IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Commentary_and_Principles_on_Jurisdictional_Conflicts_over_Transfers_of_Personal_Data_Across_Borders

The Sedona Conference Working Group Series

The Sedona Conference

Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders

A Project of The Sedona Conference Working Group
on International Electronic Information Management,
Discovery, and Disclosure (WG6)

June 2019
Public Comment Version
Submit comments by **August 10, 2019**,
to comments@sedonaconference.org.

The Sedona Conference Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

June 2019 Public Comment Version

Author: The Sedona Conference

Drafting Team Leaders

Wayne Matus David C. Shonka

Drafting Team

Michael Bahar
Susan Bennett
Oliver Brupbacher
Conor R. Crowley
Emily Fedeles
Jerami Kemnitz
Brian Ray
Alexander White

Steering Committee Liaison

Taylor Hoffman

Staff Editors

David Lumia Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

REPRINT REQUESTS:

Requests for reprints or reprint information should be directed to The Sedona Conference at info@sedonaconference.org.

Copyright 2019
The Sedona Conference
All Rights Reserved.
Visit www.thesedonaconference

Preface

Welcome to the public comment version of The Sedona Conference *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders ("Commentary")*, a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The Sedona Conference acknowledges and thanks Drafting Team Leaders David Shonka and Wayne Matus for their leadership and commitment to the project. We thank drafting team member Jerami Kemnitz for his significant efforts. We also thank drafting team members Michael Bahar, Susan Bennett, Oliver Brupbacher, Conor Crowley, Emily Fedeles, Brian Ray, and Alexander White for their efforts and commitments in time and attention to this project. We thank Ava Dixon and Juanda Moore for their assistance. Finally, we thank Taylor Hoffman for his guidance and input as the WG6 Steering Committee Liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by August 10, 2019, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
June 2019

Table of Contents

Choice-of-law Principles

Principle 1: A nation has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, natural persons and organizations in or doing business in its territory, regardless of whether the processing of the relevant personal data takes place within its territory.

Principle 2: A nation usually has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, the processing of personal data inextricably linked to its territory.

Principle 3: In commercial transactions in which the contracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction.

Principle 4: Outside of commercial transactions, where the natural person freely makes a choice, that person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data.

Principle 5: Data in transit ("Data in Transit") from one sovereign nation to another should be subject to the jurisdiction and the laws of the sovereign nation from which the data originated, such that, absent extraordinary circumstances, the data should be treated as if it were still located in its place of origin.

Principle 6: Where personal data located within, or otherwise subject to, the jurisdiction or the laws of a sovereign nation is material to a litigation, investigation, or other legal proceeding within another sovereign nation, such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data.

I. INTRODUCTION

Businesses today navigate, with difficulty, a bewildering maze of conflicting and confusing data protection and privacy laws. When the free flow of physical goods in global commerce faced analogous constraints in navigating the seas, nations met and resolved the most crucial issues by agreement.[1] We submit that a similar agreement is needed today to ensure the continued flow of necessary information in global commerce. Indeed, the European Union (EU) has intimated as much in Article 48 of the General Data Protection Regulation (GDPR).[2] Although it would be presumptuous to suppose that this *Commentary* might resolve these issues, the Sedona Conference hopes that it will contribute in some small way to the incipient dialogue that is beginning to take place and that sooner, rather than later, there will be an international forum to address, and ultimately resolve, the conflicts between international data protection regimens to the extent they adversely impact global commerce.

The goal of this *Commentary* is to provide: (1) a practical guide to corporations and others who must make day-to-day operational decisions regarding the transfer of data across borders; and (2) to provide a framework for the analysis of questions regarding the laws applicable to cross-border transfers of personal data.

A. The Underlying Tension

Data lies at the crossroads of the inherent tension between the free flow of information on the one hand and security and privacy on the other. Those who support free flow note that the use of that data is now critical to successful enterprise, and that tremendous wealth and power comes to those who can gather and make the best use of it. Yet McKinsey Global Institute reported in 2017 that, "Flows of physical goods and finance were the hallmarks of the 20th-century global economy, but today those flows have flattened or declined. Twenty-first-century globalization is increasingly defined by flows of data and information."[3] And that is because others value security and privacy highly and believe that free flow needs to be limited based upon principles such as consent, data minimization, and security by design. For example, whereas the U.S. generally distinguishes between public and private data, and affords the latter protections in specific areas, Europe protects the underlying

---

1 Today such issues are governed by international conventions such as the United Nations Convention on the Law of the Sea (UNCLOS III) and the Hague Rules (International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading) (CIGS).

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

3 By 2015 cross-border data flows were 45 times larger than a decade earlier and were forecast to grow another nine times by 2020. *See* MCKINSEY GLOBAL INSTITUTE, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS (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.

right of a natural person to determine the disclosure and use of his or her personal data and affords such right general constitutional protection.

B. Comity[4]

What is therefore needed, and what this *Commentary* hopes to achieve, is to distill and update key choice-of-law principles with respect to personal data. In our view, comity is the bulwark against chaos, and how comity should be applied is one of the goals of this guide. When comity cannot be the answer, the *Commentary* proposes steps on how conflicts should be resolved. This paper outlines the complex data and legal backdrops that cause conflict and proposes a set of principles to help achieve resolution.

One of the classic statements on "comity" comes from the U.S. Supreme Court, which in *Hilton v. Guyot*, held:

> "Comity," in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws.[5]

The European Union acknowledges the concept of comity without further describing it. For example, the foundational treaties and case law reference the "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law.[6]

---

[4] *See* Hilton v. Guyot, 159 U.S. 113 (1895). For example, in JP Morgan Chase Bank v. Altos Hornos de Mexico, S.A. de CV., 412 F.3d 418, 424 (2d Cir. 2005), the Second Circuit determined that U.S. courts should ordinarily decline to adjudicate creditor claims that are the subject of a foreign bankruptcy proceeding, and deference should be given to the foreign court, so long as the foreign proceedings are procedurally fair and do not contravene the laws or public policy of the U.S. It is a recognized principle of jurisprudence in the United States. William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071 (2015).

[5] *Hilton*, 159 U.S. at 163–64. Other Supreme Court decisions have discussed comity in terms of interpretive canons of restraint. For example, in *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100, 2107 (2016), the Court stated that the extraterritoriality canon when interpreting domestic law "avoid[s] the international discord that can result when U.S. law is applied to conduct in foreign countries," and "the need to enforce the presumption is at its apex" when there is a "risk of conflict between [an] American statute and . . . foreign law" (quotation marks omitted). In addition, under the famous "Charming Betsy" canon, U.S. courts seek to avoid interpreting domestic law in a way that violates the law of nations "if any possible construction remains," and to interpret the domestic law in light of "principles of prescriptive comity" that prohibit "unreasonable interference with the sovereign authority of other nations" (internal quotation marks omitted). F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 164 (2004).

[6] *See* The Treaty on European Union arts. 3(5), 21(1), 2008 O.J. C 115/17, 115/28, *available at* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:EN:PDF; Case 52/69, Geigy v. Commission,

The United States, with its passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act explicitly authorizing American law enforcement officials to compel U.S. providers to produce data, even if it is stored outside the U.S., set up an exception and mechanism to enhance comity.[7] It left undefined, however, what the principles guiding a comity analysis should be.

C. Legal and Practical Complexity

The challenges just identified cut across multiple legal[8] and practical contexts.[9] Existing frameworks for bilateral and multilateral cooperation are insufficient and under increasing stress not only from the rapid expansion of data and difficulty in determining its precise location, but also from significant confusion over the appropriate criteria for showing jurisdictional nexus. The diverse—and often competing—range of legal issues data implicates, ranging from criminal investigations and civil discovery to human rights and national security, further complicates the picture. Taken together, the factual, political, and legal complexities surrounding data pose new and distinctive challenges for establishing norms and principles to guide transnational cooperation.

At the core of the problem is the lack of robust coordination mechanisms for resolving competing and often conflicting legal requirements from multiple jurisdictions. This primarily procedural issue is magnified by a set of contentious debates over substantive legal issues, including the striking difference in privacy protections between nations. Further compounding these issues are a set of political and economic incentives that have resulted in a marked increase in new regulatory measures designed to increase local control over data through various means, in particular data localization laws.[10]

¶ 11, ECLI:EU:C:1972:73; Case C-366/10, Air Transport Ass'n of America v. Sec'y of State for Energy and Climate Change, ¶ 123, ECLI:EU:C:2011:864.

7 Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong. (2d Sess. 2018). The U.S. legislature, in the CLOUD Act, mandates a judicial comity analysis in certain circumstances, but similarly does not further define it. In its savings clause, the CLOUD Act provides that it shall not "be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis . . . to instances of compulsory process issued under [the Stored Communications Act [SCA]] and not covered under [Section 2703](h)(2)]." *See* CLOUD Act § 103(c). In other words, for all cases not covered by new Section 2703(h), the CLOUD Act does not change the "common law" comity standards, which currently apply to the SCA process, but it does not define those standards.

8 For a full discussion of the legal complexity and background, please review Appendix: Data Privacy Complexity and Background, *infra*.

9 Data frequently resides across multiple services, providers, and locations, often spanning several jurisdictions. The Cloud Standards Consumer Council has published a report that nicely captures many of the risks that result from confusion over the precise location and movement of data, including: penalties that result from violating conflicting government laws or regulations; increased costs of doing business in countries that require data localization; hiring local staff; and heightened cybersecurity risk due to the multiplication of localized data centers. *See* CLOUD STANDARDS CONSUMER COUNCIL, DATA RESIDENCY CHALLENGES: A JOINT PAPER WITH THE OBJECT MANAGEMENT GROUP, 8 (2017), https://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf.

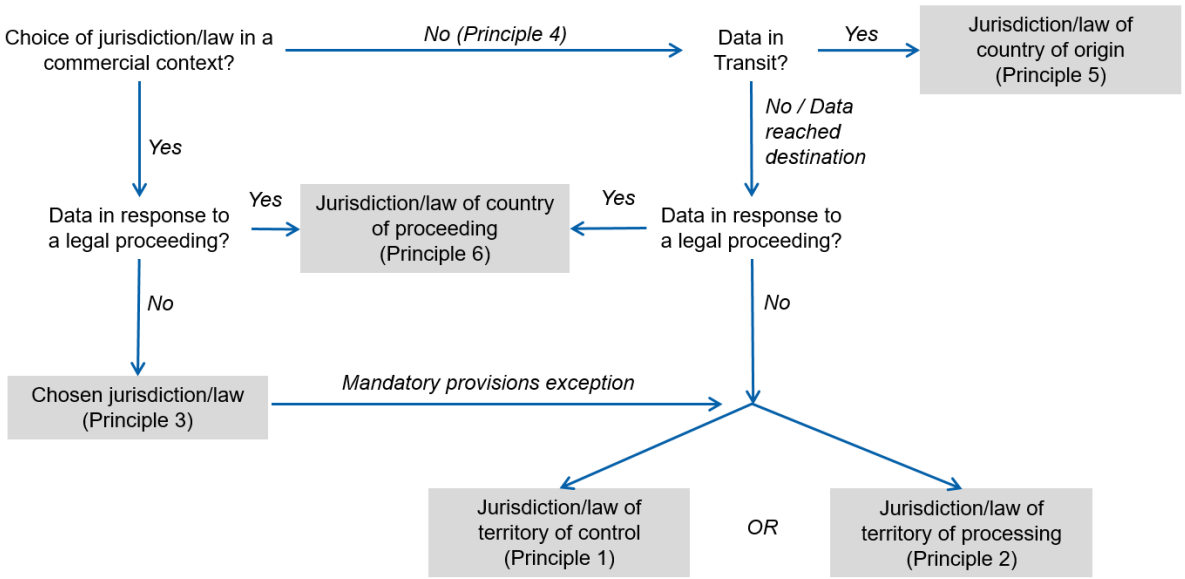
10 A detailed survey of the origins and status of legal complexity is provided in Appendix, *infra*.

II. CHOICE-OF-LAW PRINCIPLES

At present, there is no universal framework for cross-border data transfers in a globalized context. There are, however, certain generally recognized International Law Principles that apply to all nations, which can serve as a starting point for mitigating the conflict-of-laws issue with respect to personal data.

For example, as with other physical property, states have sovereign rights over any cyber infrastructure, such as servers and computers, located in their territory. According to the Tallinn Manual, which is concerned with cyber law in military operations . . . "[a]lthough territoriality lies at the heart of the principle of sovereignty, in certain circumstances, States may also exercise sovereign prerogatives such as jurisdiction over cyber infrastructure and activities abroad, as well as over certain persons engaged in those activities."[11]

Basic principles of International Law relating to sovereignty, due diligence, jurisdiction, and the rights enjoyed by natural persons can help support a set of principles that can serve as a framework for analyzing cross-border transfers of personal and confidential data in a global economy. The six Principles put forth in this *Commentary* serve to guide readers in determining which nation's laws should apply in a given context. The following diagram illustrates a process for applying the six Principles.



[11] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 11 (2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

Principle 1: A nation has nonexclusive jurisdiction over, and may apply its data protection and privacy laws to, natural persons and organizations in or doing business in its territory, regardless of whether the processing of the relevant personal data takes place within its territory.

Comment a: Principle 1 focuses on the location of data subjects and organizations, as opposed to the location of data processing, which is the subject of Principle 2.[12]

Comment b: The starting point is to ask where the organizations or natural persons who control personal data, whether their own or others, are established. That location determines the jurisdiction and the applicable law for any processing of personal data. Conversely, if there is no sufficient connection between a nation and such data subject or organization, the data is not subject to that nation's jurisdiction and laws. That leaves open the question of which jurisdiction and laws govern such data processing activities. The answer to that question is addressed by Principle 2. Consequently, this *Commentary* accepts the possibility that different jurisdictions and laws could apply to data subjects or organizations that are in one jurisdiction on the one hand, and to parties that process such data but have no other contact with that jurisdiction, on the other.

Comment c: Under existing law, nations have a sovereign right to "territorial" and "political" independence, and there shall be no interference "in matters which are essentially within the domestic jurisdiction of any state."[13] Accordingly, the only restrictions on the rights of nations are either by consent of the nation or by agreed international norms of conduct. Nor is there room for an argument that cyber activities belong to a lawless "global domain" and that it "lacks physicality and is virtual in nature." After all, "[c]yber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise sovereign prerogatives . . . although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more States."[14]

---

[12] This basic approach is in line with the European Data Protection Board (EDPB) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)—Version for public consultation (adopted on 16 November 2018), *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.

[13] U.N. Charter art. 2.

[14] TALLINN MANUAL 2.0, *supra* note 11, at 11.

Comment d: Among those matters that are essentially within the rights of a nation is the power to confer or withhold citizenship, residence, or any other type of legal status that conveys upon such data subjects and organizations certain varying rights and obligations.[15] Generally, all citizens, residents, and persons with another legal status within a nation are obligated to comply with laws that compel them to appear before an authority, to produce information, or to suffer penalties for failing to do so. Correspondingly, citizens, residents, or persons with another legal status have an expectation that their nation(s) will protect the rights that it (or they) afford them.[16] Likewise, organizations that engage in purposeful activity (e.g., processing) in the jurisdiction of the sovereign should generally be obligated to comply with a nation's laws and regulations when processing personal information.

Comment e: In the context of such natural persons or organizations within its territory, a nation generally has the right to exercise jurisdiction over and apply its laws to the control over or the targeting of personal information.[17] By exercising jurisdiction and applying its laws, a nation is protecting both its data subjects' rights and the integrity of the personal data itself, irrespective of whether the data belongs to its data subjects or other nations' data subjects.[18]

Comment f: Insofar as it refers to personal data belonging to an organization or a natural person, Principle 1 addresses the organization and natural person as data controller in the sense of the GDPR, i.e., as a "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."[19]

Case Study 1: A multinational headquartered in Europe becomes subject to a litigation in New York that seeks the disclosure of personal data in the possession, custody, or control of both U.S. and German affiliates as well as U.S. and German employees of that multinational. Here, both the United States and Germany may assert personal jurisdiction

---

15 *See* GERARD-RENÉ DE GROOT, ELGAR ENCYCLOPEDIA OF COMPARATIVE LAW, NATIONALITY LAW, 476–92 (2006).

16 *Cf.* Charter of Fundamental Rights of the European Union art. 8(1), 2010 O.J. C 83/393 (emphasis added): "*Everyone* has the right to the protection of personal data concerning him or her."

17 TALLINN MANUAL 2.0*, supra* note 11*,* at 16.

18 *Cf.* GDPR, *supra* note 2, Recital 14.

19 GDPR, *supra* note 2, art. 4(7).

over and apply their laws to the personal data that reference natural persons who are named parties in the proceedings and who are located in their territory. To the extent other natural persons work for the named parties in the proceedings, those parties are to be considered as co-controllers for the purpose of the proceedings. Depending on where the parties are established, U.S. or German jurisdiction and laws may apply to the respective personal data. However, as shown below, Principle 6 would accommodate discovery in the U.S. court proceeding of a foreign data subject's personal data, at least to the extent that appropriate measures are taken to protect the data and limit its use and dissemination to the extent feasible.

Case Study 2: A U.S. company remotely tracks the purchasing habits of French customers in order to provide them with targeted advertising materials. The analysis of the purchasing habits amounts to monitoring of the behavior of natural persons in France. In that context, France alone has an interest in the personal information of natural persons on its territory and might rightly assert jurisdiction over and apply its laws to the processing of the personal data by the U.S. company.

Comment g: Both the data control and the monitoring or collection of personal data must have a sufficient nexus with the territory of the nation asserting jurisdiction and applying its laws. For data monitoring and collection, that criterion is straightforward and merely requires the presence of the data subject in the respective jurisdiction. As GDPR Article 3(2) asserts,[20] a nation may assert jurisdiction over an entity that monitors the behavior of natural persons within its borders or that directs a marketing campaign to natural persons into a country, and thereby collects the personal data of those who respond to the campaign. Although the organization in question may not be physically established within the nation, its activities nonetheless reach into the nation and directly affect natural persons within it. For data control, things are more complex. GDPR Article 3(1) speaks of the "establishment" of a controller in the jurisdiction, defined as the effective and real exercise of activities through stable arrangements, irrespective of the legal form of such arrangements.[21] That nexus or establishment should be more than minimal.[22] Indeed, some

---

[20] GDPR, *supra* note 2.

[21] *Id.*, Recital 22; Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság, ECLI :EU:C:2015:639, ¶ 28.

[22] *Cf.* Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, ECLI:EU:C:2016:612**,** ¶¶ 76–77.

commercial activity led by a foreign data controller entity in another country may be so far removed from the ordinary course of business data processing by this entity that the existence of such commercial activity should not be sufficient to subject that data processing to the jurisdiction and laws of that other country.[23] Consider a variant of the Case Study 1 above: If Human Resource (HR) data of employees of a U.S. affiliate that is a party in the proceedings is stored on a group server in France and can be downloaded by the U.S. affiliate in the ordinary course of business, the mere location of Information Technology (IT) infrastructure should not provide a sufficient nexus to France for it to apply its jurisdiction and laws to such HR data when it is produced in the New York litigation.

Comment h: Likewise, a foreign data controller should not become subject to a country's jurisdiction and laws simply because it chooses to use a processor in that country. The processing is carried out in the context of the controller's own activities, and the processor is merely providing a processing service. Therefore, while the processor may be subject to that country's jurisdiction and laws regarding its own data processor obligations, as governed by Principle 2, this should not cause the foreign controller, or the data itself, to become subject to the data controller obligations of that country.[24] To take the variant of the Case Study 1 a step further: Consider that the HR data of employees of a U.S. affiliate that is a party in the proceedings is stored on a cloud server operated by an external data processor in Ireland. While the operations of that processor may be subject to Irish jurisdiction and laws, the U.S. HR data itself should not.

Comment i: The jurisdiction over personal data afforded by Principle 1 is not necessarily exclusive. In circumstances where a natural person has dual or multiple citizenship, residence, or other legal status, each nation may claim jurisdiction over and apply its laws to a spectrum of issues ranging from privacy to security to the personal data of that natural person. Similarly, as illustrated in the comments to Principle 3 below, multiple jurisdictions may be able properly assert jurisdiction when

---

[23] EDPB Guidelines 3/2018, *supra* note 12, at 10.

[24] For the EU now supported by EDPB Guidelines 3/2018, *id.*, at 10-11, where the EDPB also refuses to qualify the offering of a processing service as targeting of data subjects in that country. *But see* Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, ECLI:EU:C:2014:317; and Art. 29 Data Protection Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU (Court of Justice of the European Union) judgment in Google Spain, Dec. 16, 2015, *available at* https://iapp.org/media/pdf/resource_center/wp179_CJEU-Google-Spain_12-2015.pdf.

such data crosses international borders. For example, if a person in State A contracts with a person in State B to engage in activities that have a substantial effect in State C, all three States may have jurisdiction over the personal data of the person in State A.[25]

Comment j: Because of global economic and communications interconnectedness and the mobility of citizens among countries, dual or multiple citizenships and cross-border data transfers are common. While globalization and international legal harmonization have resulted in an increased compatibility with the regulatory frameworks adopted by various nations, there remain significant differences, some of which are exacerbated by competition over data and geopolitical instability. Because of such differences, dual or multiple citizens are subject not only to multiple laws affecting or protecting their privacy, but to some laws that may be conflicting.

Comment k: Courts may resolve such conflicts between the laws of two or more nations by defining data control not in the abstract, but in a specific context. As demonstrated by Case Study 1, the context helps identify the purposes and means of the processing of personal data and, ultimately, who determines such purposes and means. Another factor courts should consider is the affirmative actions of the natural persons and organizations in question. The choice of a natural person or organization to establish itself predominantly in a particular jurisdiction and avail itself of the rights and benefits of such a jurisdiction, or a decisive and informed step to hand over its data to another jurisdiction, should count toward the primacy of a certain jurisdiction and its laws.

Case Study 3: A person received two citizenships at birth, one from its parents and one from its country of birth. As an adult, the choice to reside in one of the two countries could reflect an understanding of that country's laws and mores, a sympathy for the jurisdiction's manner of justice, and an implicit choice of preference for that country over the other country of citizenship. Further, if the country of the residence is neither of the countries of citizenship, questions of jurisdiction may need to be resolved by balancing all the factors favoring the applications of the jurisdiction and laws of the country of residence against the factors that favor the application of the jurisdiction and laws of the nation(s) of citizenship. Location of residency need not be the sole factor: other affirmative decisions or statements by a natural person may tilt the balance when considering choice of jurisdiction.

---

[25] See TALLINN MANUAL 2.0, *supra* note 11, at 56.

Principle 1 does not apply to packetized data that is in transit across borders under Principle 5. Principle 1 is also limited by Principle 6 with respect to data that is responsive in foreign legal proceedings.

Principle 2: A nation usually has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, the processing of personal data inextricably linked to its territory.

Comment a: Principle 2 focuses on the location of data processing, as opposed to the location of data subjects and organizations, which is the subject of Principle 1. Principle 1 rests upon the proposition that a state may exercise its jurisdiction over and apply its laws to those who control personal data, or whose personal data is targeted, provided they are established in its territory. Where this is not the case, Principle 2 determines under which conditions the processing activities of a data processor fall within the application of a state's jurisdiction and laws.

Comment b: Principle 2 accepts the GDPR's definition of data processing 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."[26]

Comment c: As with Principle 1, the data processing must have a sufficient nexus with the territory of the nation for it to assert its jurisdiction and apply its laws. This Principle may not apply when the level of processing is merely ministerial or incidental to activities of a foreign data controller that predominantly take place outside the country. As the Court of Justice of the European Union has recognized, if the activities of an entity in a country are "inextricably linked" to the processing of data carried out by a foreign data controller, that country's laws may apply to the data processing by the foreign controller.[27] Where, for example, the contact with a country is limited to the mere collection of data, without any further processing in the territory, that country should ordinarily defer to the jurisdiction with the greater interest in the data

---

[26] GDPR, *supra* note 2, art. 4(2).

[27] Case C-131-12, *Google Spain SL*, ¶ 56. *Cf.* also Advocate General's Opinion in Case C-501/17, Google v Commission Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:15, of Jan. 10, 2019, rejecting a request that search requests outside the EU should be affected by a French request to de-reference search results, thereby limiting the potential extraterritorial effect of European data privacy law in a global context such as the internet.

subject, which would usually be where the data controller principally resides (as illustrated in Comment i to Principle 1 above). For the same reasons, packetized data that is in transit across borders should not be subjected to Principle 2, but should be governed by Principle 5.

Comment d: As with Principle 1, the jurisdiction afforded by Principle 2 over personal data is not necessarily exclusive. The practical application of Principle 2 is to acknowledge the sovereign right of a state to regulate activities within its borders, while at the same time preserving the rights of a nation to exercise jurisdiction over and apply its laws to its citizens, residents, or data subjects otherwise closely connected to it. Courts may resolve potential conflicts between the laws of two or more nations by defining data processing not in the abstract but in a specific context, by asking which purpose the processing serves.

Case Study 4: Suppose, for example, that a German data subject completes an online survey in which a U.S. company in Nebraska collects the subject's personal data in order build a profile of consumers in the data subject's home country. This case falls squarely into the category of data targeting governed by Principle 1, which affords jurisdiction and applicable law to Germany. Here, Principle 2 recognizes that Germany's interest in the collected data is greater than that of Nebraska. One arrives at the same answer by identifying the main purpose of the data processing, which in this instance is the profiling in the data subject's home country and not the ministerial data analytics performed in the U.S.

Comment e: If full effect is given to this Principle and to Principle 1, there should be no need for rules requiring data users to store their data only domestically.

Principle 3: In commercial transactions in which the contracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction.

Comment a: Principles 1 and 2 recognize that a state may exercise its jurisdiction over and apply its laws to data in the possession, custody, or control of organizations and data subjects, or to data that is subject to targeting activities, as long as there is a sufficient nexus to that state's territory. Principle 3 stipulates that parties should, within certain limits, be allowed to contract on the jurisdiction and data protection law

applicable for the processing of their data and for data protection breaches in connection with their contract. As such, this Principle recognizes that natural persons ought to have the right to determine the uses of their personal information, and that within such right should be the right to consent to the jurisdiction or the application of the laws of a foreign nation in relation to their data so long as the chosen law bears a logical relationship to the parties and the transaction. The practical relevance of Principle 3 is to respect the parties' common intentions, to offer a high degree of certainty in commercial contexts, and ultimately to facilitate access to justice by allowing for a direct determination of the law applicable to personal information without reference to jurisdictional questions. This Principle thus implicates private law, whereas the first two Principles concerned public law and the right of states to assert sovereignty over people, information, and activities that are within their territorial control or that assert a substantial effect within their territory.

Comment b: The openness of a country's law to party autonomy when it comes to choice of jurisdiction and law will depend in part on its underlying conception of data privacy. Party autonomy is an established fundamental principle of private law. However, stricter requirements for individual consents to data processing apply, and burdens for a valid choice of law are higher where such choices effectively lead to waivers of existing data privacy protections and, as in the EU, data protection laws give effect to a constitutional, personality, or other fundamental right to informational self-determination.[28]

Comment c: However, it is submitted that there should be room for private autonomy in the data privacy context.[29] The right to informational self-

---

[28] *E.g.*, GDPR, *supra* note 2, Recital 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.") and 32 ("Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement . . . .").

[29] In Europe, the CJEU has not yet ruled on the question, and current doctrine and practice appear divided. Under the old Data Protection Directive 95/46/EC, 1995 O.J. (L 281), the Article 29 Data Protection Working Party had opined "that the applicability of European privacy law cannot be excluded by a unilateral declaration or contractual agreement" (Opinion 02/2013 on apps on smart devices, Feb. 27, 2013, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf). *Cf.* also the overview in Maja Brkan, *Data Protection and Conflict-of-Laws: A Challenging Relationship*, 2 EUROPEAN DATA PROTECTION L. REV. 324 (2016). The discussion in Germany provides a good illustration of the debated issues: Judgments of the Landgericht Berlin [LG][Regional Court], Mar. 6, 2012, AZ. 16 O 551/10 (enforcing an choice of applicable data protection law) and the Verwaltungsgericht Schleswig-Holstein [VG][Administrative Trial Court] in Facebook Ireland Ltd v Independent Data Protection Authority of Schleswig-Holstein, Feb. 14, 2013, 8 B 60/12 (rejecting such a choice);

determination is not absolute but must be balanced against other freedoms, in particular, economic freedom.[30] Stated differently, a natural person may be incapable of contracting away all his or her fundamental data rights, but the same person should be allowed to waive such rights under specific circumstances and for a particular purpose. Further, the principle of mutual regard for the jurisdiction of sovereign states provides that nations may apply their laws to data where such data has been designated as governed by their jurisdiction with legally valid consent. To decide differently would mean to assimilate every data subject to the weaker status of a consumer worthy of special protection, and to indiscriminately accept an overriding public interest of one sovereign state in all areas of data privacy law, even where it regulates the relationship between private parties with comparable bargaining power, as is the case in commercial contexts.[31] The benefits of the modern information society can only be effectively realized if one accepts some of the risks that go along with it. To consider all jurisdiction and choice-of-law agreements in the data privacy field as inherently unfair would appear anachronistic, given the nature of global commerce. It would also amount to disregarding commercial practice where agreements on jurisdiction and applicable law commonly occur and regularly do not treat data protection issues separately from other contractual issues.

Comment d: A specific individual waiver of rights under the jurisdiction or laws of a foreign sovereign does not per se negate the right of that sovereign to exercise sovereignty over certain data regardless of the location of such data. While Principle 3 stipulates that there should be room for a choice of jurisdiction or law regarding personal data, even where such a choice acts as a waiver of protections of another jurisdiction, it recognizes that the implied derogation of other potentially applicable jurisdictions or laws is limited where such derogation would be contrary to another sovereign's overriding national interests.

GDPR, *supra* note 2, art. 3, *in* KOMMENTAR ZUR DATENSCHUTZ-GRUNDVERORDNUNG (Jürgen Kühling, Benedikt Buchner eds., 2017), at nn.105–06.

30 Accepted by the GDPR, *supra* note 2, itself (*cf.* Recitals 2, 5, 7, and 9). Significantly, the seminal Volkszählungsurteil ("Census Verdict") of the German Federal Constitutional Court, which created the German constitutional right to informational self-determination, accepts that the guarantee of this right has its limits. Natural persons have no absolute, unrestricted control over their data. Rather, they participate through communication in their respective social contexts. Accordingly, information is a social phenomenon that cannot be exclusively assigned to an affected individual (Census Verdict, BVERFGE 65, 1; AZ. 1 BVR 209/83 *et al.*, Dec. 15, 1983, at n.174).

31 *Cf.* WOLFGANG HOFFMANN-RIEM, INFORMATIONELLE SELBSTBESTIMMUNG IN DER INFORMATIONSGESELLSCHAFT—AUF DEM WEG ZU EINEM NEUEN KONZEP DES DATENSCHUTZES 531–532 (1998).

Accordingly, Principle 3 remains subject to overriding mandatory provisions which, in the absence of choice, would have been applicable according to Principles 1, 2, and 6. This Principle accepts that in such cases, another jurisdiction or law may apply alongside the agreed one, even though they deal with the same data processing. In the interest of international comity, however, the application of such overriding national provisions should be the result of a balancing of all interests involved and be construed narrowly.

Comment e: In order to ensure the predictability of the agreement's validity, Principle 3 does not subject the choice of jurisdiction or law to any requirement as to form, unless otherwise agreed by the parties. Beyond this, it leaves questions of existence and substantive validity of the choice to the provisions of the chosen law.[32] This appears adequate because it gives effect to the parties' choice, and because the meaning of consent, and the requirements for a valid consent, differ among jurisdictions. For example, Article 4(11) GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes."[33] In contrast, in the U.S, the most fundamental principle for consent is notice, as "without notice a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[34] Accordingly, recurring to the

---

[32] Hague Conference on Private International Law, Hague Principles on Choice of Law in International Commercial Contracts, art. 5 (March 19, 2015), https://www.hcch.net/en/instruments/conventions/full-text/?cid=135 [hereinafter Hague Principles]; International Law Association (ILA), Protection of Privacy in Private International and Procedural Law, at 20, 30–31, (2018), https://www.mpi.lu/fileadmin/mpi/medien/research/ILA_Committee_Protection_Privacy_Private_International_and_Procedural_Law/ILA_Committee_Privacy_Interim_Report_Sydney_REVISED_FINAL.pdf.

[33] To be freely given, the Article 29 Working Party Guidelines on Consent under Regulation 2016/679 of April 16, 2018, as endorsed by the EDPB, stress the need for free choice, and find that free choice is lacking if there is an imbalance of power in the relationship between the data subject and the controller (such as the employer-employee relationship) and potentially invalid if a service would be denied to the data subject unless he or she gives consent. Specificity requires granular detail: "If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. [. . .] When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e., the separation of these purposes and obtaining consent for each purpose." (https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf) Informed consent requires that all relevant information be provided regarding that consent in plain and clear language. And unambiguous consent requires a clear expression of intent or clear affirmative action by the data subject. Finally, GDPR, *supra* note 2, art. 7(3) requires that consent may be withdrawn as easily as it was given.

[34] In the United States, there is no single, comprehensive national law or policy (except with respect to protecting children) regulating the use of personal data or defining consent. There are many federal and state privacy laws with varying definitions, including, most prominently, the Federal Trade Commission Act. "While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have

applicable procedural law of the court, let alone to the substantive requirements of the derogated jurisdiction or law, would endanger the goal of decisional harmony.

Comment f: Principle 3 allows both *ex ante* and *ex post* choices of the jurisdiction and the law applicable to personal data.[35] This is relevant in particular where the laws of a country qualify obligations arising out of violations of privacy and personality rights as noncontractual in nature.[36]

Comment g: In order to protect natural persons who lack bargaining power from unexpected and potentially harmful effects of a specific choice of jurisdiction and law, Principle 3 proposes two limitations.[37]

First, it accepts a free choice of jurisdiction and law only for commercial transactions in which the contracting parties have comparable bargaining power.[38] The commercial nature of a transaction should be defined on a case-by-case basis, having due regard to the nature and aim of a particular contract in the context of trade or professional activity, and not in the abstract by reference to the subjective situation of the person concerned. This is because the same person may act as a commercial operator in relation to certain transactions, and as a consumer in relation to others. It is also proposed to construe exceptions from the commercial nature of a transaction narrowly, and limit them to transactions solely for the purpose of satisfying a natural person's own needs in terms of private consumption. The qualification of a transaction should also be irrespective of whether the respective activities are planned for the present or future.[39]

---

been recognized as essential to ensuring that consumers are properly informed before divulging personal information: identification of the entity collecting the data; identification of the uses to which the data will be put; identification of any potential recipients of the data; the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information); whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data." (FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7–8 (1998).

35 Note that certain jurisdictions may have issues with *ex ante* choices of law for tortious events, such as violations of personality rights.

36 ILA, *supra* note 32, at 23.

37 *Cf.* Principle 4, *infra*.

38 *Cf.* The Hague Principles, *supra* note 32, art. 1(1).

39 In line with the CJEU's case law on the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters: Case C-269/95, Francesco Benincasa v Dentalkit Srl, ECLI:EU:C:1997:337, ¶¶ 15–16; Case C-464/01, Johann Gruber v Bay Wa AG, ECLI:EU:C:2005:32, ¶¶ 36–45. *Cf.* also ILA, *supra* note 32, at 20.

Second, a choice of jurisdiction and law should bear a reasonable nexus to the parties and the transaction. This is of particular importance in jurisdictions where obligations arising out of violations of privacy and personality rights are qualified as noncontractual in nature.[40]

Comment h: A choice of jurisdiction and law may be express or implicit. If the latter, the choice should appear clearly from the provisions of the contract or the circumstances of the case, whereby such circumstances should accord with practices that the parties have established between themselves.[41] Where data is transferred cross-border in a commercial context, Principle 3 stipulates an assumption of an implied choice of jurisdiction and law in favor of the place of destination. For example, a natural person who knowingly transfers his or her personal data, or has his or her personal data transferred, for commercial purposes to a nation other than one that would otherwise claim jurisdiction, can be assumed to have consented to the jurisdiction and law of that other sovereign nation for all purposes reasonably expected to be related to such transfer. The practical relevance is to provide certainty to the handling of the large data volumes knowingly transferred on a regular basis between jurisdictions. Accordingly, this Principle acknowledges that a single cross-border data transfer can include many different purposes and treats them all in the same way as long as it can be assumed that the data subject could, at the time of the transfer, reasonably know the potential that such purposes could materialize.

Comment i: For comparable bargaining power to exist between the parties, both parties should have knowledge, or should be informed, of the implications of a choice of jurisdiction or law, in particular where it leads to consent to data processing, and to a waiver of protections that would otherwise be afforded by the derogated jurisdiction or law. Absent such knowledge, the chosen jurisdiction or law should not claim primacy over the jurisdictions or laws which would otherwise be applicable.

Case Study 5: While residing in France, Subject A signs a contract with Subject B, who resides in New York, to perform services in Brazil and attaches his work history and other personal information to the contract, which B then forwards to Customer C, who is in Brazil, where the contract is to be performed. All parties know or should know that

---

[40] ILA, *supra* note 32, at 24.

[41] *Cf.* The Hague Principles, *supra* note 32, art. 4, at 20, 30.

courts in New York allow complete pretrial discovery practices, and they nonetheless agree that the courts of New York shall have jurisdiction and the laws of New York will apply to any disputes "regarding the contract's interpretation and performance." A dispute later arises in Brazil regarding the lawfulness of the contract under Brazilian law. Because the nature and aim of the transaction is that of a trade or professional activity, the selection of New York law, and the corresponding derogation of French law, does not impinge on France's sovereign authority. Similarly, settled principles of international law show that Brazil has jurisdiction over all three parties to the extent the effects of their actions materialize in that jurisdiction. As far as the dispute concerns the lawfulness of the contract under its laws, rather than the performance of the contract, Brazil retains the primary interest, and the courts of New York may, as a prudential matter, refrain from exercising jurisdiction over that issue, or hold any dispute concerning the lawfulness of the contract under the laws of Brazil in abeyance pending the outcome of the issue by the Brazilian administrative or judicial authorities responsible for deciding that issue.

Case Study 6: A U.S. company in Pennsylvania offers an online service that helps doctors stay abreast of treatment options for certain diseases, but it will only sell those services to doctors who accept its terms and conditions online. Its terms and conditions include a jurisdiction and choice-of-law clause in favor of Pennsylvania law with respect to all disputes involving the service. A medical doctor in Germany accordingly submits to the jurisdiction and laws of Pennsylvania for purposes of a specific processing or use of her personal data collected in dealing with the company. Under the rules of Pennsylvania, this consent is valid; under the GDPR, however, the consent might be considered invalid because it could be considered to amount to a coercive waiver of the doctor's data privacy rights. To the extent that the German doctor enters into the transaction with the Pennsylvania company in her professional capacity, and no data of third parties such as patients are affected, her right to choose the applicable jurisdiction and law must implicate her ability to give consent.

Principle 4: Outside of commercial transactions, where a natural person freely makes a choice, that person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data.

Comment a: Like Principle 3, Principle 4 recognizes that every affirmative choice of jurisdiction or law may imply a derogation of protections and standards that may be considered unacceptable by another jurisdiction for a

variety of reasons, ranging from consumer protection to protection of sovereign national interests. The practical application of Principle 3 limits the free choice of jurisdiction or law for data to the commercial context and thereby provide certainty and flexibility where the parties to a contract have comparable bargaining power, and data subjects can be expected to foresee and understand the consequences of their choice while maintaining the protections afforded by substantive laws.

Comment b: Although both Principle 3 and Principle 4 recognize that every affirmative choice of jurisdiction or law may imply a derogation of protections, this Principle also recognizes that some cross-border movements of information do not involve any affirmative or, for that matter, any conscious decisions about applicable law. Specifically, Principle 4 speaks directly to the social communications between natural persons where the cross-border transfer of personal information is merely incidental to the purpose, and there is nothing in the content to trigger any State's sovereign interests or concerns. In other words, this is the flip side of Principle 3 and involves noncommercial transactions. Here, data subjects, assuming they think about it at all, would presumably expect that they would enjoy all the rights and freedoms that their native citizenship allows them; and except when such communications betray an effort or at least an intent to violate the laws of a given jurisdiction, no sovereign has a cognizable concern that would warrant upsetting the sovereign rights of the person's State of citizenship.

Comment c: There are different approaches to distinguishing commercial and noncommercial uses of data. At the highest level, noncommercial use includes artistic, scholarly, educational, personal, family, or other uses, including social media, when they are not associated with the professional or commercial activities of a natural person.

The 2009 Creative Commons report "Defining Noncommercial"[42] lists nine qualitative factors for analyzing noncommercial use.

i. Perceived economic value of the content;

ii. The status of the user as an individual, an amateur or professional, a for-profit or not-for-profit organization, etc.;

[42] *Available at* https://mirrors.creativecommons.org/defining-noncommercial/Defining_Noncommercial_full report.pdf (last visited June 4, 2019).

iii. Whether the use makes money (and if so, whether revenues are profit or recovery of costs associated with use);

iv. Whether the use generates promotional value for the creator or the user;

v. Whether the use is personal or private;

vi. Whether the use is for a charitable purpose or other social or public good;

vii. Whether the use is supported by advertising or not;

viii. Whether the content is used in part or in whole; and

ix. Whether the use has an impact on the market or is by a competitor.

Comment d: In the commercial context, a choice of jurisdiction or law and related consent to data processing may be more readily assumed than in the noncommercial context. However, as the Comment g. to Principle 3 demonstrates, consent implied or considered given in the commercial context should be limited to such processing and use of personal data that can be considered reasonably related to the fulfilment of the commercial purpose. Consent for processing and use of personal data in excess of what is required for the fulfilment should not be implied or considered given by the operation of law. Information should be available to the natural person regarding the extent and scope of the consent implied or considered given in the commercial context.

Case Study 7: Assume the same facts as those set out in Case Study 5, and also assume that A wrote several letters and emails to his friends and business associates discussing the contract and his understanding of what it involved, and assume that he also maintained a social media account on which he shared with his friends in France his unfavorable views about the court system and elected leaders in New York and his interest in traveling to and working in Brazil. In the ensuing litigation in New York, his opponents seek discovery of all communications he has had relating to the contract and his work in Brazil. In this situation, A's letters and emails to his friends and business associates relating to his understanding of the contract should be discoverable in New York because he has consented to the jurisdiction of its courts and laws. Similarly, whether the identity of his friends and business associates must be disclosed should be resolved in the first instance by the courts in New York while giving due regard to the sensitivity of that personal data under the laws of France and their importance, or lack thereof, to resolving the pending dispute. Conversely, on the facts as stated, there is no

apparent reason why the court should allow discovery of the content of A's social media accounts. A's social media is noncommercial in nature, and he has not consented to disclosure of that information in New York, or anywhere else. Also, while his views on politicians, courts, and foreign travel may be interesting, they are not on their face sufficiently relevant or important for the courts in New York to allow discovery of them in contravention to the laws and policies of Brazil.

Comment e: Similarly, the Advocate General's January 2019 Opinion in the *Google v. CNIL*[43] matter provides an excellent example of the limits of extraterritorial jurisdiction under the EU Data Protection Directive in the context of private usage of internet search engines. That matter concerned a request by certain natural persons that Google delete all links to them on a worldwide basis. After Google refused to comply with a formal notice from the CNIL (*Commission Nationale de l'Informatique et des Libertés*), and instead limited its de-referencing to the 28 Member States, the CNIL imposed a substantial fine, which Google appealed to the Court of Justice of the European Union. In January 2019, the Advocate General issued his opinion recommending that the Court reject the CNIL's view. In short, he found that an expansive application of the extraterritorial jurisdiction to the right to be forgotten is untenable. That right, he reasoned, must be balanced against the interests of other people and nations in accessing information. He thus concluded that "if worldwide de-reference were possible, . . . persons in third States would be prevented from accessing information, and in turn, . . . third States would prevent persons in the EU Member States from accessing information." Although he reserved the possibility that wordwide de-referencing might be warranted in some situations, he clearly believed that the Google matter was not such a situation.

More specifically, the Advocate General first observed that the provisions of the EU Data Protection Directive did not expressly address the territorial scope issue. In his view, a distinction should be made based on the location of the search request, such that if a search is input outside of the EU, the results should not be impacted by the de-listing of the search results in the EU.

He further explained that the EU Treaties apply to EU Member States and that EU law should not apply beyond the territory of the EU Member States. The Advocate General recognized that EU law may

[43] Case C-507/17, Google v. Commission Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:15.

have extraterritorial effect, but such effect only applies in exceptional cases, such as in competition law or trademark law cases affecting the EU internal market.

Finally, the Advocate General stressed that the right to be forgotten must be balanced against other fundamental rights such as the legitimate public interest in accessing the information sought, and that the audience concerned is not worldwide but instead European. In his view, the CNIL's approach entailed a risk that people in non-EU countries would be prevented from accessing information and, in turn, that non-EU countries could prevent people in the EU from accessing information. Accordingly, "a race to be bottom" could occur to the detriment of the freedom of expression at both the European and worldwide levels.

Principle 5: Data in transit ("Data in Transit") from one sovereign nation to another should be subject to the jurisdiction and the laws of the sovereign nation from which the data originated, such that, absent extraordinary circumstances, the data should be treated as if it were still located in its place of origin.

Comment a: When organizations and natural persons interact across borders, they create potential data transfer situations where the data subject is located in one country and the entity possessing the data is in another. This is because through the course of doing business and defending against claims, data often leaves one nation and crosses into another. This Principle 5 rests upon the proposition that in such instances, the jurisdiction and law of the nation in which the person or entity initiating the transfer resides shall be treated as the originating jurisdiction and therefore govern the data until it reaches its country of destination. Where there is a choice of jurisdiction or law, such choice shall be recognized in lieu of the jurisdiction and law of the place of origin.

Comment b: Data transfers may be initiated by different parties depending on the circumstances. This Principle applies equally to data that is placed in transit by the data subject and data placed in transit by a data custodian. Distinguishing between these two individuals would create an uneven playing field and an unwieldy regulatory structure.

Comment c: Data in Transit should be entitled to transit without observation, alteration, or abridgement except for national security or law enforcement purposes. Such Data in Transit should be marked as such, including information as to its place of origin and final place of

destination. This Principle recognizes that even when a sovereign has the power to assert itself with respect to data in all ordinary cases, its interest in particular data or data sets will be minimal, if not wholly nonexistent. In such circumstances, mere respect for the laws and sovereign interests of other nations strongly suggests that the data's transient "host" decline from interfering with the free flow of data across its national borders.

Comment d: Data in Transit for commercial, personal, or governmental purposes shall be presumed to have a lawful purpose and should be transferred unmolested by entities, governments, or natural persons. For example, data lawfully placed in transit in Country A may be carried by fiber-optic cables that pass through Country B on the way to their intended destination in Country C, and no party may have "intended" or even been aware of the data's contact with Country B. In that situation, established principles of International Law recognize that Country B has sovereignty over the data as it passes through its territory.[44] Despite having the power, however, to act with respect to the data while it is in transit, except in limited circumstances where a country may have an overriding interest or even an obligation under International Law to act with respect to such data, it should refrain from impeding the flow of data through its territory.[45]

Comment e: This Principle does not address directly the legal standards for and potential conflicts related to national security surveillance and law enforcement access to Data in Transit. It clarifies, however, that where Data in Transit passes temporarily through a country with less restrictive laws regarding access than those of the county of origin, national security and law enforcement authorities may not take advantage of those less restrictive laws to access the data.

Principle 6: Where personal data located within, or otherwise subject to, the jurisdiction or the laws of a sovereign nation is material to a litigation, investigation, or other legal proceeding within another sovereign nation, such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data.

Comment a: A fundamental right of all people is to have their claims adjudicated by a fair and impartial tribunal and to able to defend against claims made

---

[44] TALLINN MANUAL 2.0, *supra* note 11, at 13–14; *cf. id.* at 33.

[45] *Id.* at 33–34.

in proceedings before such tribunals. Nations have broad discretion in developing tribunals and procedures that give meaning to that fundamental right and those tribunals. It therefore follows that the requirements of those tribunals are entitled to deference and respect by other nations.

Comment b: A fundamental right of all people is to have their health, safety, and welfare protected by the nations in which they reside and through which they traverse. When questions arise concerning possible law violations, all people similarly have a fundamental duty to respond to lawful inquiries from fair and impartial investigators. Here, too, nations have broad discretion in establishing investigative authorities and procedures that give meaning to the nature and scope of these duties. Those investigative procedures are entitled to the utmost deference and respect by other nations.

Comment c: It therefore follows that when courts or investigative authorities provide for the adequate protection of data transferred to the country of interest, then the data should be produced to the party that needs it, to the extent such data is relevant and material to the adjudicative proceeding or law enforcement investigation in question. Privacy laws should not restrict transfer where the data is adequately protected by appropriate safeguards.

Case Study 8: A U.S. federal agency issues a subpoena that seeks personal information about particular data subjects and relates to a law enforcement investigation the agency is undertaking. The subpoena's recipient asks that the agency stipulate to protecting the data it produces from any public disclosure and to destroy or return the information at the end of the investigation. The agency declines to so stipulate, noting that it is subject to various statutes that preclude it from making the information it receives in investigations public, unless it first gives notice to the interested parties and gives them an opportunity to seek court-ordered protections. It also notes that the Federal Records Act and other laws regulate how it disposes of records at the end of its investigation. If the party then refuses to comply, a court may properly conclude that the personal data in question is adequately protected within the meaning of Principle 6. Similarly, a Supervisory Authority who receives a complaint from the data subjects about the transfer of personal data to a U.S. federal agency should consider the legitimate interests of the U.S. government in conducting the investigation and the statutory protections that apply to the data the agency receives in the course of its investigation.

Case Study 9: In a private action to enforce a contract, the defendant issues a request for production to the plaintiff demanding that it turn over documents containing personal data that is stored in the EU and pertain to EU data subjects. The plaintiff refuses to produce the requested information, claiming that it is forbidden from doing so because of the GDPR. The defendant offers to limit its demand to documents that are uniquely in the EU and that are necessary and relevant, but adequate for the case. It also offers to stipulate to a protective order that commits it to securing the data, using it only for the litigation in question, to protect it from any further disclosures, and return or destroy the data at the end of the litigation to the extent it can do so consistent with its obligations to the client. On a motion to compel, a U.S. court may properly find that defendant's offer does not risk any significant harm to data subjects, and that the plaintiff should therefore comply with the request. Similarly, a Supervisory Authority, if called upon to review the matter, may properly conclude there are adequate assurances that the data will be secured and that the defendant has properly applied data minimization principles to its request for data. It may therefore conclude that the risk of harm to data subjects is minimal, if not nonexistent.

APPENDIX: DATA PRIVACY COMPLEXITY AND BACKGROUND

a. Origins of Data Privacy Concepts

What we mean today by data privacy begins in the modern era, roughly by the end of the 17th century, with the rise of the individual, the emergence of the modern, bureaucratically organized state, and the tensions between the two.[46]

It was not until well into the 19th century, mainly building upon the recognition of human rights in the French and U.S. constitutions, that the hitherto largely philosophical concept of individual privacy achieved legal effect. Two U.S. lawyers, Samuel Warren and Louis Brandeis, are credited with having first developed privacy protection into a coherent notion, conceptualized as "an instance of the enforcement of the more general right of natural persons to be let alone."[47]

In the early 20th century, the two main data privacy paradigms, the European and the American, evolved. As privacy law across the globe diverged, they remained motivated by a concern for governmental abuse of personal data. From the end of the 20th and by the beginning of the 21st century, the history of data privacy has been shaped by two developments: the appearance of new actors on the data privacy stage, in particular large private corporations with access to significant data in the banking, insurance, advertising, healthcare, and information technology industries; and the expansion of the internet and related information technologies. The latter led to an exponential growth of data volumes, de-localization of data processing through the development of encryption and cloud computing, and quickly shifting societal and cultural concepts of privacy.

b. Different Conceptions of Data Privacy

The foundations for the U.S. data privacy paradigm were laid by the Supreme Court rulings in the 1960s and 1970s. Building upon Warren and Brandeis' work and an earlier decision in *Griswold v. Connecticut*,[48] the Court in *Katz v. United States* defined the right to privacy by referring to a private vs. public dichotomy: "What a person knowingly exposes to the *public*, even in his own home or office, is not a subject of Fourth Amendment Protection [which provides broad limitations on the government's power to search and seize; added]. But what he seeks to preserve as *private*, even in an area

---

[46] For a more detailed history of information privacy, *cf.* Kai von Lewinski, *Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in* DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN 23 (Jan-Hinrik Schmidt & Thilo Weichert eds., 2012); Daniel J. Solove, *A Brief History of Information Privacy Law, in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE (Kristen J. Mathews ed., 2d ed. 2016), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271.

[47] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890), at 205.

[48] Griswold v. Connecticut, 381 U.S. 479, 484 (1965), finding the right to privacy to be enshrined in the "penumbras" of many of the ten amendments of the Bill of Rights.

accessible to the public, may be constitutionally protected."[49] In *Whalen v. Roe*, the Court then framed the U.S. data privacy paradigm as "individual interest in avoiding disclosure of personal matters."[50]

Around the same time, in 1983, the German Federal Constitutional Court in its seminal *Census Verdict* ("Volkszählungsurteil") created the German constitutional right to informational self-determination. Rooted in art. 2 para. 1 (right of personality) and art. 1 para. 1 (right to human dignity) of the German Constitution, such right guarantees, in principle, the power of natural persons to make their own decisions regarding the *disclosure and use* of their personal data.[51] The Court emphasized that it is not possible to limit the question of worthiness of protection exclusively to the nature of the information. Knowledge of the context in which data is used and collated is necessary to establish the importance of data and the admissibility of a restriction of the right to informational self-determination.[52]

By 1979, general data protections laws had been enacted in seven member states of the European Economic Community (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway, and Sweden). In three countries (Austria, Portugal, and Spain), data protection was incorporated as a fundamental right in the constitution. In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), the first legally binding international instrument in data protection, which became foundation of the 1995 European Data Protection Directive.[53] In the U.S., meanwhile, privacy protection receded. For example, financial privacy was curtailed throughout the 1970s. And in the 1980s, the U.S. Supreme Court decided a series of cases adopting a narrow view of what constitutes a protected reasonable expectation of privacy.[54]

---

[49] Katz v. United States, 389 U.S. 347, 351 (1967) (emphasis added).

[50] Whalen v. Roe, 429 U.S. 589, 599–600 n.26 (1977). The Court also identified a second individual "interest in independence in making certain kinds of important decisions" and characterized these decisions as dealing with "matters relating to marriage, procreation, contraception, family relationships, and childrearing and education." It noted that in these areas "it has been held that there are limitations on the States' power to substantively regulate conduct."

[51] Census Verdict, BVERFGE 65, 1; AZ. 1 BVR 209/83 *et al.*, Dec. 15, 1983, at n.173. *Cf.* also Hans-Jürgen Papier, *Verfassungsrechtliche Grundlegung des Datenschutzes, in* TALLINN MANUAL 2.0, *supra* note 11, at 67.

[52] Census Verdict, at nn.176–77.

[53] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), *available at* http://www.refworld.org/docid/3ddcc1c74.html. For an overview of the European developments *cf.* SIAN RUDGARD, ORIGINS AND HISTORICAL CONTEXT OF DATA PROTECTION LAW 9 (2012), https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf; Hielke Hijmans & Owe Langfeldt, *Datenschutz in der Europäischen Union*, *in* DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN, *supra* note 46, at 403.

[54] Solove, *supra* note 46, at 1–28, with further references. *Cf.* also DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN, *supra* note 46, at 420.

Since the 1980s, the U.S. Congress has passed major statutes to address emerging privacy issues. The U.S., however, regulates data privacy sectorally and narrowly.[55]

The U.S. largely has followed the distinction between public and private data, and it has afforded the latter protections over the former. Germany set out to protect the underlying right of a natural person to determine the disclosure and use of his or her personal data, and this conception of data privacy influenced European data privacy, from the case law of the European Court of Human Rights[56] to the GDPR.[57]

Thus in Europe, *all* processing of personal data requires a legal (constitutional) basis.[58] In the U.S., processing of personal data is allowed *unless* it is forbidden under specific circumstances.[59]

c. The European Data Privacy Paradigm

The GDPR replaces the EU Data Protection Directive and seeks to provide a comprehensive[60] data privacy framework intended to ensure a consistent level of protection for natural persons throughout the European Union and to prevent divergences hampering the free movement of personal data within the Union's free market.[61] The GDPR continues to pursue the broad European paradigm of

---

55 Solove, *supra* note 46, at 1–40.

56 Rotaru v. Romania, App. No. 28432/95, Eur. Ct. H.R. (2000) at n.43, relating to European Convention of Human Rights, art. 8: "Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life.' [. . .] Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."

57 GDPR, *supra* note 2, Recital 26.

58 *Id.*, art. 6.

59 A general limitation of the processing of personal data would arguably be seen in the U.S. as an interference with the autonomy and responsibilities of the state and the economic freedom of individuals. For the different paths that have come to define the European and U.S. data privacy paradigms *cf.* Thilo Weichert, *Datenschutz und Überwachung in ausgewählten Staaten*, *in* DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN, *supra* note 46, at 419.

60 Nevertheless, the GDPR is part of a broader data privacy "puzzle." Activities not covered by the GDPR include those falling outside the scope of EU law (such as activities concerning national security) and data processing by competent authorities for the purpose of the prevention, investigation, detection, or prosecution of criminal offenses and associated matters (GDPR, *supra* note 2, Recital 19). The GDPR is also "without prejudice" to the rules in the E-commerce Directive (Directive 2000/31/EC, 2000 O.J. (L 178/1); GDPR, *supra* note 2, Recital 21), in particular to those concerning the liability of intermediary service providers. Finally, the GDPR is not intended to impose additional obligations on top of the obligations contained in the ePrivacy Directive dealing with the processing of data across public communication networks, which therefore is to be amended to ensure consistency across the two regimes (Directive 2002/58/EC, 2002 O.J. (L 201/37) as amended by Directives 2006/24/EC, 2006 O.J. (L 105/54) and 2009/136/EC, 2009 O.J. (L337/11); GDPR, *supra* note 2, Recital 173.

61 GDPR, *supra* note 2, Recitals 10 and 13.

data privacy as a fundamental right,[62] and it conceptualizes privacy as the right to informational self-determination: "The principles of data protection should apply to *any information* concerning an identified or identifiable natural person."[63]

Despite this conceptual breadth, the GDPR leaves complexities and uncertainties for data in an international context.[64]

The GDPR claims significant extraterritorial effect. First, EU "established" controllers or processors fall into its scope where personal data is processed "in the context of their activities."[65] If these tests are met, the GDPR applies, regardless of whether the actual data processing takes place in the EU.[66] Second, the GDPR asserts jurisdiction over non-EU "established" organizations where an EU data subject's personal data is processed in connection with the "offering of goods or services" to her or him, or where the behavior of natural persons within the EU is "monitored."[67] Yet it provides no

---

62 Rooted in article 8(1) of the Charter of Fundamental Rights of the European Union (2010 O.J. C 83/393) and article 16(1) of the Treaty on the Functioning of the European Union (2012 O.J. C 326/47). *Cf.* "Everyone has the right to the protection of personal data concerning them." GDPR, *supra* note 2, Recital 1.

63 GDPR, *supra* note 2, Recital 26 (emphasis added).

64 For the following *cf.* LINKLATERS, THE GENERAL DATA PROTECTION REGULATION. A SURVIVAL GUIDE (2016), https://www.linklaters.com/en/insights/publications/2016/june/guide-to-the-general-data-protection-regulation; BIRD & BIRD, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (2019), https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic.

65 GDPR, *supra* note 2, art. 3(1).

66 It remains to be seen in practice whether, and how much, legal certainty can be provided for these tests. As for the establishment test, the CJEU under the EU Directive adopted a broad and flexible interpretation that should not hinge on legal form and instead qualified an organization as established where it has "any real and effective activity—even a minimal one—exercised through stable arrangements" in the EU. *See* Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság, ECLI :EU:C:2015:639. Data processing was qualified by the CJEU as being "in the context of the activities" of an EU establishment where such processing was "inextricably linked" to the establishment's activities, such as in the case of EU sales offices which promote or sell advertising or marketing targeting EU residents. See, Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, ECLI:EU:C:2014:317, at n.6, asserting a far-reaching "right to be forgotten."

67 GDPR, *supra* note 2, art. 3(2).

clear criteria for determining when goods or services are offered to EU data subjects[68] or when their behavior is monitored.[69]

As a Regulation, the GDPR is directly effective in member states without the need for implementing legislation. The GDPR leaves room, however, for EU member states to legislate on data privacy matters.[70] For example, member states may limit rights under the GDPR in areas such as judicial proceedings, criminal prosecutions, and national security; they may provide for further restrictions on the processing of employee data; and they may pass legislation to reconcile data protection with freedom of expression and information as well as to protect information subject to professional secrecy.[71] A significant number of data processing activities depend on member-state laws, including where the GDPR provides room for a public interest recognized under member-state law to provide a basis to transfer personal data outside of the EU or to restrict such transfer.[72]

Finally, the GDPR provides for one or more regulators, or supervisory authorities, in every member state.[73] While the European Data Protection Board has strong powers to provide guidance and coordinate enforcement of the GDPR through a consistency mechanism,[74] differences in resources and attitudes of supervisory authorities may result in variations in enforcement.

---

[68] *See, e.g.*, Kevin Kish, *What does territorial scope mean under the GDPR?,* IAPP THE PRIVACY ADVISOR (Jan. 23, 2018), https://iapp.org/news/a/what-does-territorial-scope-mean-under-the-gdpr/. In a separate context, the CJEU applied the test whether activities were "directed to" EU member states. It cautioned, however, that the question should be determined on a case-by-case basis (Pammer v. Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v. Heller [Joined cases (C-585/08) and (C-144/09)] ECLI:EU:C:2010:740). Broadly applicable factors such as the use of a language or a currency generally used in a member state with the possibility of ordering goods or services in that language, or the mentioning of customers or users who are in the EU, are considered as relevant. GDPR, *supra* note 2, Recital 23.

[69] Monitoring refers to the tracking of individuals online to create profiles, including where this is used to take decisions to analyze or predict personal preferences, behaviors and attitudes (GDPR, *supra* note 2, Recital 24).

[70] While the GDPR says when it shall be applicable, it does not prescribe the same applicability rules for national implementation laws. This leads to a "conundrum" of diverging national implementation laws rather than to the harmonization intended by the GDPR. *Cf.* Lokke Moerel, *GDPR Conundrums: The GDPR applicability regime—Part 1: Controllers*, IAPP THE PRIVACY ADVISOR (Jan. 29, 2018), https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/.

[71] GDPR, *supra* note 2, arts. 23, 85, 88, 90.

[72] *Id.*, art. 49(4) and (5). Other examples include the right of member states to provide additional justifications for the processing of personal data (art. 6(1)(c)) and to restrict the processing of personal data relating to criminal convictions and offenses (art. 10).

[73] *Id.*, art. 51.

[74] *Id.,* arts. 63–76.

d. The U.S. Data Privacy Paradigm

No single, comprehensive federal law regulates the collection and use of personal data in the United States. Instead, multiple federal and state laws and regulations govern specific sectors and aspects of data privacy and security. In addition, several federal and state agencies have issued guidelines and created frameworks for data collection and use. The following are the most prominent federal privacy laws:[75]

- The Federal Trade Commission Act[76] (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act[77] (COPPA). The FTC Act applies to companies and persons doing business in the U.S.

- The Financial Services Modernization Act[78] (Gramm-Leach-Bliley Act (GLB)) regulates the collection, use, and disclosure of financial information. It applies broadly to financial institutions and to other businesses that provide financial services and products. The GLB Act applies to financial institutions and to affiliated and nonaffiliated third parties that receive nonpublic personal information from financial institutions. It also prohibits fraudulent efforts to obtain or disclose nonpublic personal financial information.

- The Health Insurance Portability and Accountability Act[79] (HIPAA) regulates medical information. It can apply broadly to healthcare providers, data processors, pharmacies, and other entities that come into contact with medical information. HIPAA regulations apply to the collection and use of protected health information (PHI) and provides standards for protecting medical data and standards for the electronic transmission of medical data.[80] Certain business associates of covered entities may also have contractual obligations to safeguard PHI, including those operating outside of any U.S. jurisdiction.

- The Fair Credit Reporting Act[81] and the Fair and Accurate Credit Transactions Act[82], which amended the Fair Credit Reporting Act, apply to consumer reporting agencies,

---

75 These summaries are adapted from, Ieuan Jolly, *Data Protection in the United States: overview*, THOMPSON REUTERS PRACTICAL LAW (July 1, 2016), https://www.practicallaw.com/dataprotection-guide.

76 15 U.S.C. §§ 41-58.

77 15 U.S.C. §§ 6501-6506.

78 15 U.S.C. §§ 6801-6827.

79 42 U.S.C. § 1301.

80 45 C.F.R. 160 and 162.

81 15 U.S.C. § 1681.

82 Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108–159, December 4, 2003, 117 Stat 1952 (2003).

those who use consumer reports (such as a lender), and those who provide consumer-reporting information (such as a credit card company). Consumer reports are any communication issued by a consumer reporting agency that relates to a consumer's creditworthiness, credit history, credit capacity, character, and general reputation used to evaluate a consumer's eligibility for credit or insurance.

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act[83] (CAN-SPAM Act) and the Telephone Consumer Protection Act[84] regulate the collection and use of email addresses and telephone numbers, respectively.

- The Electronic Communications Privacy Act[85] and the Computer Fraud and Abuse Act[86] regulate the storage, use, and interception of electronic communications, and computer tampering, respectively.

All 50 states have passed laws relating to the collection and use of personal data, and all 50 states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify affected people of security breaches of information involving personally identifiable information.[87] These state laws fall into two broad categories: (i) Data breach notification laws[88] and (ii) substantive protections for specific types of personal information.[89]

---

83 5 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.

84 47 U.S.C. § 227.

85 18 U.S.C. § 2510.

86 18 U.S.C. § 1030.

87 Christopher Wolf & Timothy P. Tobin, Proskauer on International Litigation and Arbitration, Ch. 28 Privacy Laws (I.) Extraterritorial Application of U.S. Privacy Laws (eguide), https://www.proskauerguide.com/law_topics/28/I (last visited June 5, 2019).

88 Data breach notification laws typically define: (1) who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); (2) the scope of "personal information" (e.g., name combined with social security number, driver's license or state ID, account numbers, etc.); (3) what constitutes a breach (e.g., unauthorized acquisition of data); and (4) notice requirements (e.g., timing or method of notice, who must be notified); and contain exemptions (e.g., for encrypted information). There are also some federal regulators who enforce breach notifications.

89 For example, the New York Department of Financial Services Cybersecurity Regulations, 23 NYCRR § 500 (2017) apply to any individual or nongovernmental partnership, corporation, branch, agency, association, or other entity operating under a license, registration, charter, certificate, permit, accreditation, or similar authorization under New York banking, insurance, or financial services laws, a group that includes both foreign and domestic entities. The Regulations impose minimum standards that exceed existing federal standards and introduce additional requirements. State laws and regulations like this add further complexity and create additional potential for conflict with both federal law and the laws of other jurisdictions.

California's new Consumer Protection Act (CCPA) arguably represents a third, broader category of state laws intended to protect consumer privacy more generally.[90] The CCPA draws from the European model and provides a more comprehensive, individual-rights-based approach to protecting privacy. While it is limited to California residents, both the size of California and the fact that other states are looking to it as a potential model mean that the CCPA will significantly influence data privacy policies in organizations throughout the U.S.

U.S. law generally limits the extraterritorial effect of domestic law, including data privacy laws. Choice-of-law principles create a general presumption against extraterritorial application of domestic law.[91] Most federal privacy laws do not preempt state laws, so businesses can face multiple, at times conflicting, obligations even where they operate solely within the U.S.[92] While the proliferation of new state laws in this area has prompted numerous calls for comprehensive federal legislation that would preempt state laws, privacy advocates, state regulators and others have argued that any federal standard should merely establish a floor, leaving states free to impose more stringent standards.

e. International Frameworks

The Council of Europe's Convention 108 remains the first, and to date the most comprehensive, binding international framework to set standards for protecting personal data while also seeking to balance those safeguards against the need to maintain the free flow of personal data for the purposes of international trade. It has been ratified by 55 countries, but not by China, the U.S., or some of the other major trading nations.

The UN Special Rapporteur on the right to privacy, Professor Joseph Cannataci in his 2018 annual report, refers to consultations for the development of principles for regulating big data and open data, indicating they should be drawn from international agreements for data protection as representing "best practice." The report states, "[a]t present, these are the EU's GDPR and the 'modernised' Convention 108 (Convention 108+, 2018) which originated at the Council of Europe but is open to accession globally by States which have enacted consistent principles."[93]

---

[90] CAL. CIV. CODE §1798.140(c) (West 2020).

[91] *See, e.g.,* RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016); Kiobel v. Royal Dutch Petrol. Co., 569 U.S. 108 (2013); Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010).

[92] These state laws limit their application to persons or businesses that conduct business in the state and therefore apply to non-U.S. entities only when they engage in activities meeting that definition. In most states there is very little case law interpreting this requirement, but at least some commentary has suggested the requirement should be read as "coterminous with 'doing business' as applied by courts to personal jurisdiction analysis involving non-residents." For a complete listing of relevant state statutes and comparison of their requirements, *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 205–13 (5th ed. 2017).

[93] Office of the High Comm'r. for Human Rights, Report of the Special Rapporteur on the right to privacy, A/73/45712, at 98 (Oct. 17, 2018).

The Special Rapporteur states that, "Convention 108 is steadily being globalized," while noting that Convention 108 includes many, though not all, of the GDPR's new elements. He concludes that, "it is likely, in the next five to ten years, that the extraterritorial effects of GDPR with the ever-widening club of Convention 108 countries, will have a significant effect on the deepening world-wide privacy culture. The precise nature of this evolution is still emerging . . . ."[94]

The Special Rapporteur's comments suggest that a trend toward a comprehensive international standard may be emerging. In the European Commission's own words: "The primary purpose of [the EU data protection legislation] is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data."[95]

This trend is also driven by the need to square the territorial-based rules governing law enforcement with the inherently fluid nature of data.[96] The question has been set out most prominently in *United States v. Microsoft*, which led to passage of the CLOUD Act. On the other side of the Atlantic, the European Commission has been tasked with preparing legislative proposals to address obstacles in cross-border access to electronic evidence. Access may become more efficient and faster, including by eliminating data localization requirements, while ensuring fundamental rights of natural persons in criminal proceedings and data privacy.[97] At the same time, the Cloud Evidence Group, a working group of the Cybercrime Convention Committee that represents the state parties to the Council of Europe's Budapest Convention on Cybercrime, is exploring solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions.[98]

Despite a plethora of transnational coordination initiatives and regimes, the current system for data protection is highly fragmented and complex, with diverging and sometimes conflicting global, regional, and national regulatory approaches.[99]

---

94 *Id.* at 101.

95 European Comm'n., Commc'n from the Comm'n. to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalized World*, at 4 (Jan. 10, 2017). On Jan. 31, 2018, the European Commission endorsed horizontal provisions for cross-border data flows and personal data protection in trade negotiations, whereby the preferred avenue for the EU are adequacy decisions (*available at* http://europa.eu/rapid/press-release_MEX-18-546_en.htm). If agreed on by the EU member states, this approach can be expected to serve as a starting point for negotiations on provisions to be included in Free Trade Agreements and Bilateral Investment Treaties between the EU and third countries like Japan and Korea.

96 See Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 220–32 (2018).

97 *See e-evidence*, EUROPEAN COMMISSION MIGRATION AND HOME AFFAIRS, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en (last visited June 4, 2019).

98 *See Cloud Evidence Group*, COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/ceg (last visited June 4, 2019).

99 In 2018, The United Nations Conference on Trade and Development (UNCTAD) assessed that 21 percent of countries had no data protection legislation and that many national data protection legislations contained significant gaps and exemptions depending on, e.g., business and data size, types of data, and subject, sensitivity, sources or sector-specificity of data (UNCTAD, *Data Protection and Privacy Legislation Worldwide*, http://unctad.org/en/Pages/

In such a context, basic questions of choice of law and jurisdiction have a profound implication not just for privacy and business interests but, as one commentator put it, most fundamentally for "our understanding of and ability to shape policy going forward."[100]

f. Data Localization Laws

While the GDPR seeks to cloak European personal data in its protections wherever it goes and prohibits it from going certain places if certain conditions are not met, other countries take an even more restrictive approach to cross-border data flows by requiring all data to be stored and processed within its own territory. Data localization laws either require organizations to store and process data on servers physically located within national borders, or they subject the export of personal data to conditions. Although these laws present a significant challenge to the flow of data in commerce,[101] they also help nations protect the privacy of their citizens, as well as their sovereignty over data within their borders.

There are many reasons governments enact data localization laws. First, limiting the unfettered export of personal data can help protect citizens from those who would collect information and use it without their knowledge or consent. Second, and relatedly, data localization laws both enhance the ability of the relevant nation's consumers to seek remedies against those who misuse personal data and facilitate local law enforcement. Third, localization laws make clear to the world that protecting personal information is a national priority. Fourth, the laws have an incidental benefit of encouraging IT investment in the national economy by those who wish to do business with the nation and its residents. Fifth, such laws arguably enhance information security against foreign intelligence operations by requirement foreign intelligence agencies to "come and get" the information they seek.[102]

DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (last visited June 4, 2019)). Many national laws and regional initiatives further allow individual companies to determine the scope of data protection (e.g., by subjecting certain activities to data protection regimes such as the EU-U.S. Privacy Shield) or to exclude certain activities from protection in their public privacy policies. *See* UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016), at 8–10, *available at* https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

100 Daskal, *supra* note 96.

101 Ruslan Synytsky, *New GDPR Laws Ahead—Are Privacy Concerns Inhibiting Global Business*, FORBES (Dec. 6, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/06/new-gdpr-laws-ahead-are-privacy-concerns-inhibiting-global-business/#4beb3fb1719f.

102 The Edward Snowden revelations in 2013 that the U.S. National Security Agency was monitoring internet traffic of foreign governments and their citizens provided a platform for governments to posit that data localizations laws are necessary. As Anupam Chandler and Uyên P. Le identified:

> 'Efforts to keep data within national borders have gained traction in the wake of revelations of widespread electronic spying by United States intelligence agencies. Governments across the world, indignant at the recent disclosures, have cited foreign surveillance as an argument to prevent data from leaving their borders, allegedly into foreign hands. As the argument goes, placing data in other nations jeopardizes the security and privacy of such information.' (Anupam Chandler & Uyên P. Le, *Data Nationalism,* 64 EMORY L.J. 677, 679–680 (2015).

Sixth, and on a darker note, they also enable countries that are so inclined to maintain tighter controls over their citizens and residents.[103]

As of this writing, data localization laws take many forms. For example, Russia's Personal Data Law[104] which became law in September 2015, requires that data operators who collect personal data about Russian citizens must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia. In a similar vein, China's Cybersecurity Law, which took effect in June 2017, seeks to ensure network security, safeguard cyberspace sovereignty, national security, and the societal public interest, and protect the lawful rights and interests of citizens. The law imposes a data localization requirement on personal information and important data collected and generated by the operators of critical information infrastructure. All data must be stored within China, and a security assessment must be conducted before cross-border transfer of data. On a lesser scale, Australia and South Korea impose specific restrictions on transferring personal data cross-border in health and finance because it is sensitive. Malaysia and the Philippines have strict consent requirements and regulatory approvals for cross-border transfer of personal data.[105]

The Albright Stonebridge Group illustrated the spread of globalization in the following table, which highlights the spectrum of data localizations laws and regulations.[106]

---

[103] Chandler and Le argue that notwithstanding the arguments for data localization, it "increases the ability of governments to *surveil* and even oppress their own populations." *Id.* at 680. It is against this background that there has been in recent years a growing number of countries implementing data localization laws such as those now in force in Russia and China.

[104] On Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure of Personal Data Processing in Information-Telecommunications Networks, Russian Federal Law No. 242-FZ.

[105] Other countries that have data localization laws include: Switzerland, Turkey, Brazil, Vietnam, Brunei, Iran, India, Indonesia, and Nigeria.

[106] ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION 5 (2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf. We have added the U.S. to the table due to the Electronic Communications Privacy Act of 1984, 18 U.S.C. §§ 2510-23.

Data localization laws	Jurisdiction
Strong: Explicit requirements that data must be stored on servers within the country.	Brunei, China, Indonesia, Nigeria, Russia, Vietnam
Partial: Wide range of measures, including regulations applying only to certain domain names and regulations requiring the consent of an individual before data about them is transferred internationally.	Belarus, India, Kazakhstan, Malaysia, South Korea
Mild: Restrictions on international data transfers under certain conditions.	Argentina, Brazil, Colombia, Peru, Uruguay
Sector-specific: Tailored to specific sectors, including healthcare, telecom, finance, and national security.	Australia, Canada, New Zealand, Taiwan, Turkey, Venezuela, United States
None: No known data localization laws.	Remaining Countries

Despite the asserted advantages of data localization laws, they may not be an unmitigated good. Proponents of free trade argue that data localization laws are a barrier to companies seeking to expand physical facilities or sell to consumers through the internet. The laws limit the flow of data and increase the compliance costs of doing business. While larger international businesses may more easily assimilate the costs, the costs for smaller- to medium-sized businesses and businesses from less developed economies are barriers to trade. In litigation and regulatory investigations, the cost of cross-border processing and transfer of personal data between jurisdictions will also increase. The higher cost of doing business must be reflected either in higher prices for consumers or in fewer goods or services being made available to them.

As the Albright Stonebridge Group 2015 report states:[107]

> "On a macro basis, studies indicate that data localization regulations can have damaging long-term consequences. Potential disruptions in information flows cause uncertainty among companies and lead to lower levels of foreign investment. In addition to its impact on businesses, localization tends to reduce services and increase prices for domestic consumers."

The Albright Stonebridge Group report also referred to the study by the European Centre for International Political Economy, which examined the overall impact of localization measures in seven jurisdictions—Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam—and found negative impacts on GDP and foreign investment. The 2014 study found that localization

[107] *Id.* at 7.

regulations cost EU citizens an estimated $193 billion per year, due in part to higher domestic prices, and that Vietnam's strict 2013 data localization requirement had reduced its GDP by 1.7 percent.[108]

Data localization laws will continue to be an issue for companies operating globally, faced with complying with different regulatory regimes and increased costs. Cohen, Hall and Wood conclude:[109]

> "As these data localization laws proliferate, the cost of doing business globally increases because complying enterprises must either open new data centers, change their network architecture, or use a local cloud vendor. Meanwhile, privacy and security suffer as companies are forced to store data in a way that is not the most efficient or effective.
>
> "Data localization laws are here to stay. As companies invest in compliance and governments without these laws see the short-term benefits that accrue to the localizing government in the form of increased access to data and a boost to the local economy, more nations may want to get in the localization game. Without coalitions or policies to combat data localization efforts, the struggle between global business and nationalistic interests will most likely amplify over the years ahead."

g. Transnational Coordination Regimes

i. EU GDPR

The GDPR, on one view, is a data localization law, because personal data can only be transferred to countries outside the EU or an international organization where an "adequate level" of protection is guaranteed (Article 44). Furthermore, Article 48 states that, "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may not be recognized or enforceable in any manner unless based on an international agreement, like a mutual legal assistance treaty in force between the requesting third (non-EU) country and the EU or a member state."

Transfers may take place to a third country or international organization where the EU Commission has decided that it ensures "an adequate level of protection" (Article 45(1)). The adequacy decisions under the EU Directive[110] remain in force under the GDPR, and those jurisdictions determined by

---

[108] Matthias Bauer Et Al., European Centre for International Political Economy, The Costs of Data Localisation: Friendly Fire on Economic Recovery (2014), https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf, referred to in Albright Stonebridge Group, *supra* note 95, at 7.

[109] Bret Cohen, Britanie Hall, & Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, ANTITRUST, Vol. 32 No. 1, Fall 2017, at 107.

[110] *See Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (last visited June 5, 2019).

the EU Commission to provide "an adequate level of protection" are: Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. (Japan was added in 2019.) There are ongoing adequacy talks with South Korea. Transfers to the U.S. are permitted pursuant to the Commission's July 2016 decision on the adequacy of the protection provided by the EU/U.S. Privacy Shield, but only for those companies that are Privacy Shield certified.[111]

Transfers are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable individual rights and effective legal remedies for the data subject are available (Article 46). Appropriate safeguards include:

- Approved binding corporate rules that enable transfers within a multinational group of companies (Article 47).[112]
- Standard data protection contractual clauses approved by the EU Commission.[113]
- Approved code of conduct under Article 40, and the recipient gives binding and enforceable commitments to apply appropriate safeguards.
- Approved certification mechanism under Article 42, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.

ii. Trans-Pacific Partnership

In March 2018, 11 countries—Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam—signed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CP-TPP). Although the U.S. was a party to the negotiations for the TPP-12, it withdrew from the agreement following the change of administration in 2017, and it is now called the TPP-11.

The TPP-11 sets out rules reflecting that the internet is an essential tool for those companies within the TPP-11 doing business in the global economy. The principles for digital free trade under the

---

[111] *See EU-US data transfers: How personal data transferred between the EU and US is protected*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en (last visited June 5, 2019).

[112] See *Binding Corporate Rules: Corporate rules for data transfers within multinational companies*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en (last visited June 5, 2019).

[113] *See Standard Contractual Clauses: Standard contractual clauses for data transfers between EU and non-EU countries*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (last visited June 5, 2019).

TPP-11 are that servers can be set up in any country, data can be transferred across borders, and source codes need not be disclosed.

For the first time in a trade agreement, TPP-11 countries guarantee the free flow of data across borders for service suppliers and investors as part of their business activity. Article 14.2 states, "The Parties recognize the economic growth and opportunities provided by electronic commerce and the importance of frameworks that promote consumer confidence in electronic commerce and of avoiding unnecessary barriers to its use and development."[114]

TPP-11 governments can maintain and amend regulations related to data flows but have undertaken to do so in a way that does not create barriers to trade. Article 14.11: Cross-Border Transfer of Information by Electronic Means states:

> 1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
>
> 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
>
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> > (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> >
> > (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.[115]

Data localization is prima facie banned under the TPP-11. TPP-11 countries have committed not to impose localization requirements on computing facilities; this aims to provide certainty to businesses as they look to optimize investment decisions. Article 14.13 provides:

> 1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

---

[114] *See* Trans-Pacific Partnership, Ch. 14: Electronic Commerce, https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf (last visited June 5, 2019).

[115] *See Id.*

> 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
>
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> (a)is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
>
> (b)does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.[116]

iii. APEC Cross-Border Privacy Rules

The APEC (Asia-Pacific Economic Cooperation) Cross-Border Privacy Rules **(**CBPR**)** system was developed to build consumer, business, and regulator trust in cross-border flows of personal information. APEC members who have joined include Canada, Japan, Mexico, the United States, South Korea, Singapore, Australia, and Chinese Taipei.

The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices must be assessed as compliant with the program requirements of the APEC CBPR System by an Accountability Agent (an independent APEC CBPR system recognized public- or private-sector entity) and be enforceable by law.

Principle 48 states:

> Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.[117]

Part IV of Section B sets out the framework for International Implementation and provides:

> IV. Cross-border transfers

---

[116] *See Id.*

[117] *See* Asia-Pacific Economic Cooperation, *APEC Privacy Framework (2015)*, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

> 69. A member economy should refrain from restricting cross-border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.
>
> 70. Any restrictions to cross-border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross-border transfer.
>
> V. Interoperability between privacy frameworks
>
> 71. Recognizing that personal information flows do not stop at regional boundaries, member economies should encourage and support the development of international arrangements that promote interoperability amongst privacy instruments that give practical effect to this Framework.
>
> 72. Improving the global interoperability of privacy frameworks can bring benefits in improved personal information flows, help ensure that privacy requirements are maintained when personal information flows beyond member economies and can simplify compliance for personal information controllers and processors. Global interoperability can also assist individuals to assert their privacy rights in a global environment and help authorities to improve cross-border privacy enforcement.[118]

While the CBPR system provides a regional multilateral cross-border transfer mechanism, it is a voluntary scheme with, so far, only eight countries participating out of the twenty-one APEC member countries. Furthermore, only the U.S. and Japan have appointed accountability agents to certify organizations as CBPR compliant. When the GDPR came into effect in May 2018, with its greater restrictions on cross-border transfers and stronger enforcement mechanisms, including severe penalties, it appeared that the future of CBPR could be bleak. However, the CBPR was explicitly included in the United States-Mexico-Canada Agreement, and it has been reported that there are several other countries interesting in joining the CBPR system.

---

[118] *See Id.* at 31.

iv. APEC, CBPR, and the United States-Mexico-Canada Agreement

The United States-Mexico-Canada Agreement (USMCA), which was agreed to in September 2018 and is still to be ratified, includes a digital trade chapter. The USMCA recognizes the CBPR as a valid mechanism to facilitate cross-border information transfers while protecting personal information.

It provides that "no [p]arty shall prohibit or restrict the cross-border transfer of information, including personal information . . . for the conduct of the business of a covered person."[119] Article 19.11.2 then provides restrictions may be imposed to achieve a "legitimate public policy objective" provided that it is not "arbitrary" or a "disguised restriction on trade," and it "does not impose restrictions on transfers greater than are necessary to achieve the objective."[120]

Article 19.8 deals with personal information protection and requires that the parties adopt or maintain a legal framework for the protection of personal information of the users of digital trade. In the development of the framework, the parties are required to "take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the Organisation for Economic Co-Operation and Development (OECD) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)."[121]

Article 19.8.6 states that, "[t]he Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information."[122] And, Article 19.14.1(b) provides that recognizing the global nature of digital trade, the parties shall endeavor to, among other things, "cooperate and maintain a dialogue on the promotion and development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes."[123]

h. Other developments – EU and Asia

In August 2017, the APEC Electronic-Commerce Steering Group's Data Privacy Subgroup (DPS) met with the European Commission to discuss issues related to personal data protection regimes and the facilitation of global data flows. A release following the meeting stated:

> "The DPS and the Commission exchanged information on the APEC Cross-Border Privacy Rules (CBPR) System and the EU's GDPR, which goes into effect in May

---

[119] *See* United States-Mexico-Canada Agreement, Ch. 19: Digital Trade, 19-6, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf (last visited June 5, 2019).

[120] *See Id.*

[121] *See Id.* at 19-4, 19-5.

[122] *See Id.* at 19-5.

[123] *See Id.* at 19-7.

> 2018, with the aim of exploring interoperability between the two systems. The Commission explained that the reform facilitates data flows by simplifying the use of existing transfer mechanisms and introducing new tools for transfer. The Commission also informed the DPS about ongoing work with Asia-Pacific countries on possible adequacy findings with a view to fostering regulatory convergence and facilitating trade, and expressed its interest in strengthening enforcement cooperation between data protection authorities in the APEC region and the EU."[124]

There is considerable focus within the Asia Pacific region on the ongoing implementation of the APEC CBPR system across the region. The announcement of the adequacy decision concerning Japan and the ongoing adequacy talks with South Korea in 2018, referred to above, highlight the continuing focus on the Asia Pacific region.

A further initiative took place in early in February 2018, when ninety experts and high-level government officials in the region met in Singapore at the Asian Legal Business Institute's Forum "Towards A Shared Legal Ecosystem for International Data Flows in Asia." This event was the first time in Asia that representatives from government, data protection regulators, industry, and the legal community representing 19 jurisdictions met to discuss how to achieve a common Asian framework to share and transfer information across international borders. The Asian Legal Business Institute (ABLI) stated:

> "The fragmented data privacy laws and data localisation requirements in Asia are considered one of the biggest stumbling blocks to the development of the digital economy and e-commerce and for pushing up the costs of doing business in the region. The Forum is part of ABLI's Data Privacy Project which aims to help address these challenges."[125]

It is clear that the GDPR has set an international benchmark for the protection of personal data, which is impacting new legislation in the Asian region. This includes India's Personal Data Protection Bill 2018,[126] which uses the GDPR as a model. It requires copies of Indian personal data be stored in India and puts in place similar restrictions to the GDPR for data transfers out of India.

---

[124] See *Data Privacy Subgroup Meeting with European Union*, ASIA-PACIFIC ECONOMIC COOPERATION, https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union (last visited June 5, 2019).

[125] *See Towards A Shared Legal Ecosystem for International Data Flows in Asia*, ASIAN BUSINESS LAW INSTITUTE, https://abli.asia/NEWS-EVENTS/Whats-New/ArticleType/ArticleView/ArticleID/52 (last visited June 5, 2019).

[126] See The Personal Data Protection Bill, 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.