directive, *supra* note 91, art. 29(1). For a discussion on the role of this group, *see* FARRELL & NEWMAN, *supra* note 5, at 51 ("Informally, the Article 29 Working Party has become a powerful counterweight to firms and governments that skirt or bend European rules, and its opinions carry considerable weight with informed elite opinion").

[228] Eur. Comm'n, Justice & Consumers, The Article 29 Working Party Ceased to Exist as of 25 May 2018 (June 11, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492.

[229] *See* art. 29 Data Protect. Working Pty., Opinion 05/2012 on the Cloud Computing (July 1, 2012), WP 196, at 9, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendations/files/2012/wp196_en.pdf.

about personal data management when negotiating and drafting the provisions of a cloud service contract.[230]

The GDPR provides tools for ensuring accountability and compliance, which have been detailed elsewhere: requirements for data processing registers (with the exception of certain small and medium sized enterprises),[231] requirements for many companies to have data protection officers,[232] and requirements for high risk processing to be preceded by data protection impact assessments[233] figure among these. Furthermore, increased sanctions for data protection violation, going up to 4% of annual worldwide turnover for companies for the most serious violations, provide motivation for compliance.[234]

B. Data Governance Under the Privacy Shield

Data governance provisions about onward transfers (as well as the accountability provisions of the GDPR), may be understood as elements that make data recipients responsible for the actions of actors down the personal data global supply chain. Data controllers are subject to the requirement generally through the GDPR's accountability provisions discussed in Section A. This is reminiscent of the way that in other sectors, such as corporate social responsibility, companies dealing internationally may have to engage in due diligence for supply chain management both upstream and downstream.[235] In particular, in the area of onward transfers, the Privacy Shield sets out accountability provisions, whether such onward transfers be to "a third party

---

[230] For a discussion of the content of a cloud service contract, *see* VOSS & WOODCOCK *supra* note 59, at 190.

[231] *See European Union Data Privacy Law Reform*, *supra* note , at 227.

[232] *See* W. Gregory Voss, *Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation*, 50 REVUE JURIDIQUE THÉMIS DE L'UNIVERSITÉ DE MONTRÉAL 783, 806-14 (2016), https://ssl.editionsthemis.com/uploaded/revue/article/2269_09-RJTUM-50-3_Voss.pdf.

[233] *Id*. at 803-806.

[234] *See* Houser & Voss*, supra* note 44, at 57.

[235] "Corporate social responsibility (CSR) is increasingly concerned therefore with supply chain management and in particular with global supply chain management." Andrew Millington, *Responsibility in the Supply Chain*, *in* THE OXFORD HANDBOOK OF CORPORATE SOCIAL RESPONSIBILITY 363 (Andrew Crane et al., eds., 2008). As one example from Europe, France adopted a law that requires due diligence with respect to not only a company's activities and those of its subsidiaries, but also those of suppliers and subcontractors in the areas of human rights, health and safety, and environmental risks. *See* Constance Z. Wagner, *Evolving Norms of Corporate Social Responsibility: Lessons Learned from the European Union Directive on Non-Financial Reporting*, 19 TENN. J. BUS. L. 619, 669 (2018).

acting as a controller" or "a third party acting as an agent."[236] In the case of a third party acting as a controller, these include requirements of providing information to the data subjects (individuals) (which are couched as "notice," and would typically be considered part of "transparency") and choice,[237] where the data subject is given a right to opt-out of processing and, in the case of the processing of special categories of data (sensitive data), where an opt-in requirement is imposed.[238] Furthermore, in the case of a transfer to a controller, there must be a contract entered into with such controller setting out elements of purpose limitation and requiring that the recipient controller provide "the same level of protection as the Principles" and notify the organization "if it makes a determination that it can no longer meet this obligation," in which case such controller will either cease processing the data or take "other reasonable and appropriate steps to remediate."[239]

In the case of an onward transfer under the Privacy Shield to an agent (processor), several conditions must be met by the organization:

> (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy

---

[236] *3. Accountability for Onward Transfer*, PRIVACY SHIELD FRAMEWORK (last visited on Mar. 5, 2020), https://www.privacyshield.gov/article?id=3-Accountability-For-Onward-Transfer.

[237] *Id*. ("To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles."). The Notice Principle includes requirements as to the information that must be furnished to the data subject (individual), listing thirteen categories of information. *See 1. Notice*, PRIVACY SHIELD FRAMEWORK (last visited on Mar. 5, 2020), https://www.privacyshield.gov/article?id=1-NOTICE.

[238] *See 2. Choice*, PRIVACY SHIELD FRAMEWORK (last visited on Mar. 5, 2020), https://www.privacyshield.gov/article?id=2-CHOICE.

[239] *3. Accountability for Onward Transfer*, *supra* note 236. *See also 10. Obligatory Contracts for Onward Transfers*, PRIVACY SHIELD FRAMEWORK (last visited on Mar. 5, 2020), https://www.privacyshield.gov/article?id=10-Obligatory-Contracts-for-Onward-Transfers.

> of the relevant privacy provisions of its contract with that agent to the Department upon request.[240]

Thus, in the case of onward transfers by an organization that has received personal data under the Privacy Shield Framework, there are ongoing responsibilities (or accountability)[241] for the U.S. organization self-certifying under the Privacy Shield. These responsibilities equate to requirements to control the personal data supply chain downriver in what may be described as personal data global supply chain management.

Finally, as we have seen, the incorporation of data governance provisions similar to those under the 1995 Directive and the GDPR, has provided the substance of international agreements entered into in order to allow personal data to cross borders, such as the Safe Harbor and the Privacy Shield. Indeed, adopting the GDPR standard for data governance may be a strategic choice.[242] However, the monitoring of legal developments regarding legislative instruments with extraterritorial effect from other jurisdictions should be done, as such instruments might impact data governance requirements, although this Article has focused on the European Union's GDPR.

C. Conclusion Regarding Data Governance

Companies that adopt good data governance practices may find that this facilitates compliance with various data privacy laws that apply to their global data flow supply chain. Mapping data processing and understanding, to the extent possible, where their data are, is the first step for companies. Companies should follow what have become arguably universal principles—the FIPPs—in their effort to comply with laws around the world. As the GDPR will apply to many international companies, they should heed its accountability provisions and assess their global data flow supply chain for

---

[240] *Id*.

[241] In the case of an onward transfer to a controller, this accountability will be ensured through enforcement of the provisions of the mandatory contract discussed above. In the case of an onward transfer to a processor (agent), "the U.S. organisation will bear the responsibility to guarantee the protections provided under the Principles by exercising its powers of instruction." *See* Commission Implementing Decision of 12 July 2016, *supra* note 164, at 6 n.31.

[242] *See* Voss & Houser, *supra* note 45 at 338 ("U.S. tech companies can leverage their compliance with the GDPR to change and improve their corporate culture, resulting in greater trust among consumers. By going above and beyond legal requirements, . . . and advertising such measures to the public, they can gain a distinct trust-based competitive advantage over firms who minimally comply with the law.").

GDPR compliance. In this context, contracts are important for ensuring compliance downstream. Security and transparency are important issues here that should be addressed in contracts.

Furthermore, controllers should properly vet their processors and may audit them during processing. Provisions for the exercise of rights by data subjects must be evaluated and the use of metadata that may be easily indexed provides help in locating relevant data. Companies should exercise special care in negotiating and drafting cloud contracts. The increased sanctions in the GDPR, when compared to the 1995 Directive, provide incentive for compliance.

Under the Privacy Shield there are various requirements regarding contracts for onward transfers. These should be perceived as part of global data flow supply chain management—a concept that harkens to other fields, such as CSR, where more and more companies are becoming responsible for their international supply chains. However, the result of efforts such as these will be to help the company better to govern its personal data flows, avoid liability, and increase trust among its customers, suppliers and partners.

V. CONCLUSION

Cross-border data flows are today an important component of international trade, and the backbone of many digital service models. However, for various reasons, in the context of "rival standards" and "rule overlap" of extra-territorial laws, restrictions on the transfer of personal data and data localizations requirements have sprung up. While these complexities have served to impede certain data flows, international agreements have been resorted to, in order to allow for continued free flows of personal data, subject to providing certain protections of data subjects and their data. These agreements have included the Privacy Shield, in the case of self-certified organizations located in the United States, an adequacy decision and Supplemental Rules, in the case of Japan, BCRs and standard contractual clauses in other cases—although some of these are subject to challenge in the courts.

Parallel to the development of the concept of international supply chain management in other fields, such as for the production of products in corporate social responsibility, the GDPR, and the use of cross-border transfer mechanisms under it, demand certain actions for managing the international personal data supply chain. In the Privacy Shield we have seen that there are

requirements of accountability of U.S. Privacy Shield-certified organizations for onward data transfers. Accountability starts with knowing what data is being collected and processed and where it is. As has been shown, this is important because of the broad reach of data protection law, both in terms of subject matter and its extraterritorial reach.

When recourse is made to processors (or subsequent controllers) down the data flow supply chain, contracts must be used to control activities, to ensure data protection is ensured and to frame any future possible onward transfers. This is true whether the contracts be used in a cloud service relationship, other forms of processing, or onward transfers under the Privacy Shield.

Overlapping legislation in the area makes these activities more difficult, and it is imperative that companies constantly monitor legislative and judicial developments in this area. While this Article has focused solely on the GDPR and its predecessor, the 1995 Directive, it is important companies determine and analyze all applicable legislation, especially when compliance with the CCPA is similar, but not the same, as compliance with the GDPR. Companies must understand these complexities and follow regulatory developments wherever their global data flow supply chain goes—most likely, worldwide—in order to ensure compliance. Although there may be conflicts among the various applicable data privacy legislation, good data governance should serve compliance efforts under all such legislation, giving increased justification for its practice. Companies should apply good data governance throughout their global data flow supply chain.

Annex—OECD Guidelines (1980 & 2013 Modernization)—Basic Principles of International Applications: Free Flow and Legitimate Restrictions

Provision	**Original 1980 Guidelines Part III.** **Basic Principles of International Application: Free Flow and Legitimate Restrictions**[243]	**2013 Modernization Text Part IV.** **Basic Principles of International Application: Free Flow and Legitimate Restrictions**[244]
Consideration of Implications for Other Member Countries of Domestic Processing and Re-export of Personal Data	15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.	
Ensuring that Transborder Personal Data Flows Are Uninterrupted and Secure	16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.	
Data Controller Accountability Regardless of Data Location		16. A data controller remains accountable for personal data under its control without regard to the location of the data.

[243] *OECD Guidelines (1980)*, *supra* note 135.
[244] *OECD Privacy Framework (2013)*, *supra* note 136, at 16.

Provision	**Original 1980 Guidelines Part III.** **Basic Principles of International Application: Free Flow and Legitimate Restrictions**[243]	**2013 Modernization Text Part IV.** **Basic Principles of International Application: Free Flow and Legitimate Restrictions**[244]
Refraining from Restrictions When Other Member Country Substantially Observes Guidelines	17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.	17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
Proportionality	18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.	18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.