U.C.L.A. Law Review

ALI Data Privacy: Overview and Black Letter Text

Daniel J. Solove & Paul M. Schwartz

ABSTRACT

In this Article, the Reporters for the *American Law Institute Principles of Law, Data Privacy* provide an overview of the project as well as the text of its black letter. The *Principles* aim to provide a blueprint for policymakers to regulate privacy comprehensively and effectively.

The United States has long remained an outlier in privacy law. While numerous nations have enacted comprehensive privacy laws, the United States has clung stubbornly to a fragmented, inconsistent patchwork of laws. Moreover, there long has been a vast divide between U.S. and European Union (EU) approaches to regulating privacy—a divide that many consider to be unbridgeable.

The *Principles* propose comprehensive privacy principles for legislation that are consistent with key foundations in the U.S. approach to privacy but also better align the United States with the EU. Additionally, the *Principles* breathe new life into the moribund and oft-criticized U.S. notice-and-choice approach, which has remained firmly rooted in U.S. law. Drawing from a vast array of privacy laws and frameworks, and with a balance of innovation, practicality, and compromise, the *Principles* aim to guide policymakers in advancing U.S. privacy law.

AUTHOR

Daniel Solove is the John Marshall Harlan Research Professor of Law at George Washington University Law School.

Paul Schwartz is the Jefferson E. Peyser Professor of Law at UC Berkeley School of Law, and a Director of the Berkeley Center for Law and Technology.

The views in this Article about the *ALI Principles of Law, Data Privacy* are those of Paul Schwartz and Daniel Solove only. The authoritative text about the meaning of the Principles is the official document itself, which contains comments, notes, and illustrations.

TABLE OF CONTENTS

INTRODUCTION

Data privacy law in the United States is a bewildering assortment of numerous federal and state laws that differ significantly from each other.[1] While many countries have followed the approach of the European Union (EU) by enacting a comprehensive privacy law,[2] the U.S. approach remains highly fragmented, inconsistent, and gap-ridden. Calls for a new direction in U.S. privacy law are becoming more frequent and are emerging from all directions.[3]

Equally as dramatic as the demands for changes to American privacy law, recent years have witnessed a barrage of privacy scandals followed by inconsistent and fragmentary legal responses, including conflicting case law and a tangle of new laws.[4] The privacy scandals alone have occupied numerous news cycles over the last few years. Such scandals include Cambridge Analytica's harvesting of user data on the Facebook platform, and the subsequent microtargeting of political ads that followed during the 2016 presidential election.[5] In response, the Federal

1. For a concise introduction, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 32–40 (7th ed. 2021).
2. *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 772–73 (2019) [hereinafter Schwartz, *Global Data Privacy: The EU Way*].
3. For example, in a speech in Brussels to EU data protection commissioners, Tim Cook, the Chief Executive Officer of Apple, told EU officials, "It is time for the rest of the world—including my home country—to follow your lead." Tim Cook, Chief Executive Officer, Apple, Remarks Before the International Conference of Data Protection & Privacy Commissioners (Oct. 24, 2018) [https://perma.cc/Q5NW-KFNS].
4. In the courts, judges have wrestled with issues such as the meaning of "harm" in privacy cases, the requirements for constitutional standing in data security breach cases, and the clash between the First Amendment and statutory privacy laws. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016) (holding that plaintiffs must show a "concrete harm" to demonstrate the necessary "injury in fact" for standing); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) (holding that the challengers lacked standing because they could not demonstrate a threatened injury that was "certainly impending"); Resnick v. AvMed, Inc., 693 F.3d 1317, 1326–27 (11th Cir. 2012) (holding that plaintiffs sufficiently pleaded injury in fact by alleging a nexus between data breach and subsequent identity theft). On the First Amendment's clash with privacy, see Barr v. Am. Ass'n of Pol. Consultants, 140 S. Ct. 2335 (2020)(holding that the Telephone Consumer Protection Act's exemption for federal debt collection calls violate the First Amendment); Sorrell v. IMS Health, Inc., 564 U.S. 552, 557 (2011) (holding that Vermont's Prescription Confidentiality Law, which restricted the sale of doctors' prescribing practices without consent, violated the First Amendment); Wollschlaeger v. Governor, State of Fla., 848 F.3d 1293, 1301 (11th Cir. 2017) (holding that Florida's Firearm Owners' Privacy Act's recordkeeping, inquiry, and antiharassment provisions unconstitutionally placed speaker-focused and content-based restrictions on speech).
5. *See* Press Release, Fed. Trade Comm'n, FTC Sues Cambridge Analytica, Settles With Former CEO and App Developer (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer

Trade Commission (FTC) levied a record-setting $5 billion penalty in 2019 against Facebook. This amount represents the largest privacy or data security penalty ever imposed in the world.[6]

Although it is hard to believe that the attention on privacy could increase, the policy discussion about privacy has now entered an unprecedented new phase. In 2018, the EU began enforcing the General Data Protection Regulation (GDPR), its comprehensive privacy law.[7] The GDPR—which is hundreds of pages long and enforceable through huge fines—sparked a flurry of worldwide legislative activity on privacy law.[8] Global corporations poured huge sums of money and resources into complying with the GDPR.[9] The GDPR also prompted many to wonder whether the United States would try to keep pace and finally enact a comprehensive federal privacy law.[10]

In 2018, shortly after the GDPR went into effect, California enacted a wide-reaching privacy statute.[11] This law, the California Consumer Protection Act

[https://perma.cc/3D9A-RM23] ("The Federal Trade Commission filed an administrative complaint against data analytics company Cambridge Analytica, and filed settlements for public comment with Cambridge Analytica's former chief executive and an app developer who worked with the company, alleging they employed deceptive tactics to harvest personal information from tens of millions of Facebook users for voter profiling and targeting.").

6. *See* Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 3, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019); *see also* Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/79PG-WS24] ("The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide. It is one of the largest penalties ever assessed by the U.S. government for any violation.").

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

8. *See* Sophie Kwasny, *The GDPR at Two: Expert Perspectives, Shining Like Gold*, INT'L ASS'N OF PRIV. PROS. (2020), https://iapp.org/resources/article/gdpr-at-two-expert-perspectives [https://perma.cc/P8N7-8M6A] (Post-GDPR, there has been "an abundance of new data protection legislations, with more than 10 laws adopted in 2019 on several continents and in 2018, multiple upgrades of existing legislations, such as in Israel, New Zealand, and many EU countries obviously, as well as completely new laws in Brazil and the state of California in the U.S.").

9. For example, then U.S. Secretary of Commerce Wilbur Ross stated that companies in the United States alone "have already invested billions of dollars to comply with the new rules" of the GDPR. Wilbur Ross, Opinion, *EU Data Privacy Laws Are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c [https://perma.cc/G7WU-YHRM].

10. Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734–35 (2021).

11. California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1.81.5 (2020).

(CCPA), took effect on January 1, 2020.[12] The CCPA has kicked off a flurry of domestic legislative activity, with several states having passed laws and other states having introduced bills.[13] California enacted a major amendment to the CCPA with the California Privacy Rights Act, a state-wide referendum.[14]

Perhaps in reaction to the GDPR and this statewide activity in the United States, industry has started clamoring for a comprehensive federal privacy law after long having been opposed to the idea.[15] An unprecedented number of companies have urged Congress to pass a federal privacy law.[16] Even the U.S. Chamber of Commerce has changed its position and is now calling for such a law.[17]

12. The CCPA has continued to elicit a wide range of reactions, positive and negative, from regulators, practitioners, and academics. While many privacy advocates and academics welcome the CCPA, this reaction has not been shared by all. *See* Letter From Professor Eric Goldman on Behalf of 41 California Privacy Experts to the California Legislature Regarding the California Consumer Privacy Act (Jan. 17, 2019), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2886&context=historical [https://perma.cc/Z4TN-WAHA] (highlighting six areas of concern within the statute including its application to stakeholders who did not provide input; compliance costs for small businesses; inconsistencies with the GDPR; unintentional undermining of consumer privacy; overbroad definitions; and extraterritorial reach). In contrast, the Attorney General of California was an enthusiastic supporter of the statute. *See* Press Release, Cal. Dep't of Just., Attorney General Becerra Issues Advisory Outlining New Data Privacy Rights for California Consumers (Jan. 6, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-advisory-outlining-new-data-privacy-rights [https://perma.cc/TT3L-JZGR] ("'Knowledge is power, and in today's world knowledge is derived from data. When it comes to your own data, you should be in control,' said [then] Attorney General Becerra. 'In California we are rebalancing the power dynamic by putting power back in the hands of consumers.'").

13. *2021 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES, (Dec. 27, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx [https://perma.cc/QS2X-YTG5] ("Overall, at least 13 states in 2021 enacted 17 consumer data privacy bills . . . . [C]omprehensive privacy legislation was introduced in at least 25 states, and two states, Colorado and Virginia, followed California by enacting comprehensive consumer data privacy legislation. . . .").

14. For the official text of the referendum, see Submission of Amendments to the California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021 (Nov. 4, 2019), at https://iapp.org/media/pdf/resource_center/ca_privacy_rights_act_2020_ballot_initiative.pdf [https://perma.cc/NJT5-YAE4]. For the codified Act, see CAL. CIV. CODE §§ 1798.100–199.100, at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 [https://perma.cc/5L55-LEZD].

15. David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018, 3:30 AM), https://fortune.com/2018/11/29/federal-data-privacy-law [https://perma.cc/WH7D-CAE6].

16. Nicole Lindsey, *Top CEOs Now Pushing for Federal Privacy Legislation*, CPO MAG. (Sept. 23, 2019), https://www.cpomagazine.com/data-privacy/top-ceos-now-pushing-for-federal-privacy-legislation [https://perma.cc/A3JA-2J6B].

17. Press Release, U.S. Chamber of Com., U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law (Feb. 13, 2019),

The conversation about comprehensive privacy statutes has never been more robust than it is at this very moment.

All in all, there is a multifaceted legal response underway to the "age of surveillance capitalism." Shoshana Zuboff uses this term to describe how vast quantities of people's personal data has been digitalized and turned into fuel for corporate profit.[18] Yet the path forward remains murky. Is there a meaningful and practical way for U.S. privacy law to advance? Can U.S. privacy law become more consistent with the law of the EU without making a radical break from its foundations? What approach should the long-delayed federal privacy law take?

It is because these questions are so difficult to answer and because finding a resolution to them is so important that the American Law Institute (ALI) developed a project devoted to articulating twenty-first century concepts of privacy law, namely, the *Principles of Law, Data Privacy* (the *Principles*). We had the privilege of serving as the Reporters for this project. The ALI's mission is "to promote the clarification and simplification of the law and its better adaptation to social needs, to secure the better administration of justice, and to encourage and carry on scholarly and scientific legal work."[19] The ALI has produced a remarkable number of projects that have exercised profound influence on the law, such as the Uniform Commercial Code, the Model Penal Code, and various Restatements of the Law, including the celebrated Restatement (Second) of Torts.

Prior to these *Principles*, the ALI's only foray into privacy was the short section in the Restatement (Second) of Torts establishing the four privacy torts in 1977.[20] These four torts have not proven well-suited to contemporary privacy problems involving organizations collecting and using vast amounts of personal data.[21] With the *Principles*, the ALI has finally weighed in on contemporary privacy laws and practices.

The ALI categorizes this project as a "Principles" project. Thus, it is "primarily addressed to legislatures, administrative agencies, or private actors" as well as "to courts when an area is so new that there is little established law."[22] Accordingly, the *Principles* seeks to provide guidance for the evolution of U.S. data

https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law [https://perma.cc/9U24-QD8F].

18. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 8 (2019).
19. *How the Institute Works*, AM. L. INST., https://www.ali.org/about-ali/how-institute-works [https://perma.cc/FR7F-2T9M].
20. RESTATEMENT (SECOND) OF TORTS § 652 (AM. L. INST. 1977).
21. For criticisms of the privacy torts, see Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007 (2010); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).
22. *How the Institute Works*, *supra* note 19.

privacy law toward a more comprehensive and coherent approach. The ALI approved these *Principles* in May 2019 following a seven-year process.[23]

Data privacy law, sometimes referred to as information privacy law, concerns the collection, use, and disclosure of personal data.[24] The last few decades have witnessed a torrent of legislative, regulatory, and judicial activity regarding data privacy around the world. At present, 132 countries have privacy laws.[25] According to Graham Greenleaf, who tracks these developments, "Fifty countries have enact[ed] new data privacy laws in the first nine years of this decade, an average of 5.5 per year."[26] Among the 231 countries surveyed by Greenleaf, about 57 percent now have data privacy laws.[27]

U.S. data privacy law remains an outlier among regulatory approaches around the world. The vast majority of countries have a comprehensive privacy law modeled after EU law. The EU initially approached data privacy law with the Data Protection Directive of 1995 (the Directive).[28] The Directive established standards for information privacy and mandated that each member nation adopt a comprehensive privacy law according to its requirements.[29] In 2016, about twenty years later, the EU passed the GDPR in an attempt to better harmonize the law of EU member nations and to update its law.[30]

The Directive and its successor, the GDPR, have greatly influenced other national approaches to data privacy.[31] In fact, most countries have enacted laws closer to the EU approach than to the U.S. approach. In Greenleaf's judgment, "[S]omething reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws."[32] The divergence between U.S. and EU privacy law has led to significant problems for

23. The *Principles of Law, Data Privacy* (the *Principles*) were created not just by us, but also by our advisory group and many American Law Institute (ALI) members who contributed greatly to this project. The ALI process is a wonderful one—a thoughtful constructive discussion about how to craft meaningful regulation between practitioners, judges, and academics, among others.
24. For a discussion of the different nomenclature used in this area of law, see Schwartz, *Global Data Privacy: The EU Way*, *supra* note 2, at 775.
25. Graham Greenleaf, *Global Data Privacy Laws 2019: 132 National Laws & Many Bills*, 157 PRIV. L. & BUS. INT'L REP. 14 (2019).
26. *Id.*
27. *Id.*
28. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive].
29. *Id.*
30. GDPR, *supra* note 7.
31. Schwartz, *Global Data Privacy: The EU Way*, *supra* note 2, at 772–73.
32. Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIV. L. 68, 77 (2012).

smooth transborder data flows and efficient commerce between EU member nations and the United States.[33]

Currently, U.S. privacy law is unwieldy and conflicting. This area of U.S. law has led many foreign nations to discount the protections that *do* exist in the United States. Moreover, new laws continue to emerge in many states, which further contribute to the vast quilt of inconsistent laws.[34] There also remains significant skepticism that a meaningful compromise can be reached on a comprehensive federal law, as well as strong doubts that U.S. privacy law can ever be brought into harmony with the GDPR.[35]

Despite the prevalence of this skepticism, we contend that it is possible to craft a comprehensive approach to data privacy for the United States that bridges its divide with the EU. The true proof of our thesis is the *Principles* itself, which we publish as part of this Article. As Reporters on the *Principles*, we faced choices about many challenging and contentious privacy issues. This Article provides an overview of the approaches and solutions in the *Principles* to these issues, and it explains why we opted for the chosen direction. We then present the text of the *Principles*.

The primary contribution of the *Principles* is to attempt to revitalize the application of the Fair Information Practice Principles (FIPPs) in U.S. privacy law. The FIPPs are a set of general principles about both the rights that people should have with their personal data and the responsibilities of those organizations that collect, use, and disclose that data. In U.S. privacy law, the FIPPs have been

33. EU data privacy law has long required that before personal data about persons in the EU can be transferred to other countries, those countries must have an "adequate level of protection." Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 118 (2017). The EU has not found the United States to have an adequate level of protection. In a nonbinding opinion in 1999, the EU's Article 29 Working Party argued that the United States lacked adequate protection for personal data. *Opinion of the Working Party Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government*, at 2, 5092/98/EN final (Jan. 26, 1999). As a result, more cumbersome data transfer mechanisms must be used, such as Standard Contractual Clauses, or the Binding Corporate Rules. For an overview, see SOLOVE & SCHWARTZ, *supra* note 1, at 1173–1203.

34. *See* Matt Dumiak, *Introducing State Privacy Legislation Amidst National Privacy Law Discussions*, SC MEDIA (May 21, 2019), https://web.archive.org/web/20190807002408/https://www.scmagazine.com/home/opinion/executive-insight/introducing-state-privacy-legislation-amidst-national-privacy-law-discussions [https://perma.cc/KXC5-TYCL]; Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. (forthcoming 2022) ("[F]or Europeans the GDPR is a state of mind. And . . . a US version of the GDPR would inevitably be both a weak and inadequate version of the real GDPR.").

35. *See* John Hendel, *"Embarrassing": Congress Stumbles in Push for a Consumer Privacy Law*, POLITICO (July 12, 2019, 8:05 PM), https://www.politico.com/story/2019/07/12/congress-consumer-privacy-bill-1582540 [https://perma.cc/7KSF-Q6PW].

implemented largely through what has become known as the notice-and-choice approach.[36] Under notice-and-choice, organizations provide a statement about their privacy practices (notice), and individuals then can exercise some form of choice about their data (often to opt out of certain uses or transfers).[37] Numerous commentators have pointed out that notice-and-choice has been ineffective; many call it an outright failure.[38] Most people do not read privacy notices, do not understand the notices, and are not provided with meaningful choices.[39] So far, the FIPPs have not led to an effective privacy regulatory regime in the United States.[40]

The *Principles* seek to breathe new life into the FIPPs. The FIPPs ought not to be abandoned and can be an effective part of a privacy regulatory regime. The *Principles* also seek to build upon the U.S. approach to privacy regulation rather than break from it. Although the GDPR is the strongest and most comprehensive privacy law in the world, attempting to enact the GDPR in the United States would be impractical. Applying the EU regulatory approach directly to the United States would conflict with too much existing law, be incompatible with certain entrenched American values, and clash with the First Amendment. Instead, the *Principles* attempt to avoid a radical shift away from the U.S. approach. The *Principles* aim to be consistent with U.S. privacy law yet advance it boldly. In particular, the *Principles* revitalize notice to make it effective and meaningful, and they do so in a unique way that no other law has done thus far. The *Principles* chart a new direction in applying the FIPPs to personal data, using a risk-based approach to identification.

The *Principles* also both incorporate certain EU approaches and, where necessary, modify them to fit with the core commitments of U.S. law. We identified these commitments by studying formulations of the FIPPs in different laws, guidelines, and regulations. From this exercise, we sought to incorporate the

36. See *infra* Subpart II.B.1 for additional discussion regarding notice-and-choice; *see also* Schwartz & Peifer, *supra* note 33, at 136–37, for a critical account of notice-and-choice.

37. *See* Schwartz & Peifer, *supra* note 33, at 136–37.

38. *See, e.g.*, CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 365 (2016) ("[T]he notice-and-consent regime is a rigged game, guaranteed to result in companies getting the data they want with no guarantees against transgressive uses of it."); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821–23 (2000) (noting multiple reasons for the failure of "self-reliant consent" for privacy on the Internet). Regarding the shortcomings of "mandated disclosures" in a variety of settings, see OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 10 (2014).

39. On the reliance on ineffective "idealized consent," see Schwartz & Peifer, *supra* note 33, at 149–50.

40. *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 952–53 (2017).

central parts of the FIPPS into our *Principles*. Additionally, the *Principles* seek to provide flexibility in the law, avoiding the rigidity of other regulatory approaches. In short, the *Principles* aim to achieve a delicate balancing act, avoiding a radical break with U.S. law while trying to improve it aggressively and creatively.

In this Article, we discuss the approaches taken by the *Principles* on the key issues involving the regulation of data privacy, and we explain the rationales behind these approaches. Part I provides an overview of the general goals and approach of the *Principles*. In Part II, we offer a section by section overview of the *Principles*. Here, we highlight the most notable elements of each section and discuss our choices as well as trade-offs among alternatives. Part III sets out a brief conclusion, and Part IV contains the full black letter text of the *Principles*.

I. THE GOALS AND APPROACH OF THE ALI PRINCIPLES OF LAW, DATA PRIVACY

A. The Origins of the Project

The ALI started this project in the summer of 2012 because of a void in U.S. data privacy law. Courts, legislatures, and policymakers were struggling to understand concepts such as personal identifiable information, the nature of privacy harms, the elements of meaningful consent for data collection, and the duties that should be owed a person whose personal information is processed.[41] Consistency and comprehensiveness were also sorely lacking.

As the selected Reporters for that then-inchoate ALI privacy project, we proposed more than a dozen possible topics and provided background on each. On September 28, 2012, we held our first meeting about this project in San Francisco. On that day, we led a discussion with a remarkable array of experts. Among the thirty-five attendees were judges from federal and state courts; an FTC commissioner and the FTC director of a key division for privacy regulation; advocates from privacy NGOs; chief privacy officials and lawyers from a number of prominent information technology companies, including entities based in Silicon Valley; and attorneys specializing in privacy at law firms. Also in

41. On the complexity of defining "personal identifiable information," see Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011) [hereinafter Schwartz & Solove, *The PII Problem*]. The current debate about privacy harms is explored in Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 737–38 (2018). Finally, regarding consent and duties for data processors, see Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–82 (2013) [hereinafter Solove, *Introduction: Privacy Self-Management*].

attendance was a former general counsel for the National Security Agency and a prominent Assistant U.S. Attorney. Finally, the discussion benefited from the participation of numerous academic experts in this field, including the then-Dean of Yale Law School.[42]

This meeting produced a consensus that U.S. law would benefit from significant guidance about data privacy, and that a wide-ranging project to that end by the ALI would be valuable. We therefore developed a new project to address the most important and vexing privacy problem of the twenty-first century: the vast collection, use, and disclosure of personal data by a wide array of entities. There was also widespread agreement that we should break new ground for the ALI, and tackle issues that specifically relate to data processing and information use. The focus of our project was squarely on issues relating to the modern collection and processing of digitalized personal data. As for the section of the Restatement (Second) of Torts devoted to the privacy torts, we decided that while it would benefit from revision, this endeavor did not fit well within a proposed project about data privacy. The modernization of the privacy torts and the related topic of defamation did finally become the subject of a distinct ALI project in 2019.[43]

The *Principles* are not an attempt to write our ideal privacy law as if drafting on a blank slate, nor are they an attempt to restate existing law. The *Principles* are something in between. We build on foundations in existing law, seek fidelity to U.S. privacy law foundations, and attempt to advance the law progressively without clashing with core commitments or introducing concepts that are without precedent.

B. The Fair Information Practice Principles (FIPPs)

We began by organizing the project around key Fair Information Practice Principles (FIPPs).[44] The FIPPs are a set of principles about the responsibilities and obligations entities bear when collecting and using

42. For a list of participants, see The American Law Institute, Invitational Conference on Informational Privacy Law (Sept. 28, 2012) (on file with authors).

43. In 2019, as we were concluding our project, the ALI began such a torts project. Led by Lyrissa Lidsky (University of Missouri-Columbus School of Law) and Robert Post (Yale Law School), this project will complete the Restatement (Third) of Torts; it looks at defamation and privacy. *Restatement of the Law Third, Torts: Defamation and Privacy*, AM. L. INST., https://www.ali.org/projects/show/torts-defamation-and-privacy/#_participants [https://perma.cc/5MAN-F9RQ].

44. FIPPs are sometimes also referred to as Fair Information Practices (FIPs).

personal data.[45] They also provide the rights that people should have regarding their data.[46] As early as 1973, the U.S. Department of Health, Education, and Welfare articulated a set of FIPPs.[47] The FIPPs have been restated and expanded many times. The Organisation for Economic Co-operation and Development (OECD) Guidelines of 1980 (updated in 2013) have developed the most widely used set of FIPPs in world regulation.[48] The EU Data Protection Directive and GDPR are grounded on the FIPPs, as is the Asian-Pacific Economic Cooperation Privacy Framework of 2004.[49] Nearly every privacy statute rests on one or another of these articulations of the FIPPs.

The FIPPs form the backbone of privacy law worldwide. Yet there is no single set of FIPPs on which all parties agree, and privacy laws operationalizing them diverge significantly in effectiveness and scope. The FIPPs are also open-ended; they are but a skeleton, and meaningful regulation requires more detail. Moreover, a scaled-down version of the FIPPs have often been embodied in U.S. laws: namely, the notice-and-choice approach. As a consequence of the accepted, watered-down versions of the FIPPs in the United States, many scholars have criticized the FIPPs approach to protecting privacy as inadequate.[50] One of us has critiqued this approach as being based on privacy policies that are incomprehensible to most people.[51] The other has argued that the approach fails because people cannot self-manage their privacy: it is too vast and time-consuming to do, and too complicated to assess

45. For example, the influential formulation of FIPPs by the Privacy Protection Study Commission in 1977 required data processing organizations to be open about their practices, to have limits on the types of information that they could collect, to restrict their internal and external uses of information, and to be accountable for their personal data record-keeping practices. PRIV. PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 501–02 (1977), https://www.ojp.gov/pdffiles1/Digitization/49602NCJRS.pdf [https://perma.cc/BH96-CQ2E].

46. The Privacy Protection Study Commission also called for individuals to have a right to access information held about them and to correct or amend the substance of their records. *Id.*

47. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41–42 (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/K9LP-UZT6].

48. *See* ORG. FOR ECON. COOP. & DEV., THE OECD PRIVACY FRAMEWORK 74–81 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/R5HN-TXZJ].

49. GDPR, *supra* note 7; ASIA-PAC. ECON. COOP., APEC PRIVACY FRAMEWORK (2004); Directive, *supra* note 28.

50. *See, e.g.*, Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1702–05 (2020); Hartzog, *supra* note 40, at 959; Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343 (Jane K. Winn ed., 2006).

51. Schwartz & Peifer, *supra* note 33, at 149–50.

the costs and benefits of making choices about how and when to share their data.[52]

In our view, the ultimate problem with existing data privacy law is not with the FIPPs; rather, it is in implementing them through what one of us has called privacy self-management.[53] Although the FIPPs have certain components that involve privacy self-management, the FIPPs also contain accountability principles that place obligations on organizational uses of personal data. Moreover, the FIPPs already form the foundation of much privacy law, and as a consequence, they represented the best place to focus the ALI project. What is needed—and what the *Principles* aim to supply—is sufficient guidance to bring more substance, uniformity, and clarity to the law. Beyond the FIPPs, we drew upon countless privacy laws, regulations, enforcement actions, and cases for ideas and approaches.

Our aim in the *Principles* was to demonstrate how U.S. privacy law can maintain its essential character, build upon existing foundations, and come closer to the world's most important privacy benchmark, the GDPR. The *Principles* reflect our judgment about how far U.S. law can be pushed within the ALI process, which requires approval first by a group of senior advisors, then the Council, and finally by Members as a whole. It is an interesting question as to whether we could have pushed further in one direction or another. We welcome this discussion as privacy law is a constantly evolving area of law. We hope that the *Principles* contribute to this evolution as other ALI projects have done in their respective fields.

II. AN OVERVIEW OF THE *PRINCIPLES*

Our goal is to advance U.S. privacy law significantly while maintaining fidelity to its foundations. In our view, the *Principles* are a step forward that will be useful to legislatures working on privacy statutes, to policymakers evaluating tradeoffs in this area, and to everyone who is concerned about privacy law. Regarding the international dimensions of the project, we found that the GDPR could not merely be transferred to the United States. There are some fundamental differences that make reaching consensus about certain elements of the GDPR difficult or that even make it incompatible with existing U.S. law. Nonetheless, in certain elements of the *Principles*, we were able to find ways to bridge differences between the United States and EU approaches.

52. *See* Solove, *Introduction: Privacy Self-Management*, *supra* note 41, at 1884–86.
53. *Id.* at 1895.

A. Chapter 1: Purpose, Scope, and Definitions

1. Section 1: Purpose and Scope of the Data Privacy Principles

The *Principles* are designed to cover organizational activities rather than personal ones. We thus focus on "the sale and provision of goods or services" and "the functioning of institutions and organizations . . . including the employment of persons."[54] The *Principles* explicitly exclude personal-data activities involving, or intended to involve, purely interpersonal or household relationships and personal activities. Otherwise, a person's contact list, information that parents maintain about their children, or anything about other individuals that people write in their diaries would be covered by the *Principles*. As we note, such situations are "ill-suited for the responsibilities assigned to the data user in these Principles—such as providing notice and access—and for the rights provided to individuals in these Principles. Tort law and sometimes even criminal law are better at dealing with these situations."[55]

Also excluded from the *Principles* are "intelligence and law enforcement" activities and activities relating to "the administration of the judicial system" because these areas raise significantly different issues from those of businesses and other governmental organizations.[56] Intelligence and law-enforcement activities are carried out as part of the protection of the nation's international and domestic security interests. As for the judicial system in the United States, it has a strong tradition of permitting public access to proceedings and court records. Nevertheless, certain provisions in the *Principles* can apply to these entities, and we encourage law enforcement entities and the judicial system to follow the *Principles* when possible.

Finally, we included two exceptions to address potential conflicts with the First Amendment.[57] This part of the project was among the thorniest in terms of competing goals and complex questions regarding draftsmanship. The language of the exceptions had to reflect current constitutional law, but also be open-ended enough to avoid becoming obsolete due to future U.S. Supreme Court decisions protecting free speech. As an indication of the sensitivity of the free speech issues implicated by the *Principles*, the discussions about and editing of this subsection

54. PRINCIPLES OF THE LAW, DATA PRIVACY § 1(b)(1)(A–B) (A.L.I. 2020).
55. *Id.* § 1 cmt. (f).
56. *Id.* § 1(b)(2)(C–D). A further explication of these different issues can also be found in *United States v. United States District Court* (*Keith*), in which the U.S. Supreme Court noted the special issues related to electronic surveillance in internal security matters. United States v. United States District Court, 407 U.S. 297, 321–23 (1972).
57. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 1(b)(2)(E–F).

continued even during the morning of May 22, 2019, the date of the final vote on the project.

2. Section 2: Definitions

An important goal for this project is to achieve greater consistency between U.S. privacy law and privacy law around the world. Accordingly, we use much of the same terminology as the GDPR, including *data subjects*, *data controllers*, and *data processors*. The United States lacks consistent terminology in its law relating to these concepts, but it also has statutes and regulations with similar ideas. We also use the EU terminology because the GDPR has made these EU terms widely known in the United States.[58] Additionally, using the same terminology better harmonizes U.S. and EU privacy law, as well as U.S. law and laws of other nations. Here is one of the areas where we were able to build a link between concepts found in both the United States and the EU.

We also use the term *personal data* for the type of information covered by the *Principles*. We use the term personal data in order to harmonize to the greatest extent possible U.S. law with privacy law worldwide. The definition of personal data fixes the scope and boundaries of privacy statutes and regulations because all privacy laws are limited to covering personal data rather than reaching information itself. Otherwise, these laws would regulate everything ever said or written, including nearly infinite arrays of information.[59]

The term personal data is used in the GDPR as well as in its predecessor, the EU Data Protection Directive.[60] In U.S. law, various terms have been used to refer to the personal data covered by privacy laws: customer proprietary network information (CPNI) in telecommunications laws;[61] protected health information (PHI) in the Health Insurance Portability and Accountability Act;[62] education records in the Family Educational Rights and Privacy Act;[63] and so on, including at times the term personal data.[64] Generally, the terms *personal information* or *personally identifiable information (PII)* are used in the United States.[65]

58. Schwartz, *Global Data Privacy: The EU Way*, *supra* note 2, at 813–17.
59. Schwartz & Solove, *The PII Problem*, *supra* note 41, at 1866.
60. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 882–86 (2014) [hereinafter Schwartz & Solove, *Reconciling Personal Information*].
61. 47 U.S.C. § 222.
62. 45 C.F.R. § 160.103 (2021).
63. 20 U.S.C. § 1232; 45 C.F.R § 160.103.
64. Schwartz & Solove, *Reconciling Personal Information*, *supra* note 60, at 887–90.
65. *See id.* at 887.

Beyond issues of nomenclature, the definition of personal data is also one that lacks uniformity in U.S. privacy statutes and regulations. In many U.S. privacy laws, definitions of PII or personal data focus primarily on data that identifies an individual. In contrast, personal data is defined in the EU as data that relates to an identified or identifiable individual.[66] Identifiable means that an individual might not currently be identified but could be identified by combining various pieces of data.[67] For example, an IP address often does not identify an individual, but sometimes can be readily linked to a person with additional data. Thus, under EU law, IP addresses are identifiable to individuals.[68]

Although the term PII includes the word identifiable, in definition and practice, many U.S. privacy laws do not extend to data that are identifiable but do not yet relate to an identified person. In the last decade, however, the concept of identifiable data has been taking root in the United States. As an example, in its 2012 report, *Protecting Privacy in an Era of Rapid Change*, the FTC stated that its proposed framework applies to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."[69] The report stated that "the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data's privacy implications."[70] Newer privacy laws such as California's CCPA use a definition that includes identifiable data.[71] Thus, the clear trend and contemporary approach is to define personal data to include identifiable data, and we have done so. The *Principles* define personal data as "any data that is identified

66. *Id.* at 885–86.
67. *Id.* at 886.
68. For example, the European Court of Justice (CJEU) has found that IP addresses are "personal data" under certain circumstances. *See* Case C-582/14, Patrick Breyer v. Fed. Ct. of Just., Ger., para. 39, (2016) http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945 [https://perma.cc/RHS6-8XLT] (holding a dynamic IP address may be identifiable data depending on whether "the additional data necessary in order to identify the user of a website that the services provider makes accessible to the public are held by that user's internet service provider"); Joined Cases C-293/12 and C-594/12, Digit. Rts. Ir. v. Minister for Commc'ns, para. 26, (2014), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&from=EN [https://perma.cc/T3XE-YYQY] (holding data necessary to trace and identify the source of a communication, such as an IP address, implicates the constitutional rights of privacy under the Charter of Human Rights of the EU).
69. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 15 (2012).
70. *Id.* at 19.
71. CAL. CIV. CODE § 1798.140(o)(1) (West 2020). For a discussion, see LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY U.S. FEDERAL AND CALIFORNIA LAW 64–65 (4th ed. 2020).

or identifiable to a specific living individual."[72] This definition is similar to that of the GDPR.

We diverge from the GDPR in one key respect. Under the GDPR, identified and identifiable data are treated the same. The *Principles* treats these categories of personal data differently: "When data is identifiable, it is personal data under the Data Privacy Principles and is subject to some of the Principles but exempt from others."[73] We took this approach because some privacy principles are not as relevant to and do not work well with identifiable data. As we noted in a comment:

> Certain Data Privacy Principles are not relevant or helpful when personal data falls into the identifiable category; indeed, certain Data Privacy Principles might undermine the privacy protection of such personal data by requiring personal data to be identified to comply with the Principles. For example, providing individuals with access . . . rights to their personal data requires that the data be identified to them. Thus, the Data Privacy Principles encourage that data be kept in identifiable form, rather than identified form, when possible. Regulating identified and identifiable data the same way not only removes any incentive to avoid keeping data in identified form, but also, arguably, forces the maintaining of data in the state of being identified.[74]

Our approach encourages organizations to avoid maintaining personal data in identified form. This strategy contrasts with privacy laws that would force organizations to identify personal data in order to administer privacy rights. That approach is counterproductive, as it will increase rather than limit the possible threat to individual privacy.

B. Chapter 2: Data Privacy Principles

1. Section 3: Transparency Statement

Countless privacy laws require entities to have a privacy policy or notice which explains to individuals the personal data that the entity collects and how it uses and shares that data.[75] This perspective emerged in the mid-1990s in the United States when the modern commercial Internet was developing. U.S. privacy

72. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 2(b).
73. *Id.* § 2(b)(2).
74. *Id.* § 2 cmt. (c). For a further elaboration of this rationale, see Schwartz & Solove, *The PII Problem, supra* note 41, at 1880.
75. For a discussion of this trend, see Schwartz & Peifer, *supra* note 33, at 148–50.

law coalesced around this standpoint, which became known as the notice-and-choice approach.

Two foundational concepts underpin notice-and-choice. The first idea is that this approach is significantly self-regulatory. Organizations define their own rules for how they will collect, use, and share data.[76] Organizations are the ones that decide the choices given to people.[77] Consistent with this perspective, entities have significant freedom concerning their data processing. The main limitation on data processing is to adhere to what the entities declare about their practices in the notice. The second dimension of notice-and-choice is what one of us terms privacy self-management.[78] The onus is placed on individuals to manage their own privacy by reading notices and making choices. As the FTC, America's leading regulator of information privacy, has stated, the goals of notice-and-choice are to "[m]ake information collection and use practices transparent" and to provide people with "the ability to make decisions about their data at a relevant time and context."[79]

The problems with the notice-and-choice approach are legion and the approach has been extensively criticized. Hardly anyone actually reads privacy notices.[80] And the few people who actually try to read privacy notices struggle to comprehend their long dense legalistic prose.[81] The choices that people can exercise in response to reading privacy policies are also severely limited.[82] Privacy self-management does not scale: People lack the time to review the privacy notices of every organization with which they interact.[83] Moreover, people lack the knowledge to make meaningful cost-benefit decisions involving their data.[84]

The EU's GDPR largely rejects the notice-and-choice approach, though elements of this approach can still be found in it in some form.[85] The GDPR's general approach, however, is different from notice-and-choice. It relies on the

76. For a discussion of how "the information industry has entrenched practices" determinative of privacy, see Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV (forthcoming 2022).
77. ARI EZRA WALDMAN, INDUSTRY UNBOUND (2021).
78. Solove, *Introduction: Privacy Self-Management*, *supra* note 41, at 1880–82.
79. FED. TRADE COMM'N, *supra* note 69, at i.
80. *See* Florian Schaub, Rebecca Balebako & Lorrie Faith Cranor, *Designing Effective Privacy Notices and Controls*, 21 IEEE INTERNET COMPUTING 70, 72 (2017).
81. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230–32 (2002).
82. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).
83. Solove, *Introduction: Privacy Self-Management*, *supra* note 41, at 1888–89.
84. *See id.* at 1897.
85. Schwartz & Peifer, *supra* note 33, at 142–44.

assignment of strong rights to its data subjects and the creation of independent regulatory authorities with enforcement powers.[86]

Although both of us have strongly criticized the notice-and-choice approach, we concluded that moving away from it entirely would be too drastic a paradigm shift for U.S. privacy law and would likely undermine the reception of the *Principles* in the United States. We therefore introduce several innovations aimed at correcting some critical defects of notice-and-choice. Perhaps the most important of these innovations is to bifurcate notice into two separate statements. We drew this distinction because the current approach with privacy notices seeks to achieve two goals that are in tension with each other: (1) to inform people about how their data is used and shared; and (2) to enable regulators, policymakers, and experts to determine whether an organization's practices are appropriate and whether the organization is following the promises in their notices.[87] The tension between these goals arises because many nonexpert individuals can only comprehend and digest short and simple privacy notices. Such brevity and simplicity will often omit the details that regulators, policymakers, and experts need to evaluate what the organization is doing.

The "fundamental dilemma of notice" is a choice between either "making it simple and easy to understand" or "fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful."[88] We separated transparency and individual notice because these two processes have different purposes, which are not consistent with each other. The transparency notice of Section 3 of the *Principles* aims to provide sufficient information for organizations to be accountable to regulators, policymakers, and experts. It requires that data controllers and data processers "clearly, conspicuously, and accurately explain the data controller's or data processor's current personal data activities."[89]

2. Section 4: Individual Notice

Standing alone from the transparency statement, the individual notice requirement of the *Principles* seeks to inform individuals about how their personal data is being collected, used, and shared. Individual notice traditionally has

86. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1976 (2013) [hereinafter Schwartz, *The EU-U.S. Privacy Collision*].
87. For a discussion, see PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 3 cmt. a.
88. Solove, *Introduction: Privacy Self-Management*, *supra* note 41, at 1885.
89. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 3(b)(1).

struggled to work effectively for the reasons we describe above. We thus attempt to improve how individual notice works.

To make individual notice more meaningful, the *Principles* create two levels of notice—ordinary notice and heightened notice. The idea behind heightened notice is that notice is most necessary when the collection, use, or disclosure of personal data is potentially harmful to people or is significantly outside the norm.[90] The *Principles* provide that heightened notice "shall be made more prominently than ordinary notice and closer in time to the particular data activity."[91] The *Principles* define the trigger for heightened notice as follows:

> For any data activity that is significantly unexpected or that poses a significant risk of causing material harm to a data subject, the data controller should provide reasonable "heightened notice" to the data subject. A significantly unexpected data activity is one that a reasonable person would not expect based on the context of the personal data activities. . . . A significant risk may exist with a low likelihood of a high-magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of heightened notice.[92]

Heightened notice should be more conspicuous, such as a pop up that appears at the moment a data activity is about to occur.[93]

The timing and method of heightened notice make it more relevant to individuals, pointing out when they should be paying most attention. Otherwise, important information about privacy will be drowned out in the oceans of privacy notices through which consumers must sift. Heightened notice serves to lower the information burdens of mandated privacy disclosures. As Omri Ben-Shahar and Carl Schneider have noted, "[P]eople strip [information] away to make choices manageable."[94] Moreover, the privacy practices of many organizations are quite similar in many respects, and basic norms of data processing have emerged. As a result, individuals are best informed when there are practices outside the norm or practices that could potentially harm them.[95]

---

90. *See, e.g.*, *id.* § 4 cmt. d.
91. *Id.* § 4(e)(6).
92. *Id.* § 4(e)(1)–(3).
93. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2012) (arguing that policymakers should use "innovative new ways to deliver privacy notice" and that privacy notice should be made in a more "visceral" way).
94. BEN-SHAHAR & SCHNEIDER, *supra* note 38, at 10.
95. For an FTC privacy enforcement action that points in this direction, see Complaint, *In re* Sears Holdings Mgmt. Corp., No. C-4264 (2009), https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf [https://perma.cc/2XY9-BBTR]. *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*,

In our review of privacy law, we have not found a requirement of heightened notice akin to the one we propose. A number of laws require that regular notice be conspicuous, but this typically involves only including a prominent link on a website's homepage.[96] The heightened notice in the *Principles* goes far beyond conspicuous regular notice. Heightened notice aims to call out instances where people should pay special attention to privacy practices that are outside of the norm and that could be potentially harmful. Heightened notice also aims to notify people at the most appropriate time. These innovations strive to address the problem of people not reading notices and of people having to wade through dense prose to figure out what is relevant to know. The U.S. approach to privacy depends upon meaningful notice; the *Principles* endeavor to chart a path forward by making that notice more effective. The alternative is to move away from notice, which we believe would be too radical a shift from current U.S. law.

Combined with the transparency statement, the notice requirements of the *Principles* lead to a tripartite structure: (1) a transparency statement aimed for accountability purposes, to be used by regulators, public-interest organizations, and experts; (2) a regular individual notice that describes privacy practices in a way that individuals can understand; and (3) heightened notice that points out to individuals, at the relevant time, when there are privacy practices that are unexpected or when there is a significant risk of harm.

3. Section 5: Consent

A core element of privacy laws is consent. In the United States, an emphasis on notice is also accompanied by a strong reliance on the affected party's consent to data processing.[97] The OECD's FIPPs and the EU's GDPR likewise contain a concept of consent.[98] As a general matter, however, the United States relies far

114 COLUM. L. REV. 583, 634–36 (2014); Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 5 (2009).

96. CalOPPA, the California Online Privacy Protection Act, led the way in 2004 by requiring the conspicuous posting of privacy policies by commercial websites and online services. CAL. BUS. & PROF. CODE § 22575 (West 2014). For a similar requirement proposed in New York for ad networks and publishers, see N.Y. State Assemb., A03818 (N.Y. 2019).

97. *See, e.g.*, the Privacy Act, which prohibits the disclosure of records without the "consent" of the individual, 5 U.S.C. § 552a(b), and the Health Insurance Portability and Accountability Act (HIPAA) and its requirement of patient "authorization" before release of protected health data, 45 C.F.R. § 164.508(a)(1).

98. *See* ORG. FOR ECON. COOP. & DEV., *supra* note 48, at 14 ("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."); GDPR, *supra* note 7, at art.

more heavily on the data subject's agreement to justify data processing than the EU does.[99]

In the United States, there are divergent approaches to consent. One common approach is to view people's failure to opt out of various forms of data activities as a form of consent.[100] In contrast, other U.S. laws require people to affirmatively opt in to a data activity.[101] The GDPR's approach to consent is to require affirmative consent—equivalent to opt in.[102] Opt out is not valid consent under the GDPR.[103] As for opt out under U.S. law, where the law sometimes permits it, this approach is problematic because people often do not read or understand privacy notices.[104]

Nevertheless, we avoided the radical step of taking a clean sweep to the messy approach to consent in U.S. privacy law. The *Principles* do not embrace either opt out or opt in; instead, consent is left deliberately open-ended so the standard can evolve situationally and contextually. The *Principles* provide that the "form by which consent is obtained must be reasonable under the circumstances, based on the type of personal data involved, the nature of the personal data activity, and the understandings of a reasonable data subject."[105]

In at least one way, however, we have tightened up consent. According to the *Principles*:

> In situations in which heightened notice is required pursuant to Principle 4(e), only clear and affirmative consent shall suffice for valid consent. Clear and affirmative consent cannot be inferred from inaction.[106]

7 (setting out the requirements for valid consent). On the GDPR's strict restrictions placed on consent as a lawful basis for data processing, see Schwartz & Peifer, *supra* note 33, at 143–44.

99. For a discussion of "idealized consent" in the U.S. legal privacy regime, see Schwartz & Peifer, *supra* note 33, at 149–50.

100. *See, e.g.*, 15 U.S.C. § 6802(b).

101. For example, the Fair Credit Reporting Act permits a consumer reporting agency to share a "consumer report" if the consumer to whom it pertains provides written permission, that is, opts in to the sharing. 15 U.S.C. § 1681b(2). As a further example, the Telephone Consumer Protection Act requires businesses to have opt in consent from a consumer before sending an automated text message. 47 U.S.C. § 227(a)(4); 47 C.F.R. § 64.1200(f)(9).

102. GDPR, *supra* note 7, at art. 7. The Article 29 Working Party of the EU has provided extensive guidelines on interpreting consent under the GDPR. ARTICLE 29 DATA PROT. WORKING PARTY, ARTICLE 29 WORKING PARTY GUIDELINES ON CONSENT UNDER REGULATION 2016/679 (Apr. 10, 2018).

103. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 102, at 5.

104. Schwartz, *Privacy and Democracy in Cyberspace*, *supra* note 82, at 1685.

105. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 5(g)(1).

106. *Id.* § 5(g)(2).

Accordingly, in situations involving data activities that are unexpected or that are potentially harmful, affirmative opt in consent is required. Our approach avoids the tsunami of opt in consent requests that this legal requirement might otherwise provoke.[107] Such opt in requests would quickly become meaningless and annoying when people are bombarded with them about matters that are trivial.

4. Section 6: Confidentiality

Oddly, the principle of confidentiality is not explicitly included in many of the expressions of FIPPs or in many privacy laws, though it is a byproduct of the FIPPs and implied in certain statutes.[108] The *Principles* include an explicit section on confidentiality. The *Principles* recognize duties of confidentiality when there is "an express or implied promise of confidentiality" or when "required by law [or] . . . ethical standards."[109] The *Principles* also recognize a duty of confidentiality under the following circumstances:

> A data controller or data processor shall also maintain confidentiality when it (i) holds itself out to be privacy-respecting to gain the trust of data subjects who use its product or service, and (ii) causes data subjects to reasonably believe that it will not disclose their personal data based on reasonable social expectations. Such a reasonable belief can be based on privacy norms, or established practices.[110]

By adding confidentiality to the FIPPs, the *Principles* close an important gap in U.S. privacy law. We also create a bridge here to recent scholarship that advocates a fiduciary approach to privacy law.[111] The idea here is that data processors are trusted parties with inherent duties towards data subjects.[112] This

107. The GDPR guards against this risk largely by heightening the requirements for consent to be valid, which thereby makes it a relatively unattractive path for justification of legal processing. The guidance on consent under the GDPR from the United Kingdom's Information Commissioner's Office demonstrates this tendency. *What Is Valid Consent?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent [https://perma.cc/WLS9-6347].

108. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 181–82 (2007).

109. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 6(a).

110. *Id.* § 6(b).

111. Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BLOGS (Oct. 29, 2018), https://blogs.harvard.edu/jzwrites/2018/10/29/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/7NCY-UMFB]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

112. *See* Balkin, *supra* note 111, at 1193–94.

section of the *Principles* takes an important step in developing a sound structural basis for the information fiduciary idea.[113]

5. Section 7: Use Limitation

A fundamental difference between the U.S. and EU approaches is that the EU requires a lawful basis for the processing of personal data.[114] This requirement is anchored at the constitutional level in the EU.[115] The United States does not generally require a justification to process personal data. Indeed, through the courts' interpretation of the First Amendment, U.S. data privacy law features strong protection for a free flow of information.[116] In the United States, the law regulates and restricts the processing of personal data primarily when this activity might cause harm.

A general departure from this aspect of U.S. privacy law would make the *Principles* too fundamentally different from the existing U.S. law. In biology and law, transplants work best if compatible with a host organism.[117] Our goal is to find an approach that would not break radically from existing concepts in U.S. law.

Although the *Principles* do not rely on the lawful basis approach for the initial collection of personal data, we followed this approach for secondary uses of personal data. A secondary use of personal data is one "unrelated to those stated in the notice to the individual as required by Principle 4."[118] For these uses, an initial consent to use the data does not exist, so greater limitations should be placed on such unrelated processing. It is here where the idea of a lawful basis to process personal data, such as found in the GDPR, fits quite well. Principle 7 calls for either consent by the data subject or the fulfillment of the *Principles*' exceptions for consent. These exceptions include the fulfillment of a contract to which the data subject is a party; the significant advancement of the protection of health or safety of the data subject or other people; and, as in the GDPR, a catch-all for serving a "significant legitimate interest" without "pos[ing] a significant risk of material

113. For an important critique of the information fiduciary idea as lacking a foundation in current privacy law, see generally Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

114. CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW 242 (2d ed. 2007).

115. Schwartz & Peifer, *supra* note 33, at 123–27.

116. *Id.* at 134–35.

117. In the comparative law literature, this idea is that of an appropriate "fit" between a law and a recipient culture. Like much else in comparative law, the concept is not uncontested. *See, e.g.*, Michele Graziadei, *Comparative Law as the Study of Transplants and Receptions*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 441, 472–73 (Mathias Reimann & Reinhard Zimmermann eds., 2006).

118. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 7(a).

harm to the data subject or others" and without being "significantly unexpected."[119]

6. Section 8: Access and Correction

The *Principles* include a right for individuals to access their personal data and request corrections of errors. This is a common set of rights in privacy law, and our approach does not take a dramatically new direction. At the same time, we were careful to strike a balance between the interests of data processors and data subjects. As one example, data processors need only provide "reasonable process to challenge the accuracy of the data subject's personal data."[120] It is left for legislatures and courts to further define, for different contexts and circumstances, the kind of process that meets this reasonableness standard. As a further example, a data subject need only provide "a reasonable basis in proof" to demonstrate that stored data is incorrect.[121] Here, too, we use a reasonableness standard under the logic of reciprocal treatment.

7. Section 9: Data Portability

A trend in recent privacy laws is to include a right to data portability. This concept permits consumers to request and receive the personal data that an organization has collected about them, and then be able to move the data to another company. Such a right is found in the GDPR as well as California's CCPA.[122] We included it in the *Principles* as well.

This right is an emerging one, however, and there are many challenges involved in porting data from one platform to another. For example, one individual's personal data might be intertwined with the personal data of others. On a social media site, a person may have commented on the posts of others. These comments might lose their meaning when separated from the posts of the other users. Medical records may involve health care information about parents, siblings, and other relatives as physicians frequently collect family histories.

119. *Compare* PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 5(i)(3)(E), *with* GDPR, *supra* note 7, at art. 6(1)(f) (stating that processing shall be lawful if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data").

120. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 8(d)(1).

121. *Id.* § 8(d)(2).

122. GDPR, *supra* note 7, at art. 20; CAL. CIV. CODE § 1798.100(d) (West 2020).

The release of such combinations of data can impinge upon the privacy of third parties. Yet, redaction of this information to exclude the intermingled personal data of other individuals might affect or even change its meaning because the context has been altered. The *Principles* avoid tackling these issues because this interest is in its infancy, and more time and experience are needed to hone it. A modest amount of legal ambiguity can be a virtue; over time, the legal system should find its way forward in devising workable solutions to the problems of data portability.

8. Section 10: Data Retention and Destruction

Data destruction is a relatively straightforward concept in the United States, but data retention, the other element of this section of the *Principles*, proves more complex. Data destruction is a long established principle in U.S. privacy law. For example, the Fair Credit Reporting Act authorizes a set of federal agencies to establish rules for mandated destruction of consumer data from consumer reports.[123] Drawing on this authorization, the FTC has issued a Disposal Rule for those entities over which it has regulatory power.[124] Drawing on these and other elements of existing law, the *Principles* straightforwardly state, "A data controller may retain personal data only for legitimate purposes that are consistent with the scope and purposes of notice provided to the data subject."[125] Once retention of personal data is no longer permitted, moreover, "it shall be destroyed within a reasonable time by reasonable means that make it unreadable or otherwise indecipherable."[126]

More complicated than this notion of data destruction is the thorny concept of data retention. U.S. law generally acknowledges that legitimate business needs, legal obligations, and archival purposes require the ongoing storage of personal data. But when is data to be destroyed and not stored, or retained? The approach in the *Principles* is to establish a general rule of limits on retention: "A data controller may retain personal data only for legitimate purposes that are consistent with the scope and purposes of notice provided to the data subject."[127] We then make this rule subject to carefully drawn exceptions, such as when there is a legal obligation to retain personal data.

123. Fair Credit Reporting Act, 15 U.S.C. § 1681w.
124. 16 C.F.R. § 682 (2020).
125. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 10(a).
126. *Id.* § 10(c).
127. *Id.* § 10(a).

Finally, we did not include the GDPR's "right to erasure" (also referred to as a "right to deletion" or a "right to be forgotten")[128] in the *Principles*. This interest is highly controversial on this side of the Atlantic,[129] and has only begun to find its way into U.S. law. The leading example here is the CCPA, which contains a highly qualified right to deletion.[130] All and all, we did not think that the timing was right to propose an American "right to be forgotten." The ALI advises that Principles "should be written in the voice of the ALI."[131] In our view, there was not yet enough agreement among the ALI membership on this topic for us to speak for this organization on this topic.

9. Section 11: Data Security

We include data security in the *Principles* because we view it as an integral part of information privacy. As we noted in a comment to the *Principles*, "Nearly every version of [the] FIPPs includes protections for the security of personal data. Data security is one of the most common requirements of data privacy statutes and regulations. The privacy and security of personal data are related, and they cannot exist in isolation."[132]

Our approach to data security looks to reasonable safeguards, a method common in the United States and worldwide.[133] The primary benefit of this approach is that it is open-ended and evolves as standards and best practices develop and security threats change. Its shortcoming is that, left to their own devices, organizations can interpret "reasonable" in essentially unreasonable ways that fall short of what they need to do. This approach also does not provide detailed guidance to organizations about the specific security measures they should use.[134]

An alternative approach is to provide a list of specific standards, an approach embodied by the Health Insurance Portability and Accountability Act (HIPAA)

128. GDPR, *supra* note 7, at art. 17.
129. *See, e.g.*, Robert C. Post, *Data Privacy and Dignitary Privacy:* Google Spain, *the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981 (2018).
130. CAL. CIV. CODE § 1798.105 (West 2020).
131. Richard L. Revesz, *The Director's Letter: Toward Clearer Guidance on Drafting Principles of the Law*, ALI REP., Fall 2019, at 3.
132. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 1 cmt. c.
133. GDPR, *supra* note 7, at art. 32; Directive, *supra* note 28, at art. 32. For U.S. law, see the Gramm-Leach-Bliley Act, 16 C.F.R. § 314.3(a) (stating that covered entities should implement information security programs that are "appropriate" and are "reasonably designed to achieve the objectives" of the Act).
134. A recent opinion of the Eleventh Circuit explored these issues regarding the necessary degree of specificity in an FTC finding that a party committed an unfair trade practice due to a data security breach. LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

Security Rule and some state laws.[135] The virtue of this approach is that it provides guidance and specificity; its main shortcoming is that many organizations become obsessed with checking boxes on a "to do" list without paying sufficient attention to the quality of the substance of various security measures. Another shortcoming is that this approach might omit important safeguards, and if the mandated standards are not updated over time, the framework will lack new best practices and effective responses to threats. This risk of standards stagnating is real in today's age of legislative gridlock. We ultimately opted for the reasonableness approach because of its simplicity and ability to develop over time through input from courts and government agencies, including the FTC.

The *Principles* also include a data breach notification requirement. Data breach notification originated with a 2003 California law, and spread faster than wildfire to all fifty states in the United States as well as around the world.[136] The *Principles* define a breach broadly to include the "unauthorized access, acquisition, use, modification, sharing, or destruction of personal data."[137] This broad definition is designed to avoid arbitrary limitations on what can constitute a breach. Far too often, breach notification laws get bogged down in definitions of breach that have no relationship to the most important issue, which concerns the threat or harm that such breaches pose.[138] Our definition of a breach is similar to the one found in the HIPAA Breach Notification Rule.[139]

Many breach notification laws specify fixed time periods within which to notify affected individuals. Indeed, there seems to be an unfortunate competition among jurisdictions to have the shortest deadline to notify after discovery of a breach.[140] But early notification often does not produce good information because it can take a while to understand the extent and nature of a breach. Accordingly, we opted for a more contextual approach by requiring notification "without unreasonable delay."[141]

135. 45 C.F.R. § 164.530(c)(1). Regarding such state data breach laws, see Schwartz & Solove, *The PII Problem*, *supra* note 41, at 1831–34.
136. CAL. CIV. CODE § 1798.29 (West 2020). Regarding the spread of data breach notification laws, this concept is also found in GDPR, *supra* note 7, at arts. 33–34.
137. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 11(b)(1).
138. Hence, state data breach notification statutes split on whether mere "access" to personal data can trigger a notification, or whether there must be some indication of likely harm to an individual. For an overview of these laws, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2019, at 189–97 (2019).
139. *See* 45 C.F.R. § 164.404(a)(1) (stating a breach occurs when "unsecured protected health information" is "accessed, acquired, used, or disclosed as a result of such breach").
140. The GDPR is leading the field regarding short deadlines with its 72-hour breach notification requirement. GDPR, *supra* note 7, at art. 33.
141. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 11(b)(2).

10. Section 12: Onward Transfer

Organizations use a wide array of third-party vendors to help them process personal data, and these vendors may use additional parties for certain purposes—the chain of potential data-handling parties goes on and on.[142] The *Principles* therefore require reasonable due diligence to ensure that entities receiving personal data will protect it.[143] The idea is that the law's protection must follow personal data as an initial organization hires vendors, business associates, and other third parties to assist it and, as a consequence, shares the data with these other entities.

The law has begun to address these relationships and how contracts are to play a beneficial role in safeguarding privacy.[144] The *Principles* address the issues to be covered in the contracts between the initial data collector and the entities receiving personal data from it. When personal data passes through a vast network of entities, contracts must play a central legal role in protecting this information.[145]

The *Principles* do not include restrictions on cross-border data transfers. First, and unlike the EU, the United States lacks a governmental entity that can make a determination of adequacy.[146] Second, the *Principles*' requirements for onward transfer already require companies to provide safeguards, whether such transfer is domestic or international.[147] Third, the U.S. government has vast surveillance powers that its law does not necessarily restrict sufficiently at present.[148] An adequacy requirement might lead the United States to demand

142. As the *Principles* state, "[o]nward transfer is one of the greatest challenges to privacy protection, as accountability and control over personal data can break down as personal data is transferred along a chain of entities." *Id.* § 12 cmt. a.

143. *Id.* § 12(b).

144. HIPAA requires a business associate agreement (BAA) for onward transfers of protected health information (PHI). 45 C.F.R. § 164.502(e)(i)–(ii). HIPAA also regulates downstream personal data transfers—when any business associate (BA) transfers personal data to another entity, that entity is deemed to be a BA too. Similarly, the Gramm-Leach-Bliley Act and its applicable regulations place numerous requirements on a financial institution concerning its selection and use of third-party service providers. 15 U.S.C. § 6802(b)(2).

145. Daniel Solove, *Our Privacy and Data Security Depend Upon Contracts Between Organizations*, TEACHPRIVACY (May 5, 2014), https://teachprivacy.com/privacy-data-security-depend-upon-contracts-organizations [https://perma.cc/4SE2-EGE2].

146. On the historical background of the adequacy requirement, see Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 86, at 1977–81. On the GDPR's approach, see GDPR, *supra* note 7, at art. 45.

147. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 12(a).

148. Comparative assessments of respective national schemes for regulation of national surveillance apparatuses prove to be extremely difficult. For a comparative set of essays that evaluates the United States as well as other countries regarding a subset of their surveillance of

more of the rest of the world than of itself. Alternatively, an adequacy standard might set the bar for a transfer so low as to be meaningless.

C. Chapter 3: Accountability and Enforcement

1. Section 13: Accountability

As a policy idea, the accountability principle focuses on whether a data processing entity has created internal processes that are commensurate with potential data threats.[149] At an international level, there has been a strong level of interest in data privacy standards of accountability for the twenty-first century.[150] This effort began with the Irish Data Protection Commissioner's multiyear Galway initiative.[151] These initial steps were followed by accountability projects led by the French Data Protection Commissioner and an announcement of international standards of privacy including an accountability principle issued in 2009 by EU data protection commissioners in Madrid.[152]

As part of achieving accountability, the *Principles* require an organization to develop a reasonable comprehensive privacy program. Such a program should include written privacy and security policies and procedures, personal data inventory, risk assessment, plans for training, privacy and security by design, and privacy and security by default.[153] For privacy by design, the *Principles* do not specify design choices. Mandating specific technological approaches is quite a

private sector information, see BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (Fred H. Cate & James X. Dempsey eds., 2017). For a concise overview and critique of the U.S. system, see LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016). For a recent controversy in this area in the United States, see the report of the Department of Justice's Office of the Inspector General regarding the FBI's "Crossfire Hurricane" investigation of the 2016 Trump campaign. OFF. OF THE INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (rev. ed., 2019).

149. CTR. FOR INFO. POL'Y LEADERSHIP, DATA PROTECTION ACCOUNTABILITY: THE ESSENTIAL ELEMENTS 8–9 (2009).

150. *Id.* at 6.

151. *Id.* at 3.

152. COMMISSION NATIONALE DE I'INFORMATIQUE ET DES LIBERTES, PRIVACY SEALS ON PRIVACY GOVERNANCE PROCEDURES (2015). On the French accountability project, see Winston Maxwell, *New CNIL Accountability Standard May Become European Model*, HOGAN LOVELLS CHRON. OF DATA PROT. (Jan. 14, 2015), https://www.hldataprotection.com/2015/01/articles/international-eu-privacy/new-cnil-accountability-standard-may-become-european-model [https://perma.cc/HRH4-HRYF]; Paula J. Bruening, *Accountability: Part of the International Public Dialog About Privacy Governance*, 10 BNA INT'L WORLD DATA PROT. REP. 1–3 (2010); INT'L CONF. OF DATA PROT. & PRIV. COMM'RS, INTERNATIONAL STANDARDS ON THE PROTECTION OF PERSONAL DATA AND PRIVACY: THE MADRID RESOLUTION (2009).

153. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 13.

challenging undertaking for law,[154] and moreover, it would likely face unified and strong opposition from the tech industry. Although the law probably should do more to regulate design, we were concerned about how to do this well while also being practical about not pushing U.S. law too far. The *Principles*, therefore, opt merely to require that "[d]esign choices and the reasoning that supports them shall be documented."[155] Policymakers, regulators, and other actors can then evaluate these decisions. We leave it up to these parties to delve into the substance of design decisions on a case-by-case basis.

This approach to privacy by design is furthered by the *Principles'* requirement of documentation. This secondary condition is something that other laws often fail to require when they address privacy by design. Any organization can claim that it is practicing privacy by design, but mandated documentation forces organizations to create a record that later can be evaluated and critiqued by regulators or others. This step adds accountability to the process. Documentation showing that the design process for privacy was incomplete or poorly conceived could be damaging later on, as during post-breach litigation. Our hope is that the documentation requirement will prevent organizations from treating privacy by design as a meaningless shibboleth.

2. Section 14: Enforcement

Enforcement issues proved to be one of the most hotly debated areas of the entire *Principles* project. In the landscape of privacy law, there are widely divergent perspectives on enforcement and penalties. Within the ALI, we heard much from representatives of these different viewpoints, including parties who strongly opposed our assigning specific remedies to specific sections of our *Principles*. As an initial decision, we decided to save final drafting of this crucial section until the end of our work while debating this topic throughout the lifespan of the project. With the strategic help of Ricky Revesz, Director of the ALI, we were able to identify an agreeable solution.

The initial breakthrough was to use this section of the *Principles* to present a menu of options from which legislatures, judges, policymakers, and privacy professionals could choose. In providing a broad range of possible ingredients, or

154. Despite or perhaps due to the challenges of legal mandates for design, there have been rewarding academic studies on this topic. *See*, *e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018). Another problem is the lack of interaction at many companies between the technologists and the lawyers. *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 694–95 (2018).

155. PRINCIPLES OF THE LAW, DATA PRIVACY, *supra* note 54, § 13(d)(2).

factors, we acknowledge that an attempt on our part to shape more definitive or harder-edged rules would have created significant disagreement among ALI members. Hence, we place our trust in the legal process to work out specific remedies in an evolving fashion for different data processing contexts.

To prevent the choice of ineffective remedies, and as the second element of our breakthrough solution to the enforcement section, the *Principles* includes a requirement that a remedy be "effective, proportionate, and have a deterrent effect."[156] In deciding whether a remedy met this test, the factors to be considered include the gravity of the infringement, the fault of the infringer, unjust enrichment, and the "need for general deterrence" among other things.[157] Hence, while this section does not mandate explicit remedies tied to distinct privacy violations or harms, it requires that the law be strong enough to constrain the behavior of data controllers and data processors.

Notably, the *Principles* do not require proof of a privacy harm in order for there to be a remedy. Despite the growth of the intentional infliction of emotional distress tort and the privacy torts, courts in privacy cases still struggle to recognize that emotional or psychological harm alone should be able to form a basis for a lawsuit. In dealing with harms created by data security breaches, for example, federal appellate courts have issued a series of conflicting opinions, many rejecting emotional distress as sufficient to establish cognizable harm.[158] The Supreme Court also has been dismissive of emotional distress as a basis for harm. For example, in *FAA v. Cooper*,[159] the Court held that the Privacy Act does not recognize psychological harms as solely sufficient to create an actual injury. The *Cooper* Court's reluctance to find actionable harms from privacy invasions is representative beyond its particular statutory context. Courts are also skeptical of tort and contract actions that point only to emotional or mental harms. Already in 2003, Joel Reidenberg concluded his critique of privacy enforcement actions by warning, "privacy remedies for personal wrongs are not easily accommodated within the existing set of legal rights."[160] A similar negative judgment can be

156. *Id.* § 14(a).
157. *Id.* § 14(c)(5).
158. Solove & Citron, *supra* note 41, at 746.
159. FAA v. Cooper, 566 U.S. 284, 300 (2012) ("[T]he term 'actual damages' *can* include nonpecuniary loss. But this generic meaning does not establish with the requisite clarity that the Privacy Act, with its distinctive features, authorizes damages for mental and emotional distress.").
160. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 892 (2003).

reached today. Too often, courts only recognize a narrow range of privacy harms and leave plaintiffs without a remedy.[161]

In sum, there are real benefits to combining a menu of possible remedies with a general requirement of effectivity, proportionality, and dissuasiveness. The *Principles* are designed to serve in a broad range of settings, including legislation, adjudication, and the shaping of internal policies and procedures. Their approach to enforcement provides the necessary flexibility in vastly different settings for development of remedies that effectively respond to real harms.

III. CONCLUSION

The *Principles* represent the ALI's first foray into modern data privacy law. The goal of the project is to provide much needed conceptual clarity and direction for an area of law that is highly fragmented, inconsistent, and gap-ridden. The *Principles* reflect a comprehensive, consensus position, and one that is tailored to legal needs and precedent in the United States. They develop concepts that will serve a range of stakeholders in a broad range of settings, including enacting legislation, adjudicating cases, and developing

161. For example, federal circuit courts are divided on the issue of whether an increased risk of a pecuniary harm like identity theft, or reasonable expenditures to avoid such harms, are injuries giving rise to Article III standing. *Compare* the expansive holdings in Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (finding standing when victims of a data breach "allege[d] that their data ha[d] already been stolen and [was] now in the hands of ill-intentioned criminals," because the risk of harm was "sufficiently substantial" and "incurring mitigation costs [was] reasonable"); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967, 969 (7th Cir. 2016) (finding injury when victims of credit and debit card data breach alleged that they had already "experienced fraudulent charges" and were at "increased risk of fraudulent charges and identity theft" in the future); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140–43 (9th Cir. 2010) (finding that plaintiff with "generalized anxiety and stress" as a result of the theft of his information had standing); *and* Attias v. Carefirst, Inc., 865 F.3d 620, 626–29 (D.C. Cir. 2017) (finding standing in a health insurance breach case when plaintiffs alleged that their "personal identification information, personal health information, and other sensitive information" had been stolen, "creat[ing] a material risk of identity theft"); *with* the narrow holdings on the harm issue in Katz v. Pershing, LLC, 672 F.3d 64, 79–80 (1st Cir. 2012) (finding no standing when plaintiff alleged failure to provide notice of security breach, because there were no allegations of actual access of plaintiff's personal information by an unauthorized user); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 43 (3d Cir. 2011) (finding no standing when "no evidence suggests that the data [that had potentially been accessed without authorization] has been—or will ever be—misused"); *and* Beck v. McDonald, 848 F.3d 262, 273–77 (4th Cir. 2017) (finding no standing when plaintiffs did not allege intentional targeting or actual misuse of personal information, and rejecting a "substantial risk" of future harm theory when 66 percent of those affected by the breach "will suffer no harm"). For an analysis of how these cases handle the issue of privacy harm, see generally Courtney M. Cox, *Risky Standing: Deciding on Injury*, 8 NE. U. L.J. 75 (2016) (placing the cases in a conceptual framework).

organizational policies and procedures. While remaining true to the character of U.S. data privacy law, the *Principles* also propose reforms to certain features of American information privacy law, such as notice-and-choice.

Moreover, this project highlights where the U.S. law shares elements with EU law, which sets a benchmark for most of the world. For example, the *Principles* include a right to data portability, which is found in the GDPR as well as in California's CCPA. The *Principles* have also bridged differences with EU law when possible. One way that they have done so is by promoting a standardized terminology between the two systems. The *Principles* adopt the EU nomenclature of data subjects, data controllers, and data processors. U.S. law already has similar ideas but lacks consistent terminology in this area. We hope that the *Principles* will enable U.S. laws to be better harmonized with the EU approach to data privacy. In our view, this seven year project indicates a path forward for U.S. data privacy law.

IV. APPENDIX: THE BLACK LETTER OF THE ALI PRINCIPLES OF LAW, DATA PROTECTION

This Part presents the complete black letter for the *Principles of Law, Data Protection.* The entire *Principles* project is more than 100 pages and includes illustrations, commentary, and reporters' notes. It can be obtained from the ALI at *https://www.ali.org*.

§ 1. Purpose and Scope of the Data Privacy Principles

(a) *Purpose of the Principles.* The Data Privacy Principles are designed to inform the development of best practices, to bring coherence to existing law, and to guide the development of emerging law. These Principles can serve as the framework for laws, a data privacy model code, or industry-specific codes. The Data Privacy Principles cover some, but not all, data activities regarding personal data.

(b) *Scope*

(1) *Covered Personal Data Activities.* These Principles cover personal data activities involving, or intended to involve:

(A) the sale and provision of goods or services; and

(B) the functioning of institutions and organizations—governmental, for-profit, and nonprofit—and natural persons, including the employment of persons.

(2) *Personal Data Activities Not Covered.* The Data Privacy Principles do not cover personal data activities involving, or intended to involve:

(A) purely interpersonal or household relationships;

(B) personal activities;

(C) national intelligence and law enforcement;

(D) the administration of the judicial system, including judicial matters;

(E) communications seeking to promote public understanding or discussion, or data activities that are intended to support such communications, including data activities connected with libraries, archives, journalism, public commentary, scholarship, blogging, biography, satire, or the arts; or

(F) the public exchange of publicly available information, except insofar as such exchange is made for particular purposes that would justify the application of these Principles and is consistent with the First Amendment.

§ 2. Definitions

(a) *Data.* "Data" means information recorded in any form or medium.

(b) *Personal Data.* "Personal data" means any data that is identified or identifiable to a specific living individual.

(1) Data is "identified" when it is directly linked to a specific natural person, or when there is a high probability that it could be linked to a specific person. When data is identified, it is personal data under the Data Privacy Principles and is subject to all relevant Principles.

(2) Data is "identifiable" when there is a moderate probability that it could be linked to a specific natural person by the intended recipient(s) or by others reasonably foreseeable to have access to the data. When data is identifiable, it is personal data under the Data Privacy Principles and is subject to some of the Principles but exempt from others.

(3) Data is "nonidentifiable" when there is a low probability that it could be linked to a specific natural person. Such data is not personal data under these Data Privacy Principles.

(4) Data controllers and data processors are under a continuing obligation to take reasonable measures to review their activities for circumstances that may have altered the ability to identify a specific natural person. If a data controller or data processor finds that information previously classified as nonidentifiable is actually identified or identifiable, it is obligated to change its handling of this information so as to comply with these Principles.

(c) *Data Subject.* A "data subject" is a natural person to whom the personal data relates.

(d) *Personal Data Activities.* A "personal data activity" is any of the activities defined below:

(1) "Collection" means the acquisition of personal data either directly from the individual or from other sources, including a third party.

(2) "Access" means the retrieval or viewing of personal data by the person or entity who initially collected it, or by another person or entity.

(3) "Retention" means the maintenance or storage of personal data.

(4) "Use" means the processing of personal data or the making of decisions based in whole or in part on that personal data.

(5) "Sharing" means providing others with personal data or with access to personal data.

(6) "Destruction" means disposing of, or deleting, personal data in a manner that makes it permanently incomprehensible.

(e) *Data Controller.* A "data controller" is any person, organization, or agent thereof that engages in any covered personal data activity and that determines the purposes of such activity.

(f) *Data Processor.* A "data processor" is any person, organization, or agent thereof that engages in any covered personal data activity on behalf of a data controller or another data processor.

§ 3. Transparency Statement

(a) *Requirement.* A data controller or data processor that engages in personal data activities shall provide a publicly accessible transparency statement about these activities.

(b) *Content*

(1) The transparency statement shall clearly, conspicuously, and accurately explain the data controller's or data processor's current personal data activities, including policies and practices regarding the protection of personal data.

(2) When the law requires or permits a data controller or data processor to withhold certain information, such as trade secrets or confidential information, the transparency statement need not include this information.

(c) *Accessibility.* The transparency statement shall be reasonably accessible to any interested person. In the event that the transparency statement is changed, previous versions of the statement shall be retained and kept reasonably accessible.

(d) *Proportionality.* A transparency statement is required for both identified and identifiable personal data. The detail and sophistication of the transparency statement shall be proportional to the magnitude of the privacy and security risks of the personal data activities.

§ 4. Individual Notice

(a) *Requirements for individual notice*

(1) A data controller that engages in a data activity involving identified personal data that implicates a data subject's interests, as recognized by these Data

Privacy Principles, shall provide notice individually to that data subject. This notice shall fulfill the requirements of subsection (d) below.

(2) The individual notice shall be distinct from and in addition to the transparency statement required in § 3.

(3) All aspects of the notice should be provided as reasonably practicable. A data controller's capabilities and resources are factors in determining whether providing a particular aspect of notice is reasonably practicable.

(4) Individual notice need not be provided when personal data is only identifiable, but not yet identified.

(b) *Accessibility.* The notice shall be reasonably accessible to the data subject.

(c) *Timing of notice.* The notice shall be provided to the data subject at an appropriate time that will enable the data subject to exercise interests recognized by these Data Privacy Principles.

(d) *Content of notice*

(1) The notice shall be clear and intelligible to a reasonable person.

(2) The notice shall inform the data subject of the nature of the data activity, the uses made of the data, the interests implicated, and how the data subject may exercise those interests.

(3) The notice shall inform the data subject of any rights provided by applicable law that are relevant to the data activities in which the data controller is engaging.

(4) The notice shall contain information enabling the data subject to contact the data controller with questions or complaints about the data controller's data activities. When a data subject contacts the data controller in the manner described in the notice, the data controller shall respond as soon as reasonably practicable.

(e) *Heightened notice*

(1) For any data activity that is significantly unexpected or that poses a significant risk of causing material harm to a data subject, the data controller should provide reasonable "heightened notice" to the data subject.

(2) A significantly unexpected data activity is one that a reasonable person would not expect based on the context of the personal data activities. Activities regarding personal data are "significantly unexpected" when they are at substantial variance with the expectations of a reasonable person.

(3) A significant risk may exist with a low likelihood of a high-magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of heightened notice.

(4) Heightened notice shall follow all of the requirements of notice specified above, as well as additional requirements specified in this subsection.

(5) Material harm exists when a reasonable person would recognize that a data subject may suffer financial loss, reputational damage, embarrassment, emotional distress, chilling of activities protected under federal or state constitutional law, or a revelation of personal data that the data subject wants to conceal.

(6) Heightened notice shall be made more prominently than ordinary notice and closer in time to the particular data activity.

(f) *Material changes in policies and practices.* Additional notice shall be provided to a data subject when a data controller makes any material change in its policies and practices with respect to personal data.

(g) *Exceptions to individual notice.* A data controller may refrain from providing notice if there is no reasonably practicable way to inform the data subject. The data controller shall document why providing notice is not reasonably practicable and include this information in the transparency statement in § 3. This statement should also be publicized on the data controller's website home page or through other reasonable means.

§ 5. Consent

(a) Consent means the willingness of the data subject to permit the personal data activity in question.

(b) When consent is required, a data subject shall be given understandable and easy-to-use means to permit exercise of meaningful choice in relation to personal data activities regarding the data subject's personal data.

(c) When the law requires the consent of the data subject for personal data activities, or a data controller relies on the consent of the data subject as the justification for personal data activities, these Principles apply in the absence of a valid exception.

(d) The data controller is responsible for obtaining consent. A data controller may contract with another entity to obtain the consent of data subjects.

(e) Consent is invalid unless the data subject is provided reasonable notice that satisfies the standards of Principle 4.

(f) Consent is invalid if it is obtained in a misleading or deceptive fashion.

(g) *Form of consent*

(1) The form by which consent is obtained must be reasonable under the circumstances, based on the type of personal data involved, the nature of the personal data activity, and the understandings of a reasonable data subject.

(2) In situations in which heightened notice is required pursuant to Principle 4(e), only clear and affirmative consent shall suffice for valid consent. Clear and affirmative consent cannot be inferred from inaction.

(3) Except for paragraph (2) above, consent can be apparent whenever it can reasonably be understood that the individual consents to a particular use of personal data. Apparent consent occurs when words or conduct are reasonably understood by another to be intended as consent.

(h) *Withdrawal of consent.* An individual shall be permitted to withdraw consent, subject to legal or otherwise reasonable restrictions, by providing reasonable notice to the entity that collected the personal data.

(i) *Exceptions to the consent requirement.* Personal data activities may be conducted without consent if:

(1) the personal data activity is required by law;

(2) obtaining consent would be impermissible under law; or

(3) obtaining consent would be impractical, or too costly or difficult, and the use satisfies one or more of the following criteria:

(A) the personal data activity is necessary in the performance of a contract to which the data subject is a party;

(B) the personal data activity significantly advances the protection of the health or safety of the data subject or other people;

(C) the personal data activity significantly advances protection against criminal or tortious activity by or against a data subject;

(D) the personal data activity significantly advances the public interest, and it would not pose a significant risk of material harm sufficient to trigger heightened notice pursuant to Principle 4(e); or

(E) the personal data activity serves a significant legitimate interest, and it neither poses a significant risk of material harm to the data subject or others, as is defined in § 4(e)(3), nor is significantly unexpected, as is defined in § 4(e)(2).

§ 6. Confidentiality

(a) *Duty of confidentiality.* A data controller or data processor shall maintain the confidentiality of personal data when:

(1) confidentiality is required by law;

(2) confidentiality is required by ethical standards (such as professional rules of conduct); or

(3) when the personal data is collected under an express or implied promise of confidentiality.

(b) *Relationships of trust.* A data controller or data processor shall also maintain confidentiality when it (i) holds itself out to be privacy-respecting to gain the trust of data subjects who use its product or service, and (ii) causes data subjects to reasonably believe that it will not disclose their personal data based on

reasonable social expectations. Such a reasonable belief can be based on privacy norms, or established practices.

(c) *Service providers and onward transfers.* An onward transfer of personal data by a data controller or data processor to another data processor is not a breach of confidentiality if authorized by Principle 12 (Onward Transfer).

(d) *Breach of confidentiality.* A duty of confidentiality is not breached under the following circumstances:

(1) the data subject consents to the disclosure of personal data;

(2) disclosure is required by law, such as judicial process or a statute requiring disclosure; or

(3) disclosure is necessary for the health or safety of the data subject or other people.

Any disclosures under these circumstances should involve only the minimum necessary personal data related to the disclosure's purpose, and be released only to individuals or entities that are best suited for such purpose.

§ 7. Use Limitation

(a) *Secondary uses.* Personal data shall not be used in secondary data activities unrelated to those stated in the notice required by Principle 4 without a data subject's consent. Secondary data activities are those unrelated to those stated in the notice to the individual as required by Principle 4.

(b) *Exceptions.* Personal data may be used in secondary data activities based on the exceptions to consent set out in Principle 5(i).

(c) *Transparency and notice*

(1) Notice of the specific justification for using data shall be conveyed to the data subject as soon as practicable.

(2) When it is reasonably foreseeable that personal data will be used in the future in a way authorized by subsection (b), the transparency statement (Principle 3) and individual notice to data subjects (Principle 4) shall be updated to state this fact. Such additional notice shall be provided in a fashion consistent with Principle 4(f).

§ 8. Access and Correction

(a) *Information about identified personal data.* A data controller must inform a data subject whether the data controller or data processor acting on behalf of the data controller stores identified personal data about the data subject. This information shall be communicated in a reasonably timely fashion after a request by a data subject who provides reasonable proof of identity. This interest does not extend to identifiable personal data.

(b) *Access.* Unless access can be refused under subsection (e) or (f), a data subject is entitled on request to access personal data about the data subject stored by a data controller or data processor acting on behalf of the data controller. A data controller must provide access or a reason for denying access within a reasonable period of time after the request is made.

(c) *Verification of identity.* When access to personal data is requested by a data subject or a person acting on behalf of a data subject, a data controller shall use reasonable means to verify the identity of the data subject or the validity of the legal authority of the person acting on behalf of the data subject before providing such access.

(d) *Correction*

(1) A data controller shall provide a data subject with a reasonable process to challenge the accuracy of the data subject's personal data.

(2) When a data subject provides a reasonable basis in proof to demonstrate that the data subject's personal data is incorrect, the data controller shall correct the data by amending or deleting it, or by other means. The data controller shall take reasonable steps to ensure that the errors are corrected in any copies of the personal data stored by data processors that have received it from the data controller.

(3) A data controller that rejects a data subject's contention of error shall provide a timely explanation. When reasonably practicable, the data subject may add a statement of disagreement to the record where the data is stored. This statement shall be included when the personal data is shared with another person or entity.

(e) *Exceptions.* Access and an opportunity for correction need not be provided when:

(1) disclosure of the data subject's personal data is prohibited or restricted by law, or a duty to protect proprietary information or trade secrets;

(2) disclosure would violate the privacy of persons other than the data subject; or

(3) the balance of interests between the data controller and the data subject weighs against access and an opportunity for correction. Factors in assessing this balance include whether the burden, expense, or security risks of access and correction would be unreasonable or disproportionate to the harms to the data subject's privacy.

(f) A data controller may not provide access and opportunity for correction to a data subject when the law prohibits these interests.

§ 9. Data Portability

(a) *Data portability request and a usable format.* When a data subject makes a data portability request and when required by law, or when appropriate, reasonable, and practicable, a data controller shall provide to the data subject a copy of the data subject's personal data in a usable format. A usable format is one that is structured, commonly used, and machine-readable in a way that permits a reasonable data subject to use this information in other platforms or situations without undue burden.

(b) *Scope of portable personal data.* Portable personal data is personal data that the data subject provided to the data controller or that the data subject generated while using the data controller's services or products and that was stored by the data controller or by a data processor on the controller's behalf.

(c) *Verification of identity and authority.* Before providing the personal data in response to a data portability request, a data controller shall use reasonable means to verify that the requestor is the data subject or a person who has legal authority to make the request.

(d) *Redaction of personal data of others.* A response to a data portability request shall redact identified and identifiable personal data about other data subjects when providing such data would violate these Principles.

(e) When appropriate, a data controller may require a reasonable fee for responding to a data portability request.

(f) If only identifiable personal data is maintained about a data subject and if complying with a data portability request would require identifying this personal data, then the data controller does not have to comply with the data portability request.

§ 10. Data Retention and Destruction

(a) *Scope of retention of personal data.* A data controller may retain personal data only for legitimate purposes that are consistent with the scope and purposes of notice provided to the data subject. A data processor shall retain personal data only as justified by its contract with the data controller or the data processor that provided the personal data and when consistent with these Data Privacy Principles.

(b) *Data retention for archival or research purposes.* When personal data is stored for archival or research purposes, reasonable access limitations shall be set to protect privacy.

(c) *Destruction of personal data.* When retention of personal data is no longer permitted under subsection (a), it shall be destroyed within a reasonable time by reasonable means that make it unreadable or otherwise indecipherable. A data

controller that has provided personal data to a data processor shall take reasonable steps to ensure that the data processor properly destroys the data.

(d) *Exceptions to data destruction.* Exceptions to the data-destruction requirement include:

(1) a legal obligation to retain the personal data;

(2) protecting the data controller's or data processor's legitimate interests, or legal needs, including possible litigation; or

(3) archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

(e) *Duty to destroy personal data.* If a data controller or data processor obtains or stores personal data in violation of these Data Privacy Principles, it shall destroy the personal data unless an exception in subsection (d) above applies.

(f) *Policies and procedures.* A data controller and data processor shall develop written policies and procedures for the storage and destruction of personal data when doing so is reasonable given the entity's size and the amount and sensitivity of the personal data that it stores. These policies and procedures shall permit it to meet its obligations under this Section. A data controller or data processor shall also implement reasonable means for data destruction as part of its system design. These steps for data destruction shall take into account the cost of implementation and the nature of the risks to a data subject.

§ 11. Data Security and Data Breach Notification

(a) *Reasonable security safeguards*

(1) A data controller shall adopt reasonable security safeguards to protect against foreseeable risks, including unauthorized access, acquisition, use, modification, sharing, or destruction of personal data.

(2) Reasonable security safeguards are proportionate to the risk of harm in the event that the personal data is compromised. Proportionality is to be assessed in light of the type and nature of personal data used, the likely severity of harm to data subjects, the number of data subjects affected, and the cost of security safeguards.

(3) Reasonable security safeguards include administrative, physical, and technical measures that include training of employees.

(b) *Personal data breach notification*

(1) A personal data breach is the unauthorized access, acquisition, use, modification, sharing, or destruction of personal data.

(2) When a personal data breach creates more than a low probability that personal data will be compromised, the data controller must notify affected data

subjects without unreasonable delay, and must notify public authorities to the extent required by law.

(3) A data controller must provide a public notice for a personal data breach that involves more than 500 data subjects.

(4) A data processor that has a personal data breach shall notify the data controller as soon as reasonably possible. The data controller shall provide notice of a personal data breach of its data processor as set forth in paragraphs (1), (2), and (3) above.

(5) The factors to be considered in determining whether there is a low probability that personal data will be compromised include:

(A) the nature and extent of the personal data involved, including the types of identifiers and the likelihood of reidentification;

(B) the identity of the unauthorized person to whom the personal data was disclosed or who used it;

(C) whether the personal data was actually acquired or accessed; and

(D) the extent to which the risk of compromise of the personal data has been mitigated.

(6) Notification is not required when the personal data was properly encrypted and the encryption keys are not compromised or breached.

§ 12. Onward Transfer

(a) *Limits on onward transfers.* A data controller or data processor that has personal data may make an onward transfer of this information to a data processor for personal data activities only if:

(1) the data subject has received notice of the activities;

(2) the transfer is required by law; or

(3) the transfer is for uses specified in Principles 7(b) and 5(i) (exceptions to use limitation) and the requirements of Principle 7(b) and (c) are met.

(b) *Due diligence review of recipients of personal data.* Before making an onward transfer, a data controller or data processor shall exercise due diligence to ensure that the recipient will protect the personal data under these Principles.

(c) *Contracts with data processors.* Before making an onward transfer to a data processor, a data controller or data processor must enter into a binding contract with the recipient of the personal data. The contract shall include remedies for failing to comply with its terms, such as termination of the contract, and require the personal data recipient to:

(1) protect the personal data according to these Principles;

(2) protect the personal data according to the transparency statement and individual notice;

(3) carry out only the personal data activities that are necessary to comply with the contract or that are expressly authorized by the data controller or data processor that transferred the data;

(4) notify the data controller of any onward transfer before it is made and allow the data controller to approve or reject the transfer;

(5) take the following steps when transferring data to another data recipient:

(A) exercise due diligence;

(B) transfer data only to a recipient that will provide the required protection under (c)(1);

(C) enter into a contract that includes the same or greater protections as in its contract with the data controller or data processor and that requires the other data recipient to comply with the obligations of a data processor under this subsection;

(D) require that any subsequent data recipients follow the requirements of this subsection if they transfer the personal data to other downstream data recipients;

(6) return or destroy the data at the data controller's request when the recipient no longer has a legal or contractual need to retain it;

(7) train its employees who have access to the personal data about their obligations under the Principles and the transparency statements and individual notice;

(8) devote appropriate resources, including sufficient personnel, to the protection of the personal data;

(9) facilitate the data controller's compliance with the Principles by cooperating with the data controller's oversight activities. The means of cooperation shall include providing information to the recipient that is required for compliance and assisting the data controller in responding to a data subject's exercise of rights under these Principles. When necessary for the data controller's compliance with these Principles, cooperation shall extend even after the contract ends or is terminated;

(10) develop and maintain a reasonable comprehensive privacy program as specified in Principle 13(c);

(11) provide information necessary for the data controller or data processor to evaluate the recipient's compliance with these Principles; and

(12) notify the data controller promptly upon discovery of a personal data breach or any noncompliance with the contract or these Principles, and cooperate fully with the data controller's efforts to address the matter.

(d) *Reasonable oversight.* A data controller or data processor that transfers personal data shall engage in reasonable oversight of the recipient. If it finds that the recipient of the personal data is deficient in performing any of its contractual

obligations related to this Principle, the data controller or data processor shall invoke appropriate measures under the contract to promptly correct the deficiency, and also shall demand reasonable assurances from the personal data recipient that the deficiency will not recur in the future.

(e) *Downstream onward transfers.* A data recipient that transfers personal data to a downstream data recipient shall follow the requirements of this Principle. Unless prohibited by law, every recipient of personal data is covered by these Principles.

§ 13. Accountability

(a) Data controllers and data processors are accountable for complying with these Principles. Accountability requires data controllers and data processors regularly to assess privacy and security risks associated with their data activities and to maintain a reasonable comprehensive privacy program of oversight and governance mechanisms.

(b) *Reasonable comprehensive privacy program.* A comprehensive privacy program is reasonable when it is appropriate to the entity's size, complexity, and resources; the amount and types of personal data used; and the risks that the entity's activities pose to the data subjects' privacy and security.

(c) *Components of a reasonable comprehensive privacy program.* A reasonable comprehensive privacy program shall include at least these components:

(1) written privacy and security policies and procedures addressing all personal data activities;

(2) a regular inventory of personal data collected, received, stored, or used that includes examination of:

(A) the types of data,

(B) the location of this personal data,

(C) the need to retain it,

(D) the protections that secure it,

(E) the individuals who have access to it, and

(F) the individuals responsible for overseeing its proper use and protection;

(3) a risk assignment conducted before a system goes live and at reasonable periodic intervals afterwards to identify and to fix, improve, and remedy within a reasonable period of time:

(A) any noncompliance or nontrivial risks of noncompliance with:

(i) these Data Privacy Principles,

(ii) applicable privacy or data-security laws,

(iii) the policies and procedures of the data controller or data processor,

(B) the effectiveness of the policies, procedures, and practices of the data controller or data processor in light of the evolution of risks and the law, and

(C) the efficacy of the training of its workforce by the data controller or data processor;

(4) a training program that reaches all employees or contractors who have access to or handle personal data, and employees or contractors whose actions materially affect the data that can be accessed or handled by others. This training shall be reasonably designed to permit the employee or contractor to understand the entity's policies and procedures and to be aware of and minimize any reasonably anticipated risks to personal data. At a minimum, training shall be conducted upon hiring or contracting and on an annual basis.

(d) *Privacy and security by design*

(1) A data controller or data processor shall analyze the privacy and security implications of any new product, service, or process early on in its development. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with reasonable thoroughness. This analysis shall be documented.

(2) A data controller or data processor shall examine how the product, service, or process should be designed to address the privacy or security issues identified in the analysis. The final design of the product, service, or process shall incorporate reasonable design choices based on this analysis. Design choices and the reasoning that supports them shall be documented.

(e) *Privacy and security by default*

(1) A data controller or data processor shall analyze the default settings of any existing or new product or service and how such settings implicate privacy and security. A default setting refers to the preset settings of a product or service. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with a reasonable thoroughness. This analysis shall be documented and repeated at reasonable intervals.

(2) A data controller or data processor shall draw on this analysis to make reasonable final default settings. Default-setting choices and the reasoning that supports them shall be documented.

§ 14. Enforcement

(a) To the extent that the law recognizes any remedies for these Principles, these remedies shall be effective, proportionate, and have a deterrent effect.

(b) *Enforcement mechanisms.* Enforcement, if any, of these Principles can be through various mechanisms, including individual redress and collective means of enforcement. Enforcement proceedings can include actions by the Federal Trade Commission, other governmental agencies, and state Attorneys General, as well as

class-action lawsuits and other civil proceedings involving the pursuit of civil remedies. Remedies can include compensation to injured parties, fines paid to the government, injunctions or administrative directives ordering future compliance, orders to comply, restitution of unjust enrichment, and other measures. Governmental decisionmakers may consider factors and elements that are not available to private parties claiming infringement.

(c) *Factors for deciding whether to provide remedies.* Factors to be considered in deciding on the remedies, if any, for the violation of a Principle include:

(1) the duty owed by one party to another, if any;

(2) the gravity of the infringement; any past infringements; mitigation and preventive actions taken by the data controller or data processor, including adherence to approved codes of conduct or safe harbors;

(3) the intentional or negligent character of the infringement;

(4) the unjust enrichment of a party by the use of personal data; and

(5) the need for general deterrence of violations to effectuate a Principle.

(d) *Assessing the gravity of the infringement.* The extent of the infringement may be determined by assessing the magnitude and likelihood of financial, reputational, or emotional harm, including the chilling effect on a data subject. The magnitude and likelihood of harm fall along a sliding scale. A significant risk may exist if there is a low likelihood of a high-magnitude injury or a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of concern.

(e) *Future injury.* The magnitude and likelihood of future injury can be assessed by examining different factors. These include the types of personal data involved in a violation of a Principle, the means and methods used to exploit these types of data, the ability of these data to be combined with other available data, and the types of harm and injury reasonably expected to result. A source of information to be drawn upon in evaluating these factors is the known injury, if any, to similarly situated victims.

(f) *The role of statutory law.* Statutory law can raise or lower the thresholds for finding harm and specify the kinds of harms that are remediable in different contexts.

(1) In some instances, a statute may deem certain legal violations of privacy interests as harmful per se with a designated minimum amount of statutory damages.

(2) Under some circumstances, the risk of future harm from a data privacy violation may cause anxiety or emotional distress. Such harms may be compensable pursuant to statute or if recognized by courts.

(3) In some instances, a statute may use the unjust enrichment of a data controller through violation of these Principles as a factor in assessing the extent of the infringement.