2016

Complying with International Data Protection Law

McKay Cunningham

Follow this and additional works at: https://scholarship.law.uc.edu/uclr

Recommended Citation

McKay Cunningham, Complying with International Data Protection Law, 84 U. Cin. L. Rev. (2016)
Available at: https://scholarship.law.uc.edu/uclr/vol84/iss2/4

This Article is brought to you for free and open access by University of Cincinnati College of Law Scholarship and Publications. It has been accepted for inclusion in University of Cincinnati Law Review by an authorized editor of University of Cincinnati College of Law Scholarship and Publications. For more information, please contact ken.hirsh@uc.edu.
INTRODUCTION

Complying with data protection law is increasingly complex. In addition to federal, state, and local law, international data protection law extends beyond traditional jurisdictional norms. Companies with minimal—even tangential—international connections may fall within the strictures of foreign law or at least be affected by it. As markets flatten in the global economy, so do the laws that aim to regulate them, particularly those laws that target inherently borderless actions. It is inevitable that omnibus laws dealing with digital data are extra-jurisdictional. Digital data travels via circuitous and transnational routes from origin to terminus—if an end exists at all.1 As data flows without regard to territorial borders, so does legislation aimed at regulating it.2

As a result, organizations that use, store, transfer, or process personal data must consider a broad array of legal restrictions when assessing compliance. Counterintuitively, the compliance picture for a United States organization is among the most convoluted. As one of few developed nations without a comprehensive data protection law, the U.S. protects personal data through a disjointed mix of state and local law, federal legislation, executive orders, and self-regulation. This disparate confluence of binding law complicates commerce and presents obstacles to organizations proactively seeking compliance. As one scholar politely put it, “Companies are frustrated from the lack of harmonization and the fact that they are often subject to conflicts between data protection law and other obligations.”3

Properly presenting the full compliance measures required under

---

1 See Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 YALE J. INT’L L. 1, 22-38 (2000) for a note explaining that the exact origin of any given data, or the nations, if any, associated with that data may be impossible or impracticable to discern. See generally Miriam Wugmeister et al., Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules, 38 GEO. J. INT’L L. 449, 473 (2007).

2 See WORLD ECONOMIC FORUM & A.T. KEARNEY, RETHINKING PERSONAL DATA: A NEW LENS FOR STRENGTHENING TRUST 3 (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf (“The growth of data, the sophistication of ubiquitous computing and the borderless flow of data are all outstripping the ability to effectively govern on a global basis.”).

international data protection law is a tall task, and one that is beyond the scope of this article. This article instead identifies those companies that must comply with international data protection laws by explicating the extra-jurisdictional provisions of those laws. The article then outlines several legal means of compliance. More specifically, Part I distinguishes U.S. data protection law from international data protection law. Part II studies the European Union's (E.U.) data protection law and details why that law most aptly represents international data protection law generally. Part III analyzes the extra-jurisdictional reach of E.U. data protection law, confronting the question of which U.S. companies have an obligation to comply, and Part IV outlines legal means of compliance with international data privacy law.

I. U.S. DATA PROTECTION LAW

Data protection law itself is novel, given the nascent Age of Information.4 The commercialized Internet is but a few decades old and yet today logarithmic increases of information—terabytes of data—course through the web, much of it personal. If the world’s expanding digital content were printed and bound into books it would form a stack that would stretch from Earth to Pluto ten times.5 As more people log on and join the digital masses for the first time, cross border data flows inevitably expand, as do calls for protecting private data.6

In the United States, the laws protecting data privacy have been widely characterized as “sectoral,” a reference to fragmented, cross-governmental, and industry-specific regulation.7 Unlike in Europe, U.S. law does not recognize a fundamental right to privacy.8 The U.S. Constitution does not explicitly protect privacy, but constitutional privacy protections implicitly derive from the First, Third, Fourth, Fifth, and Fourteenth Amendments.9


7. See Ozer, supra note 6, at 217 for a note on the many and disparate privacy related statutes.


The industries constrained by data protection legislation are those that traditionally handle sensitive private data.\textsuperscript{10} The laws governing data protection often are narrowly tailored, addressing particular elements of personal information or discrete uses of discrete data.\textsuperscript{11} U.S. regulation is further complicated by state and local data privacy law. For example, the federal Health Insurance Portability and Accountability Act does not have a pre-emptive effect, leaving state governments room to create further legislation affecting medical and health information.\textsuperscript{12} Forty-seven of fifty states have breach notification laws, which generally require organizations divulge when they have been hacked if "personal information" of others was made vulnerable by the infiltration,\textsuperscript{13} with California a state leader in these changes in privacy legislation, enacting two new privacy laws in 2013.\textsuperscript{14}

Separate from government regulation, many specialized industries "self-regulate," by crafting non-legally enforceable guidelines or "best practices."\textsuperscript{15} The Clinton administration advocated industry self-regulation as the best means of protecting the personal privacy of online users without hobbling each industry with government interference,\textsuperscript{16} stating "[w]e believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation."\textsuperscript{17} Several industries claim such self-regulation today. The Direct Marketing Association, for example, provides its members with online privacy principles that call for marketers operating websites to post a prominent notice to consumers of the marketer's information collection practices.\textsuperscript{18} Private auditors also populate the self-regulatory sphere. A prominent exemplar is TRUSTe, a nonprofit initiative.

\textsuperscript{10} See Lisa J. Sotto, Privacy and Data Security Law Deskbook § 1.04 (2010).
\textsuperscript{11} See id.
\textsuperscript{14} See CAL. CIV. CODE § 1798.80; id. § 1798.81.5 (noting "the intent of the Legislature to ensure that personal information about California residents is protected").
\textsuperscript{16} See William J. Clinton & Albert Gore, Jr., A Framework for Global Electronic Commerce, 18 U.S. NAT’L ARCHIVES & RECS. ADMIN. (1997), http://clinton4.nara.gov/WH/New/Commerce/read.html (explaining that the private sector should take the lead to protect privacy over the Internet through self-regulatory regimes); but see Jessica Litman, Information Privacy/Information Property, 52 STAN. L. REV. 1283, 1284 (2000) ("From most objective standpoints, protecting information privacy though industry self-regulation is an abject failure.").
\textsuperscript{17} Clinton & Gore, supra note 16.
sponsored by Microsoft, Compaq, IBM, and AT&T among others.\textsuperscript{19} TRUSTe provides oversight and auditing functions and issues "trustmarks" to organizations that abide by stated privacy policies.\textsuperscript{20}

That is not to say that federal privacy legislation does not exist. A cadre of statutes illustrates the sectoral approach by protecting private information in discrete industries or contexts. Examples include the Telecommunications Act of 1996, which restricts telecommunications carriers' use of private customer information;\textsuperscript{21} the Gramm-Leach-Bliley Act, which restricts financial institutions' use and dissemination of private financial data;\textsuperscript{22} and the Fair and Accurate Credit Transactions Act, which restricts credit reporting and increases protections for related personal information.\textsuperscript{23} The patchwork of federal privacy laws often overlap and even contradict each other. Floundering in an array of disparate privacy laws, Google called for "global privacy standards" as early as 2007.\textsuperscript{24}

Even the most foundational questions—the definition of "personal information"—remain uncertain. The definition of personal information found in the Fair Credit Reporting Act\textsuperscript{25} differs from that found in the Video Privacy Protection Act,\textsuperscript{26} which in turn differs from that found in the Gramm-Leach-Bliley Act.\textsuperscript{27} The Children's Online Privacy Protection Act and the Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records employ circular definitions of personal information: the former states that personal information is "individually identifiable information about an individual;"\textsuperscript{28} the latter defines personal information as "information


\textsuperscript{20} See TRUSTe, supra note 19.


\textsuperscript{23} Id. §§ 1681–81x (2006).


\textsuperscript{25} 15 U.S.C. § 1681a (2006) (applying to consumer reporting agencies that provide consumer reports, defined as communications by such an agency bearing on a consumer’s credit worthiness or personal characteristics when used to establish consumer’s eligibility in certain contexts).

\textsuperscript{26} Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (defining personally identifiable information as "information which identifies a person").


\textsuperscript{28} Id. § 6501(8).
that identifies an individual." 29 Disunity among various privacy laws derives from substantial discord ranging from broad policy questions to granular legal applications. 30 Regulatory uncertainty continues to frustrate entities that deal with personal information, particularly those that are reliant on e-commerce, conduct multinational operations, or both. 31

Nevertheless, the U.S. is conspicuously resolved and increasingly isolated in its refusal to pass comprehensive data privacy legislation. Following a series of notable security breaches at large companies that exposed consumer personal information, 32 Congress stepped up regulatory efforts, but declined to pass omnibus privacy legislation that would harmonize the current regulatory patchwork. 33 In the meantime, states continue to create privacy legislation, like California’s recent law providing youth the “right to be forgotten”—a right enabling parents, on behalf of youth, to demand erasure of relevant personal information of a minor held or processed by third parties. 34 Even President Obama, through Executive Order, recently entered the regulatory fray. 35

While comprehensive legislation overriding the patchwork of federal and state legislation would certainly lend harmony, most commentators agree that such an approach is unlikely in the near term. 36 This conglomeration of varied privacy protections contrasts neatly with the approach taken by the European Union. European officials had hoped to

31. See id. at 175-94.
33. See, e.g., Personal Data Privacy and Security Act of 2014, S.1897, 113th Cong. (2014). The bill defines personal information as “sensitive personally identifiable information” and includes: (1) specified combinations of data elements in electronic or digital form, such as an individual’s name, home address or telephone number, mother's maiden name, and date of birth; (2) a non-truncated social security number, driver’s license number, passport number, or government-issued unique identification number; (3) unique biometric data; (4) a unique account identifier; and (5) any security code, access code, password, or secure code that could be used to generate such codes or passwords. See also DEP’T OF COM., INTERNET POL’Y TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010); FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010) (reports by the Department of Commerce and the Federal Trade Commission on online privacy indicating that both agencies plan to play significant roles in this area).
36. See, e.g., SOTTO, supra note 10, at § 1.04 (noting that “harmonization is not imminent”).
sway U.S. lawmakers to enact a comprehensive privacy regime, but basic differences in the role of government and fundamental rights among other differences thus far have prohibited it.

II. E.U. DATA PROTECTION LAW

Unlike in the U.S., privacy is a fundamental right in the E.U. Rather than sectoral and industry specific laws protecting privacy coupled with industry self-regulation, the E.U. promulgated omnibus legislation protecting personal data across the board. Many attribute E.U. designation of privacy as a fundamental right to Nazi exploitation of European census records during World War II. Nazi review of personal, often classified, files resulted in deportation to concentration camps and increased leverage under fascist rule. Such abuse in recent history of private and personal information undergirds European vigilance in “protecting personal privacy and resisting state intrusions into private life.” The European Convention on Human Rights adds further ideological support undergirding the regulations by identifying a right associated with “private and family life, his home and his correspondence.”

This foundation spurred a litany of attempted privacy regulations, treaties and local laws, culminating in the European Union’s Directive 95/46/EC (Directive). The Directive set the international standard for data privacy and security regulation and facilitated a trend among technologically advanced countries toward adopting nationalized data...
privacy laws.\footnote{See Graham Greenleaf, Global Data Privacy Laws: 89 Countries, and Accelerating, 115 Privacy Laws & Bus. Int'l Rep. (2014).} One of the key reasons that countries outside the E.U. adopted laws similar to the Directive resides in the strictures of the Directive itself. First, most commentators characterize the Directive as the most influential national data protection law.\footnote{See Kuner, supra note 3, at 55, for a characterization of "E.U. law as the most influential body of data protection law worldwide."} Second, and more importantly, the Directive's reach extends outside of the E.U., containing important provisions concerning international data transfers.\footnote{Data Protection Directive, supra note 39, at art. 26.} By outlawing transfers of personal data to countries or entities that fail to protect personal data in conformity with the Directive, the E.U. incentivizes international compliance.\footnote{Paul M. Schwartz, The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures, 126 Harv. L. Rev. 1966, 1972-73 (2013).} If foreign countries and their businesses cannot "process" the personal information of E.U. residents, access to the entire E.U. market is jeopardized.

It is perhaps this panoptic approach that fuels the global trend toward conformity with the Directive.\footnote{Greenleaf, supra note 45, at 3.} There were seven new national omnibus privacy laws in the 1970s, ten in the 1980s, nineteen in the 1990s, thirty-two in the 2000s, and eight so far in the first two years of this decade.\footnote{See id. at 2.} At the current rate of expansion, fifty new laws will emerge in this decade. As Professor Graham Greenleaf notes, "[t]he picture that emerges is that data privacy laws are spreading globally, and their number and geographic diversity accelerating since 2000."\footnote{Id. at 1.} The great majority of countries that have enacted data privacy laws have tracked, to a large degree, the Directive.\footnote{See generally Lee A. Bygrave, Data Privacy Law: An International Perspective (Oxford Univ. Press 2014).} The most economically significant nations notably absent are the United States and China.\footnote{Greenleaf, supra note 45.} India adopted omnibus data privacy law in 2011.\footnote{See Thomas Claborn, India Adopts New Privacy Rules, Info. Week (May 5, 2011), http://www.informationweek.com/government/policy/india-adopts-new-privacy-rules/229402835.}

In light of the Snowden revelations, some commentators have noted increased interest in regulating data protection at the international level.\footnote{Kuner, Search for an International Data Protection Framework, supra note 3, at 55.} While many individual countries have adopted data protection laws patterned after the Directive,\footnote{See SOTTO, supra note 10, at § 1.} and while the trend toward global harmonization of data protection principles is currently afoot, regulatory
conformity remains a distant goal.\textsuperscript{57} Organizations attempting to drive international dialogue include the Asia-Pacific Economic Cooperation Privacy Framework, commonly referred to as “APEC,”\textsuperscript{58} the Organisation for Economic Co-operation and Development or “OECD,”\textsuperscript{59} the United Nations, and the International Organization for Standardization. These entities offer insight into the future of international data protection regulation.\textsuperscript{60}

Notwithstanding international treaties or conventions, the E.U. endeavors to maintain its prominence as the tip of the data protection spear.\textsuperscript{61} The new E.U. Data Protection Regulation (Regulation) set to replace the Directive in 2016 confirms that goal by increasing fines for non-compliance and adding new data protection rights.\textsuperscript{62} As one unnamed E.U. official said, “with these proposals, the E.U. is becoming the de facto world regulator on data protection.”\textsuperscript{63}

\textbf{A. The Directive’s Requirements}

If a non-E.U. entity comes within the parameters of the Directive, what does the law require? First, as noted above, the Directive soon will be supplanted by E.U. Data Protection Regulation, a law that confirms the strictures of the Directive and advances the goal of protecting personal information by adding new rights and larger penalties for non-compliance.\textsuperscript{64} The Regulation likely will become effective in 2016 with graduated enforcement in the following two years.\textsuperscript{65} The basic

\textsuperscript{57} See Kuner, \textit{Search for an International Data Protection Framework}, supra note 3, at 55 (noting that “considerable differences still exist in the approaches to data protection around the world, owing to cultural, historical, and legal factors”).

\textsuperscript{58} ASIA-PACIFIC ECON. COOPERATION, APEC PRIVACY FRAMEWORK (2004), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05_ecsg_privacyframework.ashx.

\textsuperscript{59} The Organization for Economic Cooperation and Development is an international economic organization of over thirty countries founded in 1961 to stimulate economic growth and world trade. It was originated in 1947 to run the U.S.-financed Marshall Plan for reconstruction of war-torn Europe. \textit{See History, ORGANISATION FOR ECON. CO-OPERATION & DEV.}, www.oecd.org/history (last visited May 18, 2015).

\textsuperscript{60} See Kuner, \textit{Search for an International Data Protection Framework}, supra note 3, at 58-60 (“Thus far, most international initiatives concerning data protection set the agenda and formulate broad principles, but do not specify how they are to be implemented in detail.”).

\textsuperscript{61} See id.

\textsuperscript{62} PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION), EUROPEAN COMM’N (2012) [hereinafter PROPOSAL FOR A REGULATION].


\textsuperscript{64} PROPOSAL FOR A REGULATION, supra note 62.

\textsuperscript{65} See id.
requirements of both the Directive and Regulation are at the core of the global debate on privacy and data security. Both require that personal data must be:

1. Processed fairly and lawfully;
2. Collected for legitimate and specified reasons;
3. Adequate, relevant, and not excessive in relation to the purposes for which it is collected;
4. Accurate and, where necessary, kept up to date; and
5. Retained as identifiable data for no longer than necessary to serve the purposes for which the data were collected.\(^{66}\)

While these requirements may appear innocuous, application imposes a heavy burden on many entities that "process" the personal data of E.U. residents. Under these requirements, for example, an E.U. resident has the right to know when personal data is collected.\(^{67}\) Entities that collect personal data directly or indirectly must provide such notice.\(^{68}\) Personal data can only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."\(^{69}\) Even if collected for a legitimate purpose, an E.U. resident often has the right to choose not to have the personal data collected or to have it deleted or corrected.\(^{70}\) Consent must be a "freely given, specific and informed indication of [the resident's] wishes."\(^{71}\)

Moreover, an E.U. citizen has the right to know how personal data will be used and to restrict its use.\(^{72}\) Data collected by an organization must be accurate and individuals have the right to challenge accuracy, mirroring the obligation of data controllers to ensure that inaccurate or incomplete data is corrected.\(^{73}\) Finally, those who control private data must protect it. Protecting personal data, at minimum, requires that data controllers “implement appropriate technical and organizational measures to protect personal data against . . . destruction or . . . loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.”\(^{74}\) Security measures must be “appropriate to the risks represented by the processing

---

66. Id. at art. 6; Data Protection Directive, supra note 39, at art. 6.
67. Id. Data Protection Directive, supra note 39, at art. 10. E.U. residents are entitled to know the identity of the data controller, the purposes for which their personal data will be processed, as well as other information regarding fair processing. Id.
68. Id. at arts. 6-7.
69. Id. at art. 6(1)(b).
70. See id. at art. 2(b).
71. Id.
72. Id. at art. 6(1)(d).
74. Id. at art. 17(1).
and the nature of the data be protected." These requirements place immediate and often burdensome obstacles in the path of those who "process" and "control" personal data.

B. The Directive's Transnational Reach

The Directive has an impressive and much criticized reach. Even organizations based in the U.S. with no office in the E.U. are not necessarily exempted. As noted above, the Directive restricts personal data transfers to any country or entity that fails to comply with the Directive's strictures. Only eleven countries have been deemed "adequate" by the E.U., and the U.S. is not among them. E.U. businesses wishing to transfer personal data of E.U. citizens outside the E.U. must first ensure that the country or organization receiving that data complies with the Directive. This can be accomplished in a number of ways, as discussed below.

Aside from restricting transfer of personal information outside the E.U., the Directive includes other provisions, deemed extra-territorial, extra-jurisdictional, or both. If a non-E.U. data controller, for example, "makes use of equipment" situated in the E.U. for the processing of personal data, the Directive may control:

Each Member State shall apply . . . this Directive to the processing of personal data where: (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

In principle, any online business trading with E.U. citizens would process some personal data and use equipment in the E.U. to process the
data—the customer’s computer. Notably, the E.U. Regulation set to replace the Directive in 2016 extends this extra-jurisdictional provision. The Regulation applies in cases where non-E.U. entities offer goods or services to persons in the E.U., including entities that monitor the behavior of E.U. residents. Abandoning the “equipment” nexus, the Regulation broadens its grasp and, as one researcher suggests, “seems likely to bring all providers of Internet services such as websites, social networking services, and app providers under the scope of the E.U. Regulation as soon as they interact with data subjects residing in the European Union.”

These provisions are not insignificant. Companies with only one office or principal place of business within the U.S. have not been identified historically as “international.” Normative jurisdictional law insulates such entities from being haled into the court of a foreign country to answer claimed infractions of that country’s law. However, commerce is no longer primarily local, or even regional. Information services and goods constitute the world’s largest economic sector. The U.S. Department of Homeland Security stated it broadly: “Our economy and national security are fully dependent upon information technology and the information infrastructure.” In short, companies that are not already online and gathering and processing more and more digital data are becoming the shrinking minority.

Article 4 of the Directive states that if a data controller is located outside the E.U., but uses equipment within the E.U. for any purpose other than transmission, the law of the Member State where the equipment is located will apply.

82. See PROPOSAL FOR A REGULATION, supra note 62, at art. 3.
83. See id.
84. DAN JERKER B. SVANTESSON, EXTRATERRITORIALITY IN DATA PRIVACY LAW, 107 (2013).
86. See id.
88. See id.
90. See Scott R. Peppet, Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future, 105 NW. U. L. REV. 1153, 1164 (2011) (noting that some 92% of commercial websites collect personal data from web users and that corporate data mining links at least seven thousand transactions to each individual in the United States per year).
The Regulation’s scope arguably encompasses “all providers of Internet services.” Even smaller companies that have an online presence but claim not to be a “provider of an Internet services” should take account of their data privacy policies. Such companies may not fall under the Regulation’s purview, but likely share or receive information with organizations that do. The Directive and Regulation address this eventuality by restricting transfers of personal data.

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 . . . may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.

A small business with one office in Ohio that pays a third party to operate its website may not directly fall within the Directive’s ambit, but the third party likely would. Personal information about an E.U. resident could not be transferred to the business from the business’s own website unless proper privacy policies were in place. At a certain level of abstraction, the Directive and Regulation are designed to require discrete protections of E.U. residents’ personal data no matter where that data is processed.
Of course, these extra-jurisdictional provisions within the Directive require the “processing” of E.U. citizen “personal information.” The Directive applies to (1) personal data that is (2) processed by (3) controllers or processors.  

Personal data is defined in the Directive as: Any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.  

This definition is broad by its terms and in its interpretation. It equates identifying information, even that used only to note a user interacting with an organization with identifiable information, information allowing the user to be personally identified. Most non-experts liken personal information to social security numbers, names and addresses, but the Directive’s definition is far more ambitious. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot itself make the link. The nine-digit numerical label assigned to each device that participates in a computer network amounts to personal data. The Working Party on data privacy for the European Commission confirmed that IP addresses and cookies are “personal data.” IP addresses are automatically or systematically recorded by countless computer programs—actions that technically meet the Directive’s definitions of “processing” and personal information. Some entities claim exemption from privacy laws by “anonymizing” the data they process. But recent studies reveal how simple
algorithms strip "anonymized" data of its claim rendering it personally identifiable.108 Most anonymized information that even remotely relates to an individual can be decoded with a few additional data points.109 With zettabytes already coursing through the Internet and a 2,000% increase in global data expected by 2020,110 additional data points are not hard to come by. The more data there is, the less that any of it can be said to be private.111 Promises that the personal information gathered will be anonymized before sharing112 will soon be illusory: "[advocates of anonymity] fundamentally rely on the fallacious distinction between ‘identifying’ and ‘non-identifying’ attributes."113

Similarly, the Directive’s definition of “processing” is equally broad: [A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.114 Any collection, use, and transfer—even the redaction and deletion thereof—constitutes "processing."115 This definition purposefully includes data processed automatically as part of a filing system, without regard to its use.116 The Directive defines those deemed to have “processed” personal data as either data controllers or data processors.117 A data controller is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."118

These expansive definitions, coupled with extra-territorial provisions,
reflect the borderless nature of Internet data flow. Laws that regulate the gathering, storing, and use of digital information risk futility through circumvention unless they too are borderless in nature. The European Commission website concedes the same: "Without such precautions, the high standards of data protection established by the Data Protection Directive would quickly be undermined, given the ease with which data can be moved around in international networks."

In light of the Directive's purposefully broad definitions and extra-jurisdictional provisions, companies based in the U.S. that engage in e-commerce, employ E.U. citizens, and seek to grow the business in the global economy should analyze the Directive and accompanying resources to determine whether compliance with those foreign laws is required. This is essential "because of the scope of the Data Protection Directive, any business that has contact with E.U. residents on anything other than an anonymous cash-only basis has effectively collected some form of personal data and thus would be subject to the Data Protection Directive."

III. COMPLYING WITH THE DIRECTIVE

Full compliance with data protection law, both domestic and international, is no small task. Multiple, often-conflicting laws create uncertainty. Apart from parsing the legal requirements, the cost of compliance can be daunting, including but not limited to assessing the company's information infrastructure, categorizing types of data processed and types of processing itself, identifying origins of the data, analyzing storage of the data, tracking transfer of the data, and examining the use of the data. In the age of the hacker, providing "reasonable security" for personal data is yet another requirement and a leviathan unto itself. After assessing the organization's informational

120. Schwartz, supra note 48, at 1973 ("Globalization of world data flows called for E.U. action with just such an international reach.").
123. See Kuner, Search for an International Data Protection Framework, supra note 3, at 65.
125. See id. Kenneth M. Siegel, Comment, Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information
infrastructure and integrating proper security, organizations often incorporate information protection systems across the board, devise and publish privacy policies, periodically audit compliance, and identify an executive administrator as an official data privacy officer. These steps toward compliance also create potential liability.

Failing to comply—or failing to show concerted effort to comply—can expose organizations to even more liability. The E.U. Regulation effective in 2016 increases the potential fines from the greater of €100,000,000 or 5% of annual worldwide turnover. In the United States, the Federal Trade Commission has picked up enforcement activity for data protection violations in the last decade and has vowed to do more over the next decade. Public awareness of the value of personal information in tandem with notable security breaches at established companies incentivizes others to maintain robust privacy policies.

Finally, even if a moderately sized domestic company technically falls outside the scope of E.U. privacy law on their own, interactions with other parties may make this an incorrect assumption. The extra-jurisdictional provisions of the Directive are elongated in the Regulation. The domestic company may do business (or share information) with a third party that falls under the Regulation’s reach and therefore cannot share information without, at minimum, a legal promise to protect the subject information. “The practical consequence of compliance is to raise privacy standards for customers both within and without the European Union, thus ‘ratcheting up’ the standards for data privacy regulation globally.” Additionally, the scores of nations that recently have adopted omnibus privacy laws

---


127. PROPOSAL FOR A REGULATION, supra note 62, at art. 79.


129. See, e.g., Jesse L. Noa, They Did it for the Lulz: Futuer Policy Considerations in the Wake of Lulz Security and Other Hacker Groups’ Attacks on Stored Private Consumer Data, 1 J.L. & CYBER WARFARE 155, 177-184 (2012); see also Cunningham, supra note 124, at 644.

130. See PROPOSAL FOR A REGULATION, supra note 62.


pattern them after the Directive. As only one example, if a U.S. organization has no European connections but processes information from Latin America, Argentina and Uruguay enforce well-developed, E.U.-style data protection laws.

Fortunately, a range of compliance tools and options are available. At one end of the spectrum, "privacy by design" integrates data protection systems throughout the organization and endeavors to achieve more than mere compliance with data protection laws. "The future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation." At the other end of the spectrum, several companies institute privacy protections on an ad hoc basis and rely on contractual covenants in order to receive and process personal information. There are other options between these poles, including the common method used by U.S. companies of obtaining actual consent of the data subject, standard contractual clauses, binding corporate rules, and, formerly, participation in the Safe Harbor program.

A. Consent

Consent, at first blush, seems attractive, but the Directive's drafters did not intend for this derogation to be easily met and dilute the law's effect. Article 26(1) of the Directive requires proof that the data subject gave consent unambiguously. Subsequent interpretation by the Working Party clarified that consent must be a clear and unambiguous indication of wishes, given freely, with specification, and after being fully informed. Implied and retrospective consent fails
this standard and the specificity requirement necessitates consent to be specific to each data transfer, rather than one global consent governing all uses and transfers.\textsuperscript{141}

\textbf{B. Standard Contractual Clauses}

Standard Contractual Clauses or Model Clauses are a contractual solution to facilitate data transfer from the E.U. to a country or data controller not otherwise deemed “adequate.”\textsuperscript{142} Article 26(2) of the Directive authorizes such a data transfer where the E.U. transferor relies on “appropriate contractual clauses” to provide protection.\textsuperscript{143} If such clauses are used, personal data can flow from an E.U. controller to a data controller or processor located in a country that does not enforce privacy laws commensurate with the Directive.\textsuperscript{144} These pre-drafted contractual covenants offer third party beneficiary rights to data subjects between a data exporter in the E.U. and a data importer outside the E.U. whereby both parties promise compliance with the Directive.\textsuperscript{145}

Three Standard Clauses have been approved by the E.U. Commission: (1) Standard Clauses for Controller-to-Controller transfers, approved June 2001; (2) Standard Clauses for Controller-to-Processor transfers, approved December 2001 (amended 2010); and (3) Set II Standard Clauses for Controller-to-Controller transfers, approved December 2004.\textsuperscript{146} Generally speaking, these Standard Clauses require the signatory to comply with the Directive.\textsuperscript{147} The Clauses address the parties’ responsibilities and liabilities, E.U. citizens’ rights, rights of enforcement under the contract, governing law of the exporter’s home state within the E.U., and the data processing principles at the heart of the Directive including limited use of the data, transparency, security,
rights of access, and onward transfers.\textsuperscript{148}

Importantly, Standard Clauses cannot be amended and parties must complete an appendix, describing in detail the E.U. citizens affected by the transfer, the purpose of the transfer, and the recipients of the data.\textsuperscript{149} A description of the security methods and tools employed by the transferee is also required.\textsuperscript{150}

Companies seeking a quick legal basis to facilitate international data transfers have relied on Standard Clauses, although they often require a nuanced understanding of the company's data flows and IT infrastructure.\textsuperscript{151} E.U. Member States generally approve international data transfers automatically, although organizations seeking to transfer personal data usually allow buffer time within a given project to complete authorization.\textsuperscript{152} Before choosing this route, be forewarned that exports of data under Standard Clauses are subject to the jurisdiction and enforcement of the E.U. Member State in which it is approved.\textsuperscript{153} As a result, companies embracing this compliance model avail themselves the possibility of two potential actions: (1) a civil suit by the data subject, and (2) an investigation by a foreign data protection authority.\textsuperscript{154}

\textbf{C. Binding Corporate Rules}

Aside from multinational companies, Binding Corporate Rules are somewhat rarely used as a method of compliance.\textsuperscript{155} Binding Corporate Rules are a set of legally binding rules based on the Directive's standards that ensure adequate safeguards for transfers of personal data among entities within the same corporate group.\textsuperscript{156} The European Commission depicts Binding Corporate Rules as "a solution for multinational companies which export personal data from the European Economic Area to other group entities located in third countries which do not ensure an adequate level of protection."\textsuperscript{157}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{148} See \textit{id}.\textsuperscript{148}
\item \textsuperscript{149} See \textit{SOTTO}, \textit{supra} note 10, at § 18.02 [B].\textsuperscript{149}
\item \textsuperscript{150} See \textit{id}.\textsuperscript{150}
\item \textsuperscript{151} See Schwartz, \textit{supra} note 48, at 1981-82.\textsuperscript{151}
\item \textsuperscript{152} See \textit{id}.\textsuperscript{152}
\item \textsuperscript{153} See \textit{SOTTO}, \textit{supra} note 10, at § 18.02.\textsuperscript{153}
\item \textsuperscript{154} See \textit{id}.\textsuperscript{154}
\item \textsuperscript{155} Article 29 Data Protection Working Party, Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the E.U. Data Protection Directive to Binding Corporate Rules for International Data Transfers, at 5-6, 11639/02/EN, WP 74 (June 3, 2003).\textsuperscript{155}
\item \textsuperscript{156} See \textit{id}.\textsuperscript{156}
\item \textsuperscript{157} EUROPEAN COMM'N, \textsc{Overview of Binding Corporate Rules}, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (last visited Dec. 4, 2015).\textsuperscript{157}
\end{itemize}
\end{footnotesize}
Like internal company codes prohibiting insider trading, Binding Corporate Rules seek to hold responsible those within the corporate group to data subjects whose personal information is processed by any entity or person within that group. The inefficiency and rigidity of Standard Contractual Clauses spawned Binding Corporate Rules, which were intended as a less iterative alternative. Unlike Standard Contractual Clauses, Binding Corporate Rules can be modified and tailored to the applying company’s already existing privacy policies. Once they have been approved by the E.U. data protection authority, the company is free to transfer data globally within its corporate affiliates without having to resort to Standard Contractual Clauses for each data transfer.

The cost and ineffectiveness of this alternative, however, has dissuaded many from using it. More than four years after the June 2003 publication of the Working Party’s paper detailing Binding Corporate Rules, only one company in the United Kingdom—General Electric—successfully applied for Binding Corporate Rules, and even this was limited to employee data. General Electric’s application was complex and approval required separate sanction from each applicable data protection authority. Scandinavia’s review alone took five months. The Working Party has since taken steps to streamline the application and approval process, but the process nonetheless continues to be costly and inefficient.

Even if a multinational company receives approval, Binding Corporate Rules are mandatory within the entire corporate group, so that

---

159. See Sotto, supra note 10, at § 18.02.
161. See Sotto, supra note 10, at § 18.02 (noting that “the BCR approval process was too lengthy and complex”).
164. See The Least Worst Solution, supra note 162.
the disparate laws applicable to each must be considered. Once approved, Binding Corporate Rules bestow third party beneficiary rights to data subjects including certain jurisdictional rights. Legal enforceability means that E.U. citizens are entitled to enforce compliance by filing complaints with the relevant Data Protection Authority in the E.U. Annual audits attend Binding Corporate Rules, and liberalized data transfers are only allowed within the group, leaving multinational companies saddled with Standard Contractual Clauses for most other data transfers.

D. Safe Harbor

The most common compliance method for U.S. companies, until recently, was the Safe Harbor program. However, on October 6, 2015, the European Court of Justice invalidated the EU-US Safe Harbor program in Schrems v. Data Protection Commissioner. The Safe Harbor, available only to United States entities, arose from compromise. Given the sectoral regulatory framework in the U.S. coupled with private sector self-regulation and popular disfavor of an omnibus privacy law, the U.S. Department of Commerce and the European Commission negotiated for two years before agreeing to the Safe Harbor exception in 2000. The compromise sought to bridge the differing approaches in the European Union and the United States, streamline the means for U.S. organizations to comply with the Directive, and protect E.U. organizations transferring personal data to U.S. organizations.

The recent invalidation of the Safe Harbor program raises several
questions for U.S. companies. Because the Safe Harbor program largely paralleled the Directive, compliance with the Safe Harbor as a means to be insulated from liability under the Directive remains germane. In practice, a U.S. organization that self-certified through the Safe Harbor program was then afforded automatic approval from data processing authorities in the European Union. The Safe Harbor program was voluntary, self-authorized, and minimally enforced. No government official first inspected and determined whether any given company in fact practiced Safe Harbor principles before awarding certification. In maintaining the [Safe Harbor] list, the Department of Commerce does not assess and makes no representation as to the adequacy of any organization’s privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.

As a result, it was possible for a U.S. company to self-certify compliance with the Safe Harbor requirements and thereby gain clearance to process personal data from the E.U. even if that company did not, in fact, comply with the Directive’s data privacy and security principles. E.U. authorities criticized the self-regulatory nature of Safe Harbor for precisely that reason. The Federal Trade Commission (FTC) historically was slow to prosecute U.S. companies under Safe Harbor, although there were indications that the FTC was increasing its investigations.

177. See id.
179. See U.S.-EU SAFE HARBOR OVERVIEW, supra note 174.
182. See SOTTO, supra note 10, at § 18.02[B].
183. See FTC ENFORCEMENT REPORT, FED. TRADE COMM’N, PRIVACY ENFORCEMENT AND SAFE HARBOR: COMMENTS OF FTC STAFF TO EUROPEAN COMMISSION REVIEW OF THE U.S.-EU SAFE
Safe Harbor certification shifted the jurisdiction and enforcement from European authorities to the United States Department of Commerce and the FTC. The FTC enforced the Safe Harbor requirements pursuant to Section 5 of the Federal Trade Commission Act, which generally proscribes "unfair or deceptive acts or practices in or affecting commerce." Eligibility for Safe Harbor protections required interested U.S. organizations to be subject to the jurisdiction of the FTC or Department of Transportation (DoT). In other words, only U.S. organizations subject to the jurisdiction of the FTC as well as U.S. air carriers and ticket agents subject to the jurisdiction of the DoT could participate in Safe Harbor. Many organizations that deal in foreign commerce were not eligible for the Safe Harbor program, including certain financial institutions—like banks, investment houses, and credit unions, telecommunication common carriers, labor associations, non-profit organizations, and agricultural co-operatives.

The Safe Harbor requirements themselves largely tracked the Directive's requirements, although not precisely. The Safe Harbor Privacy Principles were:

1. Notice: When their personal data is processed in the United States, E.U. citizens must be given notice of (1) the purposes for which their personal information is collected and used, (2) the types of third parties to whom their data are disclosed, (3) the certifying organization's contact information for possible complaints, and (4) the choices available to limit the use and

---


184. See SAFE HARBOR WORKBOOK, supra note 180.
186. See U.S.-EU SAFE HARBOR OVERVIEW, supra note 174.
187. Id.
190. Zaidi, supra note 176 ("Using the E.U. Directive's principles, the Safe Harbor creates a scheme by which U.S. companies are required to comply with stricter privacy standards relating to the transfer of online personal data. With respect to U.S. privacy law, this Safe Harbor regime substitutes the predominant sectoral approach with a more comprehensive approach . . ."). But see Morey Elizabeth Barnes, Comment, Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive, 27 NW. J. INT'L L. & BUS. 171, 182 (2006) (suggesting that E.U. officials may soon "reconsider whether the Safe Harbor really mirrors the letter and spirit of the Data Privacy Directive").
disclosure of their personal data.

2. Choice: E.U. citizens must have the opportunity to opt out of having their personal data disclosed to third parties or used for a purpose incompatible with that for which the data was originally collected. Opt-in consent is required for disclosures of "sensitive" personal data.

3. Access: E.U. citizens must have access to their data to ensure its accuracy.

4. Security: The U.S. organization must take reasonable steps to protect the personal data from loss, misuse, unauthorized access, disclosure, and destruction.

5. Data Integrity: The U.S. organization must ensure the data are relevant and reliable for their intended purposes.

6. Enforcement: The U.S. organization must provide effective enforcement mechanisms to facilitate complaints and disputes.

7. Onward Transfers: The U.S. organization that self-certified may only then transfer E.U. personal data to third parties who participate in Safe Harbor or who otherwise comply with the Directive.\textsuperscript{191}

To comply, an applicant must confirm the organization is subject to the jurisdiction of the FTC or DoT, develop a binding privacy policy that mirrors the Safe Harbor Privacy Principles above, post the policy conspicuously to the public with a specific reference to Safe Harbor compliance, establish an independent recourse mechanism for claimed violations of the policy, and designate a contact within the organization for data protection and Safe Harbor compliance.\textsuperscript{192}

Safe Harbor benefits attached on the date the organization self-certified compliance to the Department of Commerce.\textsuperscript{193} Self-certification itself merely required a letter signed by a corporate officer on behalf of the organization that listed the organization's contact information, described the organization's processing of E.U. personal information including the privacy policy meant to protect it, and claimed self-certification.\textsuperscript{194} The letter, of course, reflected the organization's actual data protection practices, which often began with an evaluation of

\begin{thebibliography}{99}

\bibitem{191} See U.S.-EU Safe Harbor Overview, supra note 174.
\bibitem{193} See U.S.-EU Safe Harbor Overview, supra note 174.
\end{thebibliography}
the type of data it processes, including data flow and how that data is used both within the company and when transferred to third parties.\textsuperscript{195}

The marriage of self-certification and enforceable law under Safe Harbor hinged on the organization's written policy. The policy was imperative because the FTC could only take action against those who fail to protect the privacy of personal information in accordance with their representations, commitments, or both.\textsuperscript{196} Developing a Safe Harbor compliant privacy policy statement was a critical step before submitting a self-certification letter to the Department of Commerce.\textsuperscript{197} The policy had to conform to the U.S.-E.U. Safe Harbor Privacy Principles and also reflect the organization's actual and anticipated information handling practices.\textsuperscript{198} Notwithstanding the invalidation of the Safe Harbor program, it is important to write a policy that is clear, concise, and easy to understand.\textsuperscript{199} Before Safe Harbor invalidation, government officials encouraged companies to specifically reference the company's Safe Harbor status and state that it complied with the U.S.-E.U. Safe Harbor Framework.\textsuperscript{200} Each organization was to include either a hyperlink to the Safe Harbor website or a corresponding URL, e.g. http://export.gov/safeharbor.\textsuperscript{201} The policy itself was to be prominently and publicly available.\textsuperscript{202}

The policy under the Safe Harbor program required reference to an independent recourse mechanism.\textsuperscript{203} This was the primary enforcement vehicle that self-certifying organizations set up in order to investigate and facilitate unresolved complaints.\textsuperscript{204} It leveraged private-sector

\textsuperscript{195} See \textit{Protecting Consumer Privacy}, supra note 192.
\textsuperscript{197} See Leathers, supra note 97, at 201.
\textsuperscript{198} SAFE HARBOR WORKBOOK, supra note 180.
\textsuperscript{199} See id.
\textsuperscript{200} See id.
\textsuperscript{201} See id. Given that Safe Harbor has been invalidated by the CJEU, companies likely should update their privacy policies accordingly, to remove references to Safe Harbor certification.
\textsuperscript{202} If an organization decides to post its privacy policy on an Internet or Intranet site, it must provide an accurate URL. If the organization: 1) has a public website on which it has posted a general privacy policy statement or made any other representation regarding its privacy practices; and 2) has chosen to cover personal data (e.g., client or customer data) other than the organization's own human resources data under its self-certification, then the posted privacy-related language must include an affirmative statement that the organization complies with the U.S.-E.U. Safe Harbor Framework and has certified its adherence to the Safe Harbor Privacy Principles. See U.S. DEP'T OF COM., HELPFUL HINTS ON SELF-CERTIFYING COMPLIANCE WITH THE U.S.-EU SAFE HARBOR FRAMEWORK, http://export.gov/safeharbor/eu/eg_main_018495.asp (last visited Dec. 4, 2015) [hereinafter HELPFUL HINTS].
\textsuperscript{203} SAFE HARBOR WORKBOOK, supra note 180.
\textsuperscript{204} Id.
arbiters to facilitate complaints and assist in self-regulation. Each organization had to ensure that its recourse mechanism was in place prior to self-certification and include in its privacy policy an appropriate reference to contact information for complaint resolution under the recourse mechanism. In most cases, organizations self-certifying to Safe Harbor choose to use private sector dispute resolution programs like TRUSTe or BBBOnline, but the program contemplated other recourse mechanisms. To meet this requirement, an organization could have used either a self-assessment or an outside or third-party assessment program.

After integrating an internal infrastructure designed to protect personal data in conformity with the Safe Harbor Privacy Principles, drafting a written policy, and establishing an independent recourse mechanism, Safe Harbor compliance required designation of a contact within the organization to handle data protection questions, complaints, access requests, and any other issues arising under the Safe Harbor. Little specification was given as to the rank or title this officer should have, but it was advised that organizations demonstrate their commitment to data protection by naming a high-level officer. Many multinational organizations named their General Counsel or created an executive position unto itself, Chief Privacy Officer.

As noted above, the regulatory trend points decidedly toward expanding data protection laws worldwide and companies may do well to begin the path toward compliance. Although Safe Harbor was the most popular method of compliance for U.S. companies—owing largely to the voluntary and self-certification principles—Safe Harbor’s recent invalidation reflects European dissatisfaction with the program’s effectiveness.

Implemented in 2000, the FTC did not bring an enforcement action under Safe Harbor until 2009. As one commentator notes, “[t]he
heaviest criticism is levied against the Safe Harbor’s inadequate internal and external enforcement mechanisms. This criticism appears well-founded. One 2008 study reviewed 1,597 companies that self-certified in order to determine how many complied with one of the seven Safe Harbor principles. Of 1,597 companies, only 348 complied with the enforcement and dispute resolution principle.

Responding to enforcement criticism, the FTC pointed to recent filings and investigations as evidence of elevated enforcement. But the majority of these settled disputes do not audit a company’s internal privacy protections for compliance with Safe Harbor principles. Instead, they involve technical failures like claiming Safe Harbor certification when the company failed to file an annual re-certification letter. In its 2014 report lauding settlements with twelve companies, the FTC actually charged “each company with representing, through statements in their privacy policies or display of the Safe Harbor certification mark, that they held current Safe Harbor certifications, even though the companies had allowed their certifications to lapse.” Such minor infractions draw light punishments including FTC monitoring and threatened penalties for further violations.

Moreover, Safe Harbor had not prompted widespread participation. Quite the opposite. From its inception in November 2000 to December 2006, fewer than 1,100 companies self-certified for Safe Harbor protections. At the time of invalidation approximately 5,200 companies were registered, a tenth of which were not current. In addition, several studies show that only a fraction of those that self-certified actual complied with Safe Harbor principles.

Such tepid participation reflects the program’s inadequacies. The voluntary nature of the program failed to incentivize U.S. businesses; many viewed self-certification as creating unnecessary liability and oversight.

213. See Leathers, supra note 97, at 195-96.
214. See Connolly, supra note 178.
215. See id. at 4.
216. See FTC Settlements, supra note 128; Siegel, supra note 125, at 816-81.
217. Siegel, supra note 125; FTC Settlements, supra note 128.
218. FTC Settlements, supra note 128.
219. Id.
220. Id. Siegel, supra note 125, at 816-21.
222. See The Least Worst Solution, supra note 162.
223. See U.S.-E.U. SAFE HARBOR LIST, supra note 221.
224. See, e.g., Connolly, supra note 181; SOTTO, supra note 10, at § 18.02[B].
binding obligations for itself.226 Those obligations mandatorily were published and invited scrutiny both from data subjects and the FTC.227 Much of the FTC enforcement hinged on the appropriateness of the publication, the failure to re-certify, and falsely holding oneself out as Safe Harbor certified—all avoidable by choosing not participate in the program at all.228 Finally, several Safe Harbor principles are unclear, making it difficult for companies to confidently announce their compliance.

For example, Safe Harbor restricted a participating organization from transferring E.U. personal data to third parties that do not themselves participate in Safe Harbor or who otherwise have been deemed “adequate” by the E.U.229 This means Safe Harbor was not a panacea for participating organizations. While Safe Harbor allowed receipt of E.U. personal data, it arguably had no effect on further transfer of that data—even within the same corporate family.230 Today, data flow is not a binary two-step process, origin and terminus.231 Data routinely is re-exported over and over again, often with no contemplated terminus.232 As one commentator noted, this “can have a devastating effect on the ability of the Safe Harbor member company to conduct onward transfers, since in many cases it will be difficult or impossible to find an applicable legal basis for onward transfers under the national law of the Member State from which the data were originally transferred to the

---

226. U.S.-EU SAFE HARBOR LIST, supra note 221 (noting that the FTC can only “take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments”).

227. SAFE HARBOR WORKBOOK, supra note 180; Nijhawan, supra note 225.

228. See FTC Settles, supra note 128. An organization’s reaffirmation must include the following four points: (1) the information previously submitted to the Department of Commerce is still accurate; (2) the officer is authorized to certify the organization’s continued adherence to Safe Harbor principles; (3) the officer understands that misrepresentations are actionable under the False Statements Act; and (4) acknowledgement that failure to adhere to Safe Harbor principles may lead to enforcement by government authorities. See SAFE HARBOR WORKBOOK, supra note 180.

229. See U.S.-EU SAFE HARBOR OVERVIEW, supra note 174. See SAFE HARBOR PRINCIPLES, supra note 96 (“Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote 1, it may do so if it first either ascertainment that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.”).

230. See Kuner, Onward Transfers, supra note 78.

231. See Cate, supra note 6 (“Information, especially digital information, is inherently global. Data ignores national and provincial borders, and, unlike a truckload of steel or a freight train of coal, data is difficult to pinpoint and almost impossible to block, through either legal or technological means.”).

232. See id.
Another Safe Harbor principle that clouded compliance and discouraged voluntary participation involved data security. An organization had to take reasonable steps to protect the personal data from loss, misuse, unauthorized access, disclosure, and destruction. When sophisticated multinationals like Target, Anthem, and Sony cannot prevent devastating infiltrations, and when high profile government agencies report similar breaches, a data security pledge looks like an impossible promise and an invitation to increased liability. Although U.S. companies no longer can claim compliance with European privacy law through Safe Harbor, many of the data processing principles at the heart of the Safe Harbor program remain important guidelines.

IV. CONCLUSION

The borderless flow of digital information in conjunction with the new global economy undermines the efficacy of historical legal models based largely on regional and national legislation. Effective regulation, it is argued, requires international scope to prevent effected organizations from outsourcing their information processing to less-restrictive principalities. The European Union recognized this early on and its extra-jurisdictional law leads data protection efforts internationally.

U.S. companies without an international office, but that engage in e-commerce or maintain a robust online presence, may fall within the purview of the E.U.’s data protection law. While the likelihood of being haled into an E.U. court to answer for infractions of E.U. law remains low for such companies, the possibility of handling E.U. personal data carries consequences under E.U. law. Chief among those consequences is that the transferor of that data must first ensure that the transferee has

---

233. Kuner, Onward Transfers, supra note 78.
234. SAFE HARBOR WORKBOOK, supra note 180.
235. Id.
established sufficient data protection measures before the transfer occurs, which encourages compliance not by threat of foreign enforcement but by threat of truncation from the E.U. market.

Regardless of whether a U.S. company technically falls within the purview of E.U. law, the international trend decidedly tilts toward expanding data protection laws. Most international privacy laws in the last two decades mimic the E.U. privacy law. In addition, U.S. data protection law is enlarging in the wake of high profile data security breaches. If data protection laws both domestically and internationally are multiplying and broadening, organizations that process information significant to the business should consider compliance measures.

One possible approach exhorts compliance with the most rigorous standard, allowing the organization flexibility across different legal landscapes. As noted above, the E.U. Directive is considered by many to be the most stringent standard of omnibus privacy laws. Policies patterned after the Directive and Regulation, therefore, put an organization in good standing. Alternatively, several other compliance avenues range from ad hoc Standardized Contract Clauses imposed by E.U. law, to Binding Corporate Rules. The recent invalidation of the Safe Harbor program unfortunately increases uncertainty for those companies that opted to comply through self-certification.

International data protection laws are increasing, and as economies flatten, such laws reach further than ever before. Compliance officers would do well to consider international law when developing data protection policy.