CHAPTER 13

BIG DATA AND INTERNATIONAL PRIVACY CONCERNS: CONFLICT, HARMONIZATION, AND INTERNATIONAL DATA TRANSFERS

■ ■ ■

By Mark D. Johnson*

I. INTRODUCTION

Big Data can be likened to water: it flows along the path of least resistance. Even before the advent of "cloud computing," companies transferred their data—employee medical records, customer purchase histories, and the like—from country to country for processing, analyzing, storage and, at times, further transfer to third parties. These practices have only intensified as collection and processing technologies have matured and the uses of Big Data have multiplied. These developments are putting new and growing stresses on privacy regimes around the world.

According to the Obama administration, "Big Data" is the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data.[1] The statistics regarding Big Data are staggering—and only getting larger. In 2013, it is estimated that some 4 "zettabytes" of data were created from text messages, Internet searches, mobile phones, CCTV, GPS, emails, social media, etc.[2] More than 500 million photos are uploaded and shared every day, along with more than 200 hours of video every hour.[3]

In today's economy much of this data is then sent from country to country, often passing through third countries on its way, for review, analyzing, storage, and later access. Examples of uses of Big Data include:

- Cost control and reduction;

* Senior Attorney, Squire Patton Boggs (US) LLP, Washington, D.C. The author wishes to thank his colleague, Scott Bailey, for the idea for this chapter and for his continued support and assistance in completing it. Thanks also to Kumar Jayasuriya for this opportunity and his input and assistance.

1 Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, at 2 (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

2 *Id.* A "zettabyte" is 1,000 000,000,000,000,000,000 bytes, or units of information. *Id.*

3 *Id.*

- Risk identification and mitigation;
- Optimization of operations;
- Customer retention and service;
- New customer acquisition;
- Product or service innovation; and
- Workforce optimization.

Using the practice of international data transfers between U.S. and European entities as an illustration, this chapter discusses the differing—and, at times, conflicting—privacy regimes in the European Union and the United States. Several mechanisms have been created, such as the EU-U.S. Safe Harbor Framework, Standard Contractual Clauses, and Binding Corporate Rules in particular, to try to harmonize these differing privacy regimes. The chapter closes by examining how these harmonization efforts are coming under increased pressure in the face of Big Data.

II. EU AND U.S. PRIVACY REGIMES: COMMON BACKGROUND, DIFFERING IMPLEMENTATION

The EU and U.S. privacy frameworks are based on a common origin: the first rendition of a set of internally accepted privacy principles developed by the Organisation for Economic Cooperation and Development (OECD) in 1980. These first privacy principles have withstood the test of time well, and they still inform national privacy regimes around the world. While the European Union and the United States both look to the OECD privacy guidelines as their source, their particular privacy regimes differ in significant ways. In 1995, the European Union implemented its "Data Protection Directive"[4] as a "top-down" regulatory framework, which, in turn, was to be implemented by each Member State into its national laws. In the United States, conversely, privacy laws and regulations have developed more from the bottom up to address specific issues or industry sectors, often as a reaction to a perceived problem or abuse involving collected personal data. Opinions differ—often strongly—on which approach is better equipped to provide the requisite privacy protection.

A. OECD PRIVACY GUIDELINES

In response to the development of automatic data processing and growing international transfers of these data, OECD member countries

[4] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [hereinafter EU Data Protection Directive].

concluded that there was a need to establish a basic, common privacy framework: (1) to harmonize national privacy laws, while protecting fundamental human rights concerning the use and collection of personal data, and, at the same time; (2) prevent interruptions in the international flow of data, which have caused serious economic disruptions.[5] The OECD Privacy Guidelines include a set of eight "Basic Principles of National Application":[6]

- Collection Limitation Principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Data Quality Principle—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the [Purpose Specification Principle] except:

  a) with the consent of the data subject; or

  b) by the authority of law.

- Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

---

[5] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Information C(80)58/FINAL (1980), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelines ontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [hereinafter 1980 OECD Privacy Guidelines].

[6] *Id.*, Part Two: Basic Principles of National Application.

- Individual Participation Principle—Individuals should have the right:
  a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
  b) to have communicated to them, data relating to them
    i) within a reasonable time;
    ii) at a charge, if any, that is not excessive;
    iii) in a reasonable manner; and
    iv) in a form that is readily intelligible to them;
  c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
  d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
- Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.

In 2010, in recognition of 30 years of the creation of the Privacy Guidelines, OECD started an effort to update the guidelines, culminating in 2013's revised Guidelines.[7] Importantly, OECD maintained the eight Basic Principles, updated to reflect two themes: (1) the practical implementation of privacy protection through risk management; and (2) interoperability between national privacy frameworks and governments. In addition, OECD sought to acknowledge new developments for privacy: (1) national privacy strategies by governments; (2) privacy management programs within entities (governments, companies); and (3) data security breach notification to law enforcement and affected individuals.

Credit must be given to the drafters of the OECD Privacy Guidelines, as they recognized back in 1980 the growing prevalence and economic benefits of Big Data, well before this term was created. Given these factors, the OECD Privacy Guidelines seek to facilitate such transfers between OECD member countries that have embraced the guidelines: "Member

[7] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, as amended on July 11, 2013, by C(2013)79, *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [hereinafter 2013 OECD Privacy Guidelines]. For background information about the creation of the framework, updates to OECD privacy efforts, and a stable link to the most updated guidelines, see *OECD Work on Privacy*, oe.cd/privacy (last visited July 27, 2015).

countries should avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."[8] In the 2013 updates, OECD retained the emphasis in the Privacy Guidelines as first written on the benefits of international data transfers, but with new acknowledgement of the potential risks and the need for mitigation:

> Transborder flows of personal data, to Member countries or non-Member countries, present risks, which data controllers must address. Some data flows may require close attention because of the sensitivity of the data or because the receiving jurisdiction may lack either the willingness or capacity to enforce privacy safeguards[9]

B. EU DATA PROTECTION DIRECTIVE

While it is fair to say that the EU Data Protection Directive[10] looks to the OECD Privacy Guidelines, the EU Data Protection Directive significantly altered the data protection landscape, and not only in the European Union. Adopted in 1995, the EU Data Protection Directive established a comprehensive, prescriptive privacy protection framework for all EU Member States. The EU Data Protection Directive seeks to achieve three primary goals. First, personal privacy is considered a fundamental right of all persons, which the EU Data Protection Directive recognizes and was adopted to safeguard. Second, the EU Data Protection Directive recognizes that the transfer of personal information has positive economic benefits, for both individuals and companies, and that such information should "flow freely" from one EU Member State to another. Harmonizing privacy laws across the European Union would help realize these economic benefits. Third, the EU Data Protection Directive seeks to ensure, where individuals' personal information is collected and processed, that (a) there be a legitimate (*i.e.*, legal) basis for doing so, (b) the collection and processing is done so in a lawful manner, and (c) such collection and processing is minimized.[11]

Structurally, the EU Data Protection Directive sets forth the fundamental principles and goals for the protection of "personal data" for EU residents. Administratively, it requires each of the EU Member States to implement national privacy legislation consistent with the EU Data Protection Directive.[12] It also directs each EU Member State to create its

---

[8] 1980 OECD Privacy Guidelines, *supra* note 5, Part Three. Basic Principles of International Application: Free Flow and Legitimate Restrictions.

[9] 2013 OECD Privacy Guidelines, *supra* note 7, at 30.

[10] EU Data Protection Directive, *supra* note 4.

[11] *See id.*, art. 6.

[12] *Id.*, art. 4.

own Data Protection Authority (DPA),[13] an independent government agency responsible for implementing and enforcing that Member State's national privacy legislation.

Crucially, the EU Data Protection Directive seeks to address all forms of collection and processing of personal data, regardless of the identity of the collector or the purpose for which the information is collected and processed. To this end, the definition of "personal data" is broadly worded:

> Personal data shall mean any information relating to an identified or identifiable natural person.[14]

Under this standard, personal data can be information that identifies a natural person directly, such as the person's name, or indirectly by a combination of identifying data points that a person may hold, *i.e.*, physical address, email address, national ID number, and the like.

A subset of personal data is "sensitive data," which is personal data that reveals:

> racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.[15]

The EU Data Protection Directive imposes additional restrictions on the collection and processing of sensitive data.

Other key definitions in the EU Data Protection Directive[16] are:

- Data Subject: The natural individual whose Personal Data is collected and processed.
- Data Controller: The person or entity that determines the purposes and means of collection and processing of Personal Data.
- Data Processor: A person or entity that processes Personal Data on behalf of a Data Controller.

C. U.S. DATA PROTECTION

In contrast, privacy protection in the United States has evolved more organically and from a variety of sources, legal and otherwise: U.S. and state constitutions, federal and state legislation, governmental agency regulations and enforcement, federal and state case law, common-law principles (in particular contract and tort law), contracts, and privacy policies. To date, there is no comprehensive U.S. privacy law or obvious

---

[13] *Id.*, art. 28.

[14] *Id.*, art. 2.

[15] *Id.*, art. 8.

[16] *Id.*, art. 2.

consistency. For example, the U.S. Constitution does not mention privacy, although the Fourth Amendment's protection against unreasonable government searches and seizures is seen as directly affecting individuals' privacy interests, at least where governmental action is involved.[17] Conversely, the California Constitution specifically identifies privacy as a fundamental right for its citizens.[18]

U.S. privacy law has developed along an economic or industry sector-by-sector approach, with new protections often created in response to specific privacy violations. Covered sectors include government (federal and state), financial services, health care, child welfare (especially concerning Internet use), and telecommunications. A consequence of this framework is that one sector may be covered by multiple statutes and regulations, which may not be consistent among themselves. As further discussed below, the lack of an omnibus, comprehensive privacy framework is seen by some critics, particularly from Europe, as not providing an adequate level of protection to individuals, which has had significant consequences for the cross-border transfer of personal information between the European Union and the United States.

Despite this patchwork of privacy laws, there are some fundamental commonalities for privacy protection in the United States. There is general agreement among U.S. government and business interests that industry self-regulation is the most effective mechanism for ensuring adequate protection of individuals' personal information. The Federal Trade Commission (FTC), along with the U.S. Department of Commerce (DOC), has long advocated that industry groups develop sector-specific industry codes of conduct for their privacy practices.[19] The belief is that industry is best equipped to develop the most appropriate privacy guidelines and practices for specific business sectors and activities. That said, these industry self-regulatory models do not exist in a vacuum. The FTC and the DOC have worked with industry groups to help them develop their self-regulatory models, going so far as to offer the following possible privacy principles for specific industries, such as online behavioral advertising: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material

---

[17] *See, e.g.*, *Griswold v. Connecticut*, 381 U.S. 479 (1965) (finding a constitutional right of privacy logically implied by the First, Third, Fourth, and Fourteenth Amendments).

[18] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*" (emphasis added)).

[19] *See* Federal Trade Commission, *Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change* (2010), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

retroactive changes to privacy policies; and (4) affirmative express consent for the use of sensitive data.[20]

Moreover, these self-regulatory efforts are buttressed by the FTC's development and advocacy of a standard set of Fair Information Practice Principles (FIPPs) covering: Notice, Choice, Access, and Security.[21] The FIPPs are closely modeled on the OECD Privacy Guidelines, discussed above, and have been incorporated into many federal and state privacy laws addressing multiple business sectors.

Enforcement of U.S. privacy laws may take several forms. A privacy statute may provide for specific regulatory oversight and enforcement authority, possibly by federal and/or state governmental bodies. In addition, federal and/or state privacy statutes may also provide for a private cause of action for aggrieved individuals to seek redress. Industry organizations that have established self-regulatory mechanisms may also provide for enforcement within the terms of those self-regulatory frameworks.

Specific mention should be made of the FTC's enforcement authority. Although a privacy statute may specifically identify enforcement authority for the FTC, it is more interesting (and more prevalent) when the FTC enforces the "promises" a business makes in its privacy policies and notices. Under the FTC Act,[22] the FTC has broad authority to protect consumers against "deceptive" and/or "unfair" business practices.[23] A company's failure to live up to its promises vis-à-vis privacy may constitute an unfair and/or deceptive business practice. Examples of these types of FTC enforcement actions include: (1) promising to provide adequate security but failing to do so; (2) promising not to share personal information with third parties except under certain, identified circumstances, and then disclosing the information in contravention of that representation; and (3) using personal information in a manner different from what is described in the privacy policy or notice. In most instances, the FTC does not impose a monetary fine; it instead enters into a settlement with the company requiring the company to implement internal controls and education and training programs, and to undergo periodic third-party audits of its privacy practices. These settlements most often also include a continuing obligation—for as long as 20 years—to report back to the FTC on its privacy practices and its compliance with them. In recent years, data-rich

---

[20] *See* Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (2009), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[21] Federal Trade Commission, *FTC Privacy Online: A Report to Congress* (1998), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[22] Federal Trade Commission Act of 1914 (FTC Act), 15 U.S.C. §§ 41–58.

[23] 15 U.S.C. § 45(a) (FTC Act § 5).

companies, such as Google[24] and Facebook,[25] among others, have entered into settlements with the FTC over their privacy practices that incorporate these types of requirements.

Finally, while the majority of states also have enacted privacy laws, California and Massachusetts are seen as the leading two. As noted above, the California Constitution identifies privacy as a fundamental individual right.[26] California—as the location of many of the largest information technology, computing, and Internet companies—has taken the lead on many privacy issues, particularly concerning Internet, mobile, and location privacy.[27] Massachusetts has also enacted similarly comprehensive data-protection laws.[28]

Any company that operates in California, or has customers there, must comply with its data protection and privacy laws and regulations. Given the large size of its population and economy, California's privacy requirements are effectively the *de facto* or baseline standard for compliance for many business sectors. 47 states, including California and Massachusetts, as well as the District of Columbia and Puerto Rico, have passed data breach notification laws. To date, however, there is no federal data breach notification law.[29]

III. INTERNATIONAL DATA TRANSFERS: CONFLICT AND HARMONIZATION

The implementation of the EU Data Protection Directive in 1995 set off a conflict with the United States regarding the international transfer of personal information from the European Union to the United States. Another key provision in the EU Data Protection Directive (Art. 25) specifically prohibits international transfers of personal information of EU residents to non-EU Member States deemed not to ensure "an adequate level of protection."[30] In other words, when a third country's laws, and in consideration of other indicators, are found not to provide a level of privacy protection equal to or greater than the EU Data Protection Directive, EU

---

[24] *See* Press Release, Federal Trade Commission, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[25] *See* Press Release, Federal Trade Commission, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.

[26] *Supra* note 18.

[27] *See generally* State of California Department of Justice, Office of Attorney General, Privacy Enforcement and Protection, http://oag.ca.gov/privacy (last visited July 27, 2015).

[28] *See, e.g.*, 201 MASS. CODE REGS. 17.00 (Standards for the Protection of Personal Information of Residents of the Commonwealth).

[29] David Bender, *Summary of Breach Notification Statutes*, BENDER ON PRIVACY AND DATA PROTECTION § 22App.01 (2011).

[30] EU Data Protection Directive, *supra* note 4, at art. 28.

Member States must take steps to prevent any such international transfers.

For an international company, prohibiting data transfers could have a devastating effect, both in terms of internal management of its own employees and also in identifying and servicing customers around the world. Recent developments, in which data is transferred, processed and/or stored by third-party "cloud computing" services, evidence greater reliance on the unfettered transfer of information from country to country, often passing through one or more third countries en route. Artificial barriers to international data transfers create risks of "stove piping" data-management services and potentially "walling off" a national or regional economy, with negative economic impacts to local businesses and residents. To date, only a handful of countries have been found by the European Union to have "adequate" privacy protections, including Argentina, Canada, Guernsey, the Isle of Man, Israel, New Zealand, Switzerland, and Uruguay.[31]

A. EU/U.S. SAFE HARBOR FRAMEWORK

The current EU/U.S. safe harbor framework is a response to the 1999 finding by the European Commission[32] that the United States' data-protection laws do not ensure an adequate level of privacy protection.[33] The result of this determination was to prohibit the transfer of personal information of EU residents to the United States for processing. In response, the U.S. DOC and the European Commission entered into negotiations to develop a mechanism that would enable U.S. entities to satisfy the "adequacy" requirement of the EU Data Protection Directive, thus enabling the continued transfers of personal information to the United States. After two years of negotiation, an agreement was reached in July 2000 on a set of "Safe Harbor" principles and a framework to govern these data transfers. By self-certifying its adherence to the Safe Harbor Principles, a U.S. entity represents that it will provide "adequate" privacy protections to personal information of EU residents that is transferred to the United States.

---

[31] An updated list may be found at European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated June 30, 2015).

[32] The European Commission is the EU's executive body. *See generally* European Commission, *About the European Commission,* http://ec.europa.eu/about/index_en.htm (last updated June 1, 2015).

[33] *See* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government, 5092/98/EN/final (Jan. 26, 1999), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp15en.pdf.

The seven Safe Harbor Principles,[34] summarized below, are similar to the OECD Privacy Guidelines discussed above:

- Notice—Organizations must notify individuals about the purposes for which they collect and use information about them.
- Choice—Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt-in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.
- Onward Transfers (Transfers to Third Parties)—To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Principles or is subject to the [EU Data Protection] Directive or another adequacy finding.
- Access—Individuals must have access to personal information about themselves that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
- Security—Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- Data Integrity—Personal information must be relevant for the purposes for which it is to be used.
- Enforcement—In order to ensure compliance with the Safe Harbor Principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and

[34] U.S. Department of Commerce, *The U.S-EU Safe Harbor Framework A Guide to Self-Certification*, at 4–6 (updated Mar. 2013), *available at* http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf. This publication is part of an online resource jointly managed by multiple federal agencies, including the U.S. Department of Commerce. *See Export.gov Helps American Companies Succeed Globally*, http://www.export.gov/about/ (last updated Oct. 13, 2009).

> resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies made to adhere to the Safe Harbor Principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles.

According to the DOC, the benefits to U.S. companies participating in the Safe Harbor Framework, and to their EU partners, are several. Companies participating in the Safe Harbor Framework are deemed to provide "adequate" privacy protections, and the international data transfers from the European Union to the United States can continue unabated. The Safe Harbor Framework binds all 27 EU Member States to the European Union's finding that the framework satisfies the EU Data Protection Directive's "adequacy" requirement. Accordingly, companies can avoid the cost and effort of trying to comply with potentially 27 different privacy regimes, and perhaps finding that compliance with one results in a conflict with another. In addition, any Member State's requirements for prior approval for data transfers are waived, or approval is automatically granted. Except personal information of employees of the participating company in the European Union, claims regarding a company's practices under the Safe Harbor Framework are to be adjudicated in the United States, not in the European Union.[35]

However, there are certain limits to the Safe Harbor Framework. Most significantly, the framework does not cover all business sectors. To date, the FTC and the U.S. Department of Transportation are the only U.S. governmental agencies that have signed on to the framework. Only those U.S. companies subject to the jurisdiction of these two agencies can participate. Because the financial services and telecommunications industries are not regulated by either agency, they are not included in the Safe Harbor Framework. Nonetheless, to date some 3,500 U.S. companies have self-certified to participate in the Safe Harbor Framework.[36]

B. OTHER INTERNATIONAL TRANSFER MECHANISMS

The Safe Harbor Framework is not the only accepted mechanism for facilitating international transfers of personal information from the European Union to any country it deems not to provide "adequate" privacy protection. Two other mechanisms—Standard Contractual Clauses and Binding Corporate Rules—are also accepted under the EU Data Protection Directive.

---

[35] *Id.* at 3.

[36] *See U.S.-EU Safe Harbor List*, https://safeharbor.export.gov/list.aspx (last visited July 27, 2015).

1. Standard Contractual Clauses

Article 26(2) of the EU Data Protection Directive provides that a data controller in the European Union can use "appropriate" Standard Contractual Clauses to enable international transfers of personal information to third countries lacking "adequate" privacy protections. To date, the European Commission has issued two separate sets of Standard Contractual Clauses for international transfers, one set for transfers from one data controller to another, and a second set from a data controller to a data processor.[37] The clauses can be used as a stand-alone document or incorporated into commercial agreements. As they have been approved by the European Commission, the language of the Standard Contractual Clauses is non-negotiable; if changed, then the DPAs will not automatically accept that the clauses provide adequate protection of personal information. In addition, the European Commission has implemented several Appendices that require particular language, identify mandatory "principles"[38] for data processing, and impose several administrative requirements on the contracting parties, before they enter into the agreement, as well as continuing obligations. Finally, the Standard Contractual Clauses are not limited only to international transfers from the European Union to the United States, but can also apply to transfers to other countries similarly found not to have adequate privacy protections.

2. Binding Corporate Rules

A third commonly used mechanism for international transfers is "Binding Corporate Rules" (BCRs). BCRs are a set of agreements or rules adopted by a single entity (such as a large, multinational corporation) and its affiliates regarding how the organization, collectively, will process personal information, whether about its own employees or customers. BCRs apply where the organization and its affiliates are data controllers. BCRs need to be detailed and comprehensive, addressing the full scope of an organization's privacy policies and practices, such as:

- Privacy policies;
- Employee training and guidance;
- Privacy audit programs;
- Complaint receipt and processing;
- Entities covered;

---

[37] The European Commission maintains a website to track the development of Standard contractual clauses, European Commission, *Model Contracts for the Transfer of Personal Data to Third Countries*, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (last updated June 30, 2015).

[38] Indeed, the Standard Contractual Clauses principles also track the OECD Privacy Guidelines: Purpose Limitation; Data Quality and Proportionality; Transparency; Security and Confidentiality.

- Security policies;
- Data processing review; and
- Privacy organization.

It is not sufficient that the organization draft a set of BCRs and get each of its affiliates to sign on. The set of BCRs must also be approved by the DPA in each of the EU Member States in which the organization or its affiliates operate. Once approved by a DPA, however, the set of BCRs provides legal protection for its privacy practices—in other words, the organization meets the EU Data Protection Directive's "adequacy" standard.

Initially, individual Member State DPAs viewed BCRs with disfavor. More recently, however, DPAs have been more accepting and have implemented more formal processes to review and approve BCRs. In addition, some DPAs have begun using a "mutual recognition" process for the review of BCRs, whereby one DPA takes the lead on reviewing a proposed set of BCRs, and other DPAs subsequently recognize the BCRs as approved by the lead DPA. While BCRs can cover multiple-country international data transfers, they are currently limited to international transfers to countries without "adequate" privacy protection among affiliates within the same organization.[39]

3. Derivative Safe Harbor Model: APEC Cross Border Privacy Rules

The United States is a member of the Asia-Pacific Economic Cooperation (APEC),[40] an organization devoted in part to creating a platform for voluntary cross-border data transfer. In November 2011, the United States and representatives from the other 21 APEC nations signed a new protocol for international data transfers among the member economies. The Cross Border Privacy Rules (CBPR)[41] seek to enable global entities to transfer information among APEC member economies, thus enhancing economic activity while also sufficiently protecting individuals' personal information.[42] In many ways, the CBPR is similar to the Safe

---

[39] The European Commission maintains a website with current information about BCRs, European Commission, Overview on Binding Corporate Rules, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (last updated June 30, 2015).

[40] There are 22 APEC member economies: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the United States, and Vietnam. http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (last visited July 27, 2015).

[41] APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx (last visited July 27, 2015) [hereinafter CBPR Policies and Rules].

[42] Like other privacy programs, the CBPR is based on a set of privacy principles ("APEC Information Privacy Principles") drawn directly from the OECD Privacy Guidelines: (1) Preventing Harm; (2) Notice; (3) Collection Limitations; (4) Uses of Personal Information; (5) Choice;

Harbor Framework, discussed above, in that the program relies on participating organizations' self-assessment of their privacy policies and practices. However, the CBPR includes a somewhat more rigorous review and enforcement of an applicant's privacy practices to qualify for participation in the program. The United States formally joined the CBPR in June 2012 and named the FTC as its Privacy Enforcement Authority for the program. To date, the United States, Canada, Japan, and Mexico are the only APEC member economies approved to participate in the program.[43]

The CBPR consists of four elements:[44]

(1) Self-Assessment—An organization seeking to participate in the CBPR develops and implements privacy policies and practices that are consistent with the program requirements. In addition, applicants complete and submit a program questionnaire, and any supporting documents, to an approved "Accountability Agent" for review against the CBPR requirements. Governmental and/or private organizations can be recognized as Accountability Agents for a specific member economy. In the United States, TRUSTe, an independent privacy advisor, was named in June 2013 as the first Accountability Agent in the program.[45] Shortly thereafter, in August 2013, IBM obtained the first CBPR certification as a participating organization, for which TRUSTe was the Accountability Agent.[46]

(2) Compliance Review—An Accountability Agent conducts a confidential review of an applicant's privacy policies and practices, and its program questionnaire, to confirm they are consistent with the CBPR program's standards and requirements. These standards and requirements are intended to establish a minimum baseline for privacy protection and

(6) Integrity of Personal Information; (7) Security Safeguards; (8) Access and Correction; and (9) Accountability. The APEC Information Privacy Principles are at the core of the APEC Privacy Framework, endorsed by 21 APEC member economies in November 2004. APEC PRIVACY FRAMEWORK (2005), *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx. The CBPR resulted from a call in the APEC Privacy Framework to develop a system of voluntary cross-border transfer rules for the APEC region.

[43] For an updated list of participating states see *CBPRs Cross Border Privacy Rules System: For Governments*, http://www.cbprs.org/Government/GovernmentDetails.aspx (last visited July 27, 2015).

[44] CBPR Polices and Rules, *supra* note 41, at 4–6.

[45] To date, TRUSTe remains the sole Accountability Agent in the program, recognized in June 2013 for the United States. *See CBPRs Cross Border Privacy Rules System: For Accountability Agents*, http://www.cbprs.org/Agents/AgentDetails.aspx (last visited July 27, 2015).

[46] In addition to IBM, ten other companies have obtained CBPR certification in the United States as of April 2015: Merck, Workday, Lynda.com, Yodlee, Ziff Davis, Rimini Street, JELD-WEN, Box, Hewlett Packard, and Apple. See an updated list at CBPRs Cross Border Privacy Rules System: For Consumers, http://www.cbprs.org/Consumers/ConsumerDetails.aspx (last visited July 27, 2015).

compliance that organizations should satisfy. An Accountability Agent's assessment can exceed the CBPR baseline standards.

(3) Recognition/Acceptance—Participating APEC member economies are to establish a publicly available directory of the organizations that have been certified as CBPR-compliant by an Accountability Agent. The organization's listing is also to include a contact for the Accountability Agent that certified the organization and the relevant Privacy Enforcement Authority for questions or complaints.

(4) Enforcement—The CBPR contemplates that Accountability Agents will be able to enforce the CBPR program requirements through law or contract. In addition, Privacy Enforcement Authorities have the ability to enforce CBPR requirements under applicable domestic laws or regulations. Accordingly, the FTC presumably would enforce an organization's CBPR commitments and representations in the same manner as it does for the Safe Harbor Framework under Section 5 of the FTC Act.[47] Within APEC, member economies' national Privacy Enforcement Authorities also participate in the Cross-Border Enforcement Arrangement, a multi-national advisory group created to promote information and sharing on privacy investigations and enforcement activities under the CBPR.[48]

IV. NEW PRESSURES AND NEW CONFLICTS FOR INTERNATIONAL DATA TRANSFERS

The EU Data Protection Directive was implemented in 1995. The Safe Harbor Framework was established in 2000. Much has happened since then: the worldwide proliferation of the Internet, ubiquitous use of smartphones and other mobile devices, and the development of worldwide cloud computing services, to name a few. These developments, coupled with the 2013 revelations by Edward Snowden that the U.S. National Security Agency (NSA) had been collecting the metadata of millions of mobile devices,[49] among other activities, have created new pressures and conflicts associated with international transfers of personal information.[50]

---

[47] 15 U.S.C. § 45(a).

[48] *See APEC Cross-Border Privacy Enforcement Arrangement*, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (last visited July 27, 2015).

[49] *See* Barton Gellman et al., *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST, June 9, 2013, *available at* http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

[50] *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST, Aug. 15, 2013, *available at* http://wapo.st/1cR57dW; *see also* Glenn Greenwald, *UN Report Finds Mass Surveillance Violates International Treaties and Privacy Rights*, INTERCEPT, Oct. 15, 2014, *available at* http://interc.pt/1w6UrOT (discussing UN Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/69/397, issued Sept. 24, 2014).

A. CLOUD COMPUTING

Cloud computing is the enabler of Big Data, but what is meant by the term? In short, cloud computing involves remote access to software, storage capacity, and other sources that are available on demand as needed. More formally, the National Institute of Standards and Technology of the U.S. DOC gives the following description:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[51]

The emergence of cloud computing services is a result of three technical advances. The first advance is found in Moore's Law: the number of transistors on a computer chip will double every year.[52] Accordingly, current processing power is thousands of times faster than that of the earliest chips, using fractions of the power and at greatly reduced costs. Second, it is possible to store vast amounts of data at increasingly lower costs. Finally, the current speed of data transmissions, and the development of a worldwide infrastructure of submarine cables and satellites available to users and backbone providers make it possible to send data around the world virtually instantaneously and access the data remotely. Users of cloud computing services generally seek access to large data storage capabilities and remote access to that storage, as well as software and other applications as needed. Worldwide spending on cloud IT infrastructure is predicted to top $33 billion in 2015.[53]

There are three general categories of cloud services:

- Infrastructure—A cloud service provider makes available a complete cloud infrastructure—network, storage, operating systems, transmission—to its customer for a fee. While the customer has no control over or management of the infrastructure, it can deploy and run software and other applications, with ready access to flexible amounts of storage and processing capacity when needed.

---

[51] Peter Mell & Timothy Grance, National Institute of Standards and Technology, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (Special Publication 800–145), at 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[52] Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 38 ELECTRONICS 114 (Apr. 19, 1965); *see also* Chris A. Mack, *Fifty Years of Moore's Law*, 24 IEEE TRANSACTIONS ON SEMICONDUCTOR MANUFACTURING 202 (2011).

[53] Press Release, International Data Corporation, Worldwide Cloud IT Infrastructure Spending Forecast to Grow 26% Year Over Year in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC, July 6, 2015, *available at* http://www.idc.com/getdoc.jsp?containerId=prUS25732415.

- Platform—The customer deploys its own applications, data and tools on a cloud infrastructure controlled and managed by a third party. Again, the customer does not control the underlying infrastructure, but has control over the deployed applications and other elements.
- Software—The customer accesses software running on the cloud infrastructure rather than on the customer's own hardware (*i.e.*, its own servers and/or individual computers). Access to the software is available on multiple devices (PCs, tablets, smartphones, etc.) through a common interface, such as a Web browser.

In addition, there are three common deployment models for cloud computing:

- Public Cloud—An open cloud infrastructure that is available for public use. Individuals accessing email, social media, and online storage are doing so via a public cloud service. Amazon, IBM, and Microsoft are some of the leading providers of public clouds.
- Private Cloud—A large business or government will have access to a proprietary cloud service for its own internal use. The cloud infrastructure may be hosted and managed by the entity itself or by a third party under contract.
- Community Cloud—A limited group of clients or users may establish a dedicated cloud infrastructure for their own use. They may either host and manage the infrastructure themselves or contract with a third-party cloud provider.

The legal concerns surrounding cloud computing services have come largely from EU Member States. Their concerns center on the "extraterritorial" status of cloud infrastructures and their providers. Cloud providers have established storage facilities and network operating centers throughout the world, and customer data can be transmitted within this infrastructure without regard to international borders—and without regard to country-specific laws and jurisdiction. Questions have been raised as to what country's (or countries') laws would apply to a cloud infrastructure and how to make that determination. Home country of the cloud provider? Home country of the cloud customer? Source country or countries of the data? Location of the servers that store the data? Can the customer dictate where its data is to be stored—or not stored—to try to choose the applicable jurisdiction? When the data includes personal information, these questions are all the more relevant.

These issues came to a head, for example, in an August 2014 decision by a U.S. federal district court upholding a warrant in a drug investigation

requiring Microsoft to turn over its customers' "MSN.com" Web-based emails stored in the company's servers located in Ireland, an EU country.[54] Other U.S. technology and communications companies, including AT&T, Cisco, and Verizon, submitted briefs to the court in support of Microsoft, evidencing the concern that they might lose millions of dollars in business to foreign competitors if customers fear that their data can be seized by U.S. law enforcement regardless of where it is stored, including outside the United States.[55] Relatedly, the Information Technology and Innovation Foundation estimated in August 2013 that U.S. cloud computing providers could lose between 22 and 35 billion dollars in 2014–2016 as a result of the Snowden revelations.[56]

German Chancellor Angela Merkel has commented that the European Union should construct a separate cloud infrastructure, based completely in Europe, partly to avoid having the data automatically pass through the United States.[57] She went on to explain that U.S. companies, such as Google and Facebook, can be located in countries with less data protection while conducting business—and collecting personal information—in countries that provide greater privacy protection. By establishing a European cloud infrastructure, it is thought, there would be more confidence that EU privacy protections would be applied to personal information about EU citizens.

In addition, the Snowden disclosures have the potential to put U.S. cloud providers at a competitive disadvantage vis-à-vis non-U.S. providers. Non-U.S. providers can argue that, by providing cloud services that do not touch the United States, they would not be subject to NSA intelligence-gathering. Customer mistrust of U.S. government activities could lead to mistrust of U.S. cloud providers and a resulting loss in business. For example, a recent analyst projected that U.S. cloud providers could lose as much as 20 percent market share for the provisioning of cloud services internationally, leaving non-U.S. providers to pick up this share.[58] Cognizant of these concerns, major U.S. cloud providers have sought to

---

[54] Bob Van Voris, *Microsoft Fails to Block U.S. Warrant for Ireland E-mail*, BLOOMBERG, July 31, 2014, *available at* http://www.bloomberg.com/news/2014-07-31/microsoft-fails-to-block-u-s-warrant-for-ireland-e-mail.html. Microsoft is appealing the decision.

[55] *Microsoft Must Surrender Overseas Data*, US Judge Rules, TELEGRAPH, Aug. 1, 2014, *available at* http://www.telegraph.co.uk/technology/microsoft/11005604/Microsoft-must-surrender-overseas-data-US-judge-rules.html.

[56] Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?*, INFO. TECH. & INNOVATION FOUND., Aug. 5, 2013, *available at* http://www.itif.org/publications/2013/08/05/how-much-will-prism-cost-us-cloud-computing-industry.

[57] Expatjourno, *Angela Merkel Hits the US Where It Hurts*, DAILYKOS, Feb. 15, 2014, *available at* http://www.dailykos.com/story/2014/02/15/1277859/-Angela–Merkel-hits-the-U-S-Government-where-it-counts.

[58] Matthew Schofield, *US Share of Cloud Computing Likely to Drop After NSA Revelations*, MCCLATCHY DC, Feb. 12, 2014, http://www.mcclatchydc.com/2014/02/12/217738/us-share-of-cloud-computing-likely.html.

establish or expand their European-based data centers. For example, in October 2014, Amazon announced a new data center in Germany that presumably would enable Amazon to address data sovereignty concerns by maintaining German-client data in Germany.[59]

Similarly, developers of new transoceanic fiber-optic cable networks are now considering constructing these networks to avoid landing in the United States. For example, most existing networks between Latin America and Europe run through the United States, thus making them subject to U.S. jurisdiction and NSA intelligence-gathering. Developers of new networks between Latin America and Europe are instead looking for direct routes that, while more costly, would bypass the United States completely and avoid the reach of U.S. laws and government.[60]

B. GROWING DOUBTS SURROUNDING SAFE HARBOR FRAMEWORK

The Snowden revelations have also fueled renewed criticism of the Safe Harbor Framework. Even before Snowden, critics in the European Union raised several concerns regarding the Safe Harbor Framework, particularly regarding the U.S. side of the program. For example, EU DPAs have believed that there is lax oversight and enforcement in the United States, particularly by the FTC. For example, as early as 2008, there have been allegations that participating U.S. companies falsify Safe Harbor self-certification for certain types of data or other qualifications when they do not have such self-certification.[61]

More recently, in August 2014, the Center for Digital Democracy (CDD) took matters even further by filing a formal complaint and research study with the FTC alleging that 30 companies involved in data profiling and online targeting of individuals are using the EU-U.S. Safe Harbor Framework as a "shield" regarding data practices that put at risk the personal information of millions of Europeans. The complaint states:

> The Big Data-driven companies in our complaint use Safe Harbor as a shield to further their information-gathering practices

---

[59] Jason Verge, *AWS Adds Second European Cloud Region in Germany*, DATA CENTER KNOWLEDGE, Oct. 23, 2014, http://www.datacenterknowledge.com/archives/2014/10/23/aws-launches-cloud-data-center-in-germany/.

[60] Robin Emmott, *Brazil, Europe Plan Undersea Cable to Skirt U.S. Spying*, REUTERS.COM, Feb. 14, 2014, http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224.

[61] *See generally* Chris Connolly, *The US Safe Harbor—Fact or Fiction?*, GALEXIA (2008), *available at* http://www.galexia.com/public/research/articles/research_articles-pa08.html. Galexia has continued to raise these same concerns regarding the EU/U.S. Safe Harbor Framework. In October 2013, Chris Connolly of Galexia stated in testimony before the European Parliament that 475 U.S. companies make false claims regarding their participation in the program. *Hundreds of US Companies Lie About Safe Harbor Conformance*, INFOSECURITY MAG., Oct. 10, 2013, *available at* http://www.infosecurity-magazine.com/news/hundreds-of-us-companies-lie-about-safe-harbor/ [hereinafter Galexia Testimony].

> without serious scrutiny. Companies are relying on exceedingly brief, vague, or obtuse descriptions of their data collection practices, even though Safe Harbor requires meaningful transparency and candor. Our investigation found that many of the companies are involved with a web of powerful multiple data broker partners who, unknown to the EU public, pool their data on individuals so they can be profiled and targeted online.[62]

In the complaint, the CDD asked the FTC to investigate 30 companies the CDD claims are violating their Safe Harbor self-certifications.

In fact, the German DPA imposes additional requirements on the German data exporter and its U.S. counterpart to use the Safe Harbor Framework for transmitting personal information of German residents.[63] For the German data exporter:

- Obtain evidence showing how the U.S. company fulfills its obligations under the Safe Harbor Framework; and
- Be able to prove this check upon request by the data protection authorities.

For the U.S. company, it first should declare that they provide the following information to the data subject:

- How individuals can contact the organization with any inquiries or complaints;
- The types of third parties to which it discloses the information; and
- The choices and means the organization offers for limiting its use and disclosure.

Moreover, the German DPA requires that the U.S. company inform the data subject about the processing:

- Prior to processing;
- In a clear and unambiguous form to data subjects; and
- Before it transfers data to a third party for a third time.

Then, in July 2013, after the Snowden revelations, German DPAs said that they would no longer issue any new permissions for data transfers to the

---

[62] Press Release, Center for Digital Democracy, CDD Files Complaint on U.S./EU Safe Harbor for Data Privacy at FTC/Filing Reveals Failure of U.S. Agreement to Protect European Privacy (Aug. 14, 2014), *available at* http://www.democraticmedia.org/content/cdd-files-complaint-useu-safe-harbor-data-privacy-ftc-filing-reveals-failure-us-agreement. The complaint and report are also available. *Id.*

[63] It is worth noting that a claimed benefit of the EU Directive was to harmonize privacy into a single, common regime for all EU Member States. However, the imposition of these additional requirements for the Safe Harbor Framework by the German DPA belies any claim that such harmonization has been obtained.

United States, and that they would examine whether such data transfers should be suspended under the Safe Harbor Framework and EU Model Clauses.[64] Despite these statements, however, international data transfers to the United States pursuant to the Safe Harbor Framework and the EU Model Clauses remain valid under EU law, which is binding on the German DPA.

Efforts in the European Union have continued questioning the efficacy of the Safe Harbor Framework and addressing the more general issue of international data transfers to the United States. For example, in October 2013 the EU Parliament Committee on Civil Liberties, Justice and Home Affairs (CLJHA Committee) adopted a set of recommended amendments to the EU Data Protection Directive, including addressing international data transfers.[65] The CLJHA Committee advocated that companies be required to seek permission from EU Member State DPAs prior to any international data transfer. Moreover, the CLJHA Committee proposed increased sanctions for violations of up to 100 million Euros, or 5 percent of a company's annual worldwide revenue, whichever is greater.[66]

In November 2013, the European Commission issued a sort of "white paper" in which it provided a critique and recommendations regarding the Safe Harbor Framework: "Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU."[67] The European Commission's most significant criticisms of the Safe Harbor Framework centered on transparency, onward transfers of data, alternative dispute resolution, enforcement, and access to data by U.S. governmental authorities. On transparency, the European Commission criticizes self-certified companies under the framework should not only make publicly available their privacy policies, but also publish conditions of any contracts with subcontracts for onward transfers. When a company enters into a contract to transfer data to a third party for

---

[64] Press Release, German Conference of Data Protection Commissioners of the Federation and the States, Conference of Data Protection Commissioners Says that Intelligent Services Constitute a Massive Threat to Data Traffic Between Germany and Countries Outside Europe (July 24, 2013), *available at* https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9285.de.

[65] Committee on Civil Liberties, Justice and Home Affairs, European Parliament, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, (COM(2012)0011—C7 0025/2012—2012/0011(COD)), Oct. 7, 2013, *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf (calling for compromise amendments on Articles 1–29).

[66] Press Release, European Commission, LIBE Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[67] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

processing, such as to a cloud service provider, the company should notify the U.S. DOC of the contract and also should be prepared to make public the attendant privacy safeguards.

The white paper also criticizes the current Safe Harbor Framework requirement that participating companies must identify an alternative dispute resolution process for individuals to bring claims regarding the mistreatment of their personal data. The European Commission expresses a concern that some of these programs are unreasonably expensive. For example, Galexia reports that the American Arbitration Association charges a complainant between $120 and $1,200 an hour (with a four-hour minimum), as well as a $950 administration fee.[68] In contrast, there is no cost to EU citizens to bring a Safe Harbor complaint before the EU's Data Protection Panel.

The European Commission's white paper also expressed significant concern about the enforcement efforts in the United States, specifically by the FTC, regarding the Safe Harbor Framework. Several specific criticisms and recommendations are proposed. First, the European Commission calls for there to be a more robust review of participating companies' adherence to program requirements after initial certification or annual recertification beyond just confirming adherence to the program's formal requirements. The FTC should subject a selection of companies to *ex officio* investigations of their compliance. Second, where noncompliance is found, the company should be subject to a follow-up investigation one year later. Third, where there are doubts regarding a company's compliance, the U.S. Department of Transportation should inform the competent EU DPA. Fourth, the document calls for the continued investigation of false claims of Safe Harbor compliance. Finally, the European Commission notes that, while the FTC has primary enforcement over the Safe Harbor Program, U.S. telecommunications companies are not subject to FTC jurisdiction and, therefore, cannot participate in the program. This situation creates an unfair competitive disadvantage for European telecommunications companies, which must comply with stricter data protection and transfer requirements.

Additionally, the European Commission expresses its growing concern over the ability of U.S. governmental authorities to access personal data collected by U.S. companies, including those participating in the Safe Harbor Program. Accordingly, the European Commission recommends that participating companies describe in their privacy policies the extent to which U.S. law allows governmental authorities to collect and process data protected under the Safe Harbor framework. In addition the European Commission asks that each company develop policies and procedures for when the companies will apply exceptions to the Safe Harbor Privacy

[68] Galexia Testimony, *supra* note 61.

Principles to meet national security, public interest, or law enforcement requirements.

A more recent controversy is known as "data localization." EU Member States have raised the issue through legislation intended to ensure that personal information collected about an EU citizen would stay in that country. For example, in May 2015, the German government passed a draft law that, among other provisions, would require telecommunications and Internet service providers to ensure that personal information they collect about German citizens be stored in Germany.[69] (An earlier version of the law was found to have violated the German Constitution but on other grounds.[70]) It remains to be seen how any such national data localization requirements would interact with the Safe Harbor Framework.

A separate development involves a lawsuit pending before the Court of Justice of the European Union (CJEU) that directly attacks the Safe Harbor Framework. An Austrian citizen, Max Schrems, brought a complaint against Facebook before the Irish Data Protection Commission (IDPC).[71] Schrems argued, that Facebook's transfers of personal information to the United States pursuant to the Safe Harbor Framework no longer satisfied the EU's "adequacy" requirement because U.S. authorities had access to the data, as detailed by the Snowden disclosures.[72] The IDPC rejected the complaint because the European Commission had previously determined that the Safe Harbor Framework satisfied the adequacy requirement, and the Irish Data Protection Commission did not have the authority to challenge this conclusion.[73] Schrems then sought review of this decision before the CJEU. At this time, the CJEU decision is pending. It is unclear whether the CJEU would directly address the adequacy of the Safe Harbor Framework or otherwise determine whether the DPAs of each Member State are still bound by the European Commission's finding in 2000 that the Safe Harbor Framework is adequate.

Regarding U.S. enforcement, the FTC announced in January 2014 that it had reached settlements with 12 companies regarding false claims of Safe Harbor compliance. According to the FTC's statement,[74] the

---

[69] *Germany Adopts a Telecom Data Retention Law that Includes a Localization Requirement*, Hunton & Williams, PRIVACY & INFO. SECURITY L. BLOG, June 4, 2015, *available at* https://www.huntonprivacyblog.com/2015/06/04/germany-adopts-telecom-data-retention-law-includes-localization-requirement/.

[70] *Id.*

[71] The IDPC had jurisdiction because Facebook's European headquarters is located in Ireland.

[72] Eduardo Ustaran, *Safe Harbor in the Dock*, HOGAN LOVELLS CHRON. OF DATA PROTECTION, May 2015, *available at* http://www.hldataprotection.com/files/2015/05/Safe-Harbor-in-the-Dock-Ustaran-PLB.pdf.

[73] *Id.*

[74] Press Release, Federal Trade Commission, FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework (Jan. 12, 2014), *available*

companies had represented publicly that they held current Safe Harbor certifications. However the FTC did not find that the false statements hid actual violations; rather, the companies had allowed their certifications to expire. In no instance, however, did the FTC allege that the companies had substantively violated the Safe Harbor Privacy Principles that are at the heart of the framework. The settlements set forth continuing reporting obligations for each company regarding its compliance efforts with the Safe Harbor Framework, as well as obligations to inform current and future employees regarding the company's Safe Harbor obligations. These obligations are effective for 20 years. No monetary penalties were assessed.

The settlements should be seen—and were likely intended—as a further demonstration by the U.S. government of its commitment to enforce the Safe Harbor Framework in the face of significant criticism from the European Commission and individual DPAs as to the efficacy of the program. Also notable is that the 12 companies are not small, fly-by-night organizations, but include well-known and respected businesses, such as Level 3 Communications, one of the world's largest ISPs; BitTorrent, a P2P file-sharing protocol provider; Apperian, a developer of business apps and security; and DataMotion, a platform provider for encrypted email and secure file transport. Other companies include an accounting firm, a consumer products company, a medical research lab, and three professional (American) football teams. While the FTC is publicizing the success of its enforcement efforts, it notes that its investigation resulted from complaints filed with the agency, including from Galexia, a consulting firm in the data privacy space that has been a very vocal critic of the Safe Harbor Framework and the FTC's enforcement efforts of the Safe Harbor Program. It is unknown whether the FTC would have initiated the investigations absent the complaints.

Despite the FTC's apparent increased enforcement efforts, in March 2014 the European Parliament adopted a resolution regarding proposed revisions to the EU Data Protection Directive, which included specific attacks on the Safe Harbor Program.[75] In particular, the resolution seeks the "immediate suspension" of the program, especially in light of the Snowden revelations of data privacy violations. Also proposed is that the issue of international transfers of data regarding EU citizens should not be included in EU/U.S. trade negotiations. Moreover, the European Parliament proposes establishing legal remedies for EU citizens for

at http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

[75] Press Release, European Parliament/News, US NSA: Stop Mass Surveillance Now or Face Consequences, MEPs Say (Mar. 12, 2014), *available at* http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say.

violations concerning their transferred data as well as creating an independent, European-based data cloud.

These strong anti-Safe Harbor sentiments of the European Parliament are notable for the contrast with the current official position of the European Union. During President Obama's visit to the European Union in late March 2014, the joint EU/U.S. "Summit Statement" reinforced both parties' commitment to data protection and privacy generally and, specifically, to "comprehensively strengthening" the Safe Harbor Program through "increased transparency, effective enforcement and legal certainty."[76] As of the date of this chapter, these discussions remain ongoing.[77]

V. CONCLUSION

International transfers of personal data are a fundamental and growing attribute of worldwide commercial activities. While the European Union, the United States, and other countries have established mechanisms that seek to enable such transfers while providing sufficient protections for those data, these mechanisms are under increasing pressure as the prevalence of "Big Data" uses keeps growing. However, protecting personal data while enabling their use for commercial purposes, does not necessarily have to be a zero-sum equation. The "flow" of data across international borders will continue; the market pressures are too great. However, a balance can and should be reached. As this chapter has attempted to demonstrate, finding that balance is not necessarily an easy task and is subject to continuous scrutiny and change.

---

[76] Press Release, The White House, EU-US Joint Statement (Mar. 26, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/03/26/eu-us-summit-joint-statement.

[77] In September 2014, the incoming Commission President, Jean-Claude Juncker, called for a review of the Safe Harbor Framework to be completed in six months, or by March 2015. *See* Sam Pfeifle, *What Does the New European Commission Mean for Privacy?*, PRIVACY ADVISOR, Sept. 10, 2014, https://privacyassociation.org/news/a/what-does-the-new-european-commission-mean-for-privacy/.