Florida Law Review

Volume 71 | Issue 2 Article 3

Towards a Global Data Privacy Standard

Michael L. Rustad

Thomas H. Koenig

TOWARDS A GLOBAL DATA PRIVACY STANDARD[1]

Michael L. Rustad[*] *& Thomas H. Koenig*[**]

Abstract

This Article questions the widespread contention that recent updates to European Union (EU) data protection law will drive a disruptive wedge between EU and United States (U.S.) data privacy regimes. Europe's General Data Protection Regulation (GDPR), which took effect in May 2018, gives all EU citizens easier access to their data, a right to portability, a right to be forgotten, and a right to learn when their data has been hacked. These mandatory privacy protections apply to non-EU companies that offer goods or services to EU consumers, whether through a subsidiary or a website. The "Brussels Effect" hypothesis projects a "race to the top" as multinational entities find it easier to adopt the most stringent data protection standards worldwide, rather than satisfying divergent data privacy rules. The GDPR is said to be a prime example of the Brussels Effect because of its aggressive extraterritorial scope that unilaterally imposes EU law on U.S. entities.

This Article acknowledges a Brussels Effect, but there is also an overlooked "D.C. Effect" reflected in the GDPR's adoption of many U.S. data privacy innovations. The GDPR imports long-established U.S. tort concepts for the first time into European privacy law, including deterrence-based fines, collective redress, wealth-based punishment, and arming data subjects with the right to initiate public enforcement. Under the GDPR, the EU Commission adopted "Privacy by Design" and security breach notification obligations, innovations pioneered in the U.S. The net effect of the GDPR is a bilateral transatlantic privacy convergence, which is rapidly evolving into a global data privacy

1. The authors would like to acknowledge the support, encouragement, and ideas of Professor Sara Dillon, who teaches European Union Law at Suffolk University and is Director of Suffolk University Law School's program at the National University of Ireland-Galway. The research and editorial contributions of Suffolk University Law School research assistants Gherardo Astaldi, Sarah E. Halstorm, Leonard Phillips, Gerardo Santali, Elizabeth Saylor, and Oliver Stark were very valuable. Elif Kavusturan, a Suffolk Law School SJD student, and Noe Leiva, Esquire provided insightful suggestions. Thanks also to Seth Markley, Michael Rustad's administrative assistant, for his technical and other assistance on this document.

* Michael L. Rustad, the Thomas F. Lambert Jr. Professor of Law, is the Co-Director of Suffolk University Law School's nationally ranked Intellectual Property Concentration. Professor Rustad is a member of the American Law Institute and served on the ABA Business Law Section's Subcommittee on Information Licensing. In 2017 and 2018, Professor Rustad taught law school courses on U.S. v. EU privacy law in Suffolk's summer program at the National University of Ireland-Galway.

** Thomas H. Koenig is a professor and former chair of the Sociology and Anthropology Department at Northeastern University in Boston. Professor Koenig is a founding member of both Northeastern University's Law and Public Policy and its Cybersecurity Ph.D. programs.

standard. Nations around the world, some U.S. states, and the major U.S.-based data processors are instituting policies harmonized with the GDPR.

This Article argues that the GDPR has the potential to not only bring an end to the transatlantic data privacy wars, but to become the basis of a worldwide "gold standard" for global data privacy.

INTRODUCTION 367

I. EU and U.S. Data Protection Compared 371
A. *The Fundamentals of EU Data Privacy Law* 372
1. EU Privacy as a Fundamental Right 372
2. Charter of Fundamental Rights of the European Union 373
3. Data Protection Directive of 1995.....373
4. The General Data Protection Regulation 375
B. *An Overview of U.S. Privacy Law*.....381
1. Sector-Specific Statutes 381
2. The FTC's Role as a National Data Privacy Constable.....381
3. FTC Enforcement Actions 383
4. Privacy-Based Torts.....384
5. The ALI's Data Privacy Principles Embody EU Privacy Norms 385

II. EVIDENCE OF A BRUSSELS EFFECT ON U.S. DATA PRIVACY LAW 387
A. *U.S. Companies Are Complying with the GDPR* 389
B. *U.S. Compliance with EU Data Transfer Rules*.....396
1. Safe Harbor 1.0 398
2. The ECJ's Reversal of Safe Harbor 1.0 400
3. Privacy Shield 402
4. Brussels Effect in the United States.....403
C. *Against the Brussels Effect: Areas of Divergence*.....405
1. The Right to Be Forgotten & U.S. Privacy Law.....405
2. The Right to Rectification.....409
3. EU Consumers Have Rights Just Beginning to Evolve in the United States.....410

III. THE "D.C. EFFECT" ON EUROPEAN DATA PROTECTION.....411
A. *How the United States Shapes EU Data Privacy Law*...411
1. Consent as a Common Cornerstone 412
2. Data Minimization 413
3. Privacy by Design 417
B. *"U.S.- Style" Remedies Imported into the GDPR*.....419

1. The GDPR Imports "U.S.-Style" Enforcement.....420
2. Data Security Breach Notification 422
3. The U.S. Pioneered Laws Protecting Children's Privacy.....424
4. Collective Redress Under the GDPR 425
5. Privacy Enforcement & Wealth-Based Punishment.....429

IV. TOWARDS A GLOBAL DATA PRIVACY STANDARD.....431
A. *The GDPR as a Global Privacy Standard*.....431
1. African Data Privacy Law is Generally Undeveloped 432
2. Most Asian Countries Align With the GDPR.....434
3. Central America's Data Protection Developments.....440
4. Eastern and Central America 441
5. The GDPR is in Effect in Europe.....441
6. Data Protection Development in the Middle East 442
7. GDPR Compliance in North America.....443
8. Oceania Data Protection Developments.....444
9. Data Protection Reform in South America 445
10. Data Privacy in the Caribbean.....448
B. *Evidence for an Emerging Global Data Privacy Standard*.....449

CONCLUSION 452

INTRODUCTION

Dublin's Silicon Docks is the center of operations for the European divisions of Twitter, Facebook, LinkedIn, and other top-ranked information technology companies.[2] These subsidiaries of United States (U.S.) multinational companies must either comply with European Union (EU) privacy law or withdraw from the largest economy in the world.[3]

2. Other examples of U.S.-based high technology companies with subsidiaries headquartered in Ireland include Google Dublin, Apple Operations Dublin, Cisco Galway, Dropbox, and Dell/EMC.

3. The European Commission Directorate-General for Trade stated:

> Although growth is projected to be slow, the EU remains the largest economy in the world with a GDP per head of €25 000 for its 500 million consumers. The EU is the world's largest trading block. The EU is the world's largest trader of manufactured goods and services. The EU ranks first in both inbound and outbound international investments. The EU is the top trading partner for 80

Michael Rustad taught a course titled "Emerging Issues in EU Business Law and Policy" analyzing the differences between EU and U.S. data protection regimes for the National University of Ireland-Galway's program in conjunction with Suffolk University Law School.

He took his law students to Twitter's Dublin headquarters, which is Twitter's principal office outside of California. Thomas Koenig, a guest speaker in Rustad's Emerging Issues class, participated in the meeting with Twitter's Direct Legal Counsel for European Operations. The lessons learned from speaking with the head of Twitter's public policy division and other transatlantic privacy experts led us to write this Article discussing how U.S. and EU data protection laws are converging into a globalized privacy standard.

This Article takes issue with the assertion that recent updates to EU data protection law will inevitably drive a disruptive wedge between EU and U.S. data privacy laws. Instead, this Article argues that the European General Data Protection Regulation's[4] (GDPR) convergences between EU and U.S. data privacy law far outweigh the divergent elements. Many industries in the U.S. have long followed information privacy practices paralleling the GDPR's newly recognized privacy rights.[5] For example, all fifty states enacted security breach notification laws decades before the GDPR gave European citizens the right to notice of a computer security breach affecting their data.[6]

The GDPR adopts long-established U.S. tort law remedies, including deterrence-based fines, bringing EU data protection law closer to American practices. Under the GDPR, collective redress, wealth-based punishment, and arming data subjects with the right to initiate public enforcement are recognized for the first time in European legislative

---

countries. By comparison the US is the top trading partner for a little over 20 countries.

EU Position in World Trade, EUR. COMM'N DIRECTORATE-GEN. TRADE, http://ec.europa.eu/trade/policy/eu-position-in-world-trade/ [https://perma.cc/2BGS-399V].

4. Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 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].

5. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999) (describing fair information privacy practices as "centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight").

6. "All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving identifiable information." *Security Breach Notification Laws*, NCSL (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/7ERK-K25Q].

history.[7] Innovations first instituted in the U.S., such as Privacy by Design, wealth-based punishment, and security breach notification obligations are essential to the GDPR. The net effect of this European recognition of the benefits of U.S. remedies is a bilateral transatlantic privacy convergence, rather than a divide, that is rapidly progressing into a global data privacy standard.

Part I of this Article compares EU and U.S. data privacy regimes, focusing on the differences between the European Union's centralized approach and the United States' segmented statutory approaches. While the United States and the European Union share privacy norms, they allot enforcement to disparate legal institutions.[8] EU privacy law is all-inclusive; it gives data subjects in the twenty-eight EU countries[9] and the three Member States of the European Free Trade Association (EFTA)[10] rights such as data breach notification, protections for data transferred across national borders, a right to rectify misleading information, and a right to be forgotten. In contrast to the European Union's single privacy standard, which applies to all economic sectors, the United States has traditionally employed privacy statutes calibrated to known risk factors in specific industries.[11]

U.S. multinational entities are frequently depicted as fighting in the trenches of a "transatlantic data war" as they face the thankless task of

7. GDPR, *supra* note 4, art. 83(4)–(5), at 82–83 (stating that fines are calibrated by two to four percent of the defendant's annual turnover depending upon the type of offense and aggravating factors).

8. Beneath the surface, the key is "privacy principles in Europe and the U.S. are thus quite similar, although our precise institutions for addressing privacy are different." *Internet Privacy: The Impact and Burden of EU Regulation: Hearing Before the Comm. on H. Energy & Commerce, Subcomm. on Commerce, Mfg. & Trade*, 112th Cong. 67 (2011) (statement of Peter P. Swire Professor, Moritz College of Law of the Ohio State University Center for American Progress).

9. The EU countries are: "Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK." *Countries in the EU and EEA*, GOV.UK, https://www.gov.uk/eu-eea [https://perma.cc/W6LW-8F7N].

10. These three EFTA member states are: Iceland, Lichtenstein and Norway. *Incorporation of the GDPR into the EEA Agreement*, EUR. FREE TRADE ASS'N, http://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041 [https://perma.cc/C86G-3R83]. "The EEA includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market. Switzerland is neither an EU nor EEA member but is part of the single market - this means Swiss nationals have the same rights to live and work in the UK as other EEA nationals." *Countries in the EU and EEA*, *supra* note 9.

11. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 869 (2d ed. 2006) ("U.S. and foreign privacy regimes sometimes differ in some respects. Consider the description of privacy legislation in Europe as 'omnibus' and privacy law in the United States as 'sectoral.'").

complying with conflicting legal requirements.[12] Academic observers argue that the United States has a weak tradition of data privacy[13] that is diametrically opposed to the EU's expansive data privacy laws.[14] A prominent commentator asserts, "It is common knowledge that privacy in the market and the media is protected less in the United States than in Europe."[15] However, in practice, U.S. data subjects already have functionally equivalent rights to those under the GDPR in required notification or registration before their data is processed.[16]

Part II demonstrates that the GDPR reflects a Brussels Effect on U.S. data privacy law, which is "the unprecedented and deeply underestimated global power that the EU is exercising through its legal institutions and standards, and how it successfully exports that influence to the rest of the world."[17] The Brussels Effect projects a "race to the top" as multinational entities find it easier to apply the strongest data protection standards worldwide, rather than satisfying divergent data privacy rules.[18] For American corporations, conforming to the GDPR may be easier than it first appears because the United States shares core privacy norms with the European Union and much of its data privacy policy preceded the GDPR's expansion of European data subjects' rights.

Part III contends that the Brussels Effect is just one side of a bilateral transatlantic exchange of privacy innovations. The most significant

---

12. Henry Farrell & Abraham Newman, *The Transatlantic Data War: Europe Fights Back Against the NSA*, FOREIGN AFF. (2016), https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war [https://perma.cc/TK6C-DWJH].

13. Michael A. Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462 (2000) ("You have zero privacy. Get over it." (quoting Scott McNealy, CEO of Sun Microsystems)).

14. *See, e.g.*, Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1966–67 (2013).

15. Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 609 (2007).

16. Leuan Jolly stated:

> The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising and disclose that consumers can opt out of these practices, providing an opt-out mechanism. The GLB Act requires a financial institution to provide notice of its privacy practices, but does not have the same government regulator notification or registration requirements under Directive 95/46/EC on data protection (Data Protection Directive). The HIPAA requires a covered entity to provide notice to data subjects of its privacy practices and of data subjects' rights under HIPAA, but does not have the same government regulator notification or registration requirements as under the Data Protection Directive.

Leuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS: PRAC. L., https://us.practicallaw.thomsonreuters.com/6-502-0467 (last updated Oct. 1, 2018).

17. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 1 (2012).

18. *Id.* at 8.

elements of the GDPR are commonalities long found in both U.S. and EU law. The European Commission's adoption of U.S.-style remedies, including a victim's right to compensation from law-breaking data processors[19] and wealth-calibrated corporate fines,[20] demonstrates a significant "D.C. Effect" on EU data privacy law. Examples of this D.C. Effect include Privacy by Design, breach notification rules, deterrence-based fines, data subject damages suits, and the equivalent of class actions.

Part IV concludes that the GDPR's core principles are rapidly evolving into a *de facto* globalized data protection standard. Through the adoption of a single GDPR-compliant standard, companies can save the costs of pursuing multiple privacy policies. Microsoft, for example, is extending GDPR protection to all data subjects globally.[21] The authors' empirical study demonstrates that nations around the world are updating their data privacy laws to harmonize with the European Union's comprehensive data protection regime. The United States is a possible holdout because of the Trump Administration's recent attempt to blunt the impact of this increasingly adopted EU privacy law.[22] However, powerful forces are working toward producing an armistice in the transatlantic data privacy wars. For example, the state of California enacted a data privacy law that parallels the GDPR in July 2018,[23] and Senator Mark Warner (D-Va.) is proposing a related federal statute.[24]

I. EU AND U.S. DATA PROTECTION COMPARED

Robert Kagan's article in *The Economist* entitled "Old America v. New Europe" flips the usual argument that Europe is an old continent

19. "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." GDPR, *supra* note 4, art. 82(1), at 81.

20. *Fines and Penalties*, GDPR EU.ORG, https://www.gdpreu.org/compliance/fines-and-penalties/ [https://perma.cc/AW84-W2NQ].

21. Liam Tung, *Microsoft: We're Giving You all Euro-Style GDPR Rights over How We Use Your Data*, ZDNET (May 24, 2018, 12:56 PM), https://www.zdnet.com/article/microsoft-were-giving-you-all-euro-style-gdpr-rights-over-how-we-use-your-data/ [https://perma.cc/ 8KPD-6LVF].

22. "Sweeping statements made in an Executive Order issued five days into the Trump administration have cast doubt on the legal status of the EU-US Privacy Shield and have caused at least one highly-placed EU politician to challenge its continued legal viability." Belton Zeigler et al., *Data Protection Law – A Broken Shield*, 34 WESTLAW J. COMPUTER & INTERNET 2, 2 (2017).

23. Kristen J. Matthews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/ [https://perma.cc/9YLQ-WV3Q].

24. McGuire Woods, LLP, *Warner White Paper Floats Far-Ranging Privacy Proposals*, JD SUPRA (Sept. 7, 2018), https://www.jdsupra.com/legalnews/warner-white-paper-floats-far-ranging-39615 [https://perma.cc/TV8P-5MSN].

while America is a mere teenager.[25] Europe's privacy regime is a relatively new development, first comprehensively developed in the Data Protection Directive of 1995.[26] The United States is the senior citizen as many of the EU privacy innovations were prefigured in U.S. law. The GDPR brings EU privacy law in closer conformity to U.S. practices by adopting many market-based rights and remedies such as the class action or representative lawsuit and allowing data subjects to pursue individual redress. To understand the EU/U.S. privacy law's convergent and divergent aspects, it is necessary to look to history.

A. *The Fundamentals of EU Privacy Law*

1. EU Privacy as a Fundamental Right

Europeans have long valued "data protection—specifically, protection of the citizen against abuse of his or her data—and protection of privacy."[27] Data protection and privacy law in the European Union is in large part a reaction to Adolph Hitler's Nazi Party's creation of a total surveillance state from 1933–1945.[28] During World War II, Nazi officials seized "the central registry of France's *Sûreté nationale* (National Security), which concentrated approximately 650,000 individual records and 2 million nominative files."[29] Such databases permitted unprecedented oppression in Nazi-dominated countries and in large parts of Eastern Europe during the post-war period.[30] "Europe's experience from World War II has led to laws banning Holocaust denial and hate speech. More recent experiences with East Germany's police state have turned privacy into a fundamental right that can at times trump free expression."[31]

Many Warsaw Pact governments continued intercepting data during the Cold War. For example, shortly after the end of World War II, the East German government established the Stasi, a brutal secret police

25. Robert Kagan, *Old America v. New Europe*, THE ECONOMIST, Feb. 20, 2003.

26. Council Directive 94/45/EC, 1995 O.J. (L 281) 31 (EC).

27. ALVAR FREUDE & TRIXY FREUDE, ECHOES OF HISTORY: UNDERSTANDING GERMAN DATA PROTECTION 1 (2016), http://www.bfna.org/research/echos-of-history-understanding-german-data-protection/ [https://perma.cc/GV6D-XAKL].

28. *Id.* at 2.

29. Ivan Jablonka, *The Origins of Mass Surveillance Interview with Sophie Cœuré*, BOOKS & IDEAS (Arianne Dorval trans., Mar. 17, 2016), http://www.booksandideas.net/The-Origins-of-Mass-Surveillance.html [https://perma.cc/M8AM-T7UW].

30. FREUDE & FREUDE, *supra* note 27, at 2.

31. Nick Kostov & Sam Schechner, *EU Court to Rule on 'Right to Be Forgotten' Outside Europe*, WALL ST. J. (July 19, 2017, 9:56 AM), https://www.wsj.com/articles/eu-court-to-rule-on-right-to-be-forgotten-outside-europe-1500470225 [https://perma.cc/QH2N-59QV].

force,[32] which built a network of an astounding "174,000 informants for a population of barely sixteen million in 1989."[33] The Stasi disbanded in 1989, when the Berlin Wall fell, but concerns about threats to personal freedoms remain widespread.[34]

2. Charter of Fundamental Rights of the European Union

Both privacy and data protection are enshrined in The Charter of Fundamental Rights of the European Union because the sanctity of these rights is essential to Europeans.[35] Article 7 of the Charter recognizes general privacy protection for individuals by granting all Europeans "the right to respect for his or her private and family life, home and communications."[36] Article 8 expressly recognizes the right to protection of personal data, stating, "[D]ata must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[37] Europeans possess comprehensive privacy rights across all sectors.

3. Data Protection Directive of 1995

From 1995 to May 25, 2018, the Data Protection Directive (DPD) was in effect in Europe.[38] Directive 95/46/EC, adopted in 1995, had two objectives: (1) to protect the fundamental right to data protection and (2) to guarantee the free flow of personal data between Member States.[39] With the European Commission's approval of the DPD, the European community achieved greater harmonization of data protection. The DPD requires each of the twenty-eight Member States to enact national legislation that protects "the fundamental rights and freedoms of natural

32. Gary Bruce, *The Prelude to Nationwide Surveillance in East Germany: Stasi Operations and Threat Perceptions, 1945–1953*, 5 J. COLD WAR STUD. 3, 3 (2003).

33. JOHN C. SCHMEIDEL, STASI: SHIELD AND SWORD OF THE PARTY 26 (2008).

34. Chris Burns, *CIA Files Stir Up Specter of East German Secret Police*, CNN (Nov. 7, 1999, 8:40 PM), ("Yet intimidation was the Stasi's main weapon. Tens of thousands of agents closely monitored people with television and hidden movie cameras, listening devices and reports from hundreds of thousands of informants."), http://www.cnn.com/WORLD/europe/9911/07/berlin.wall.stasi/ [https://perma.cc/S524-9NP6].

35. Charter of Fundamental Rights of the European Union, arts. 7, 8, 2010 O.J. (C 83) 389, 393.

36. *Id.* art. 7.

37. *Id.* art. 8.

38. The protection of individuals with regard to the processing of personal data is governed by Council Directive 95/46/EC, 1995 O.J. (L 281) 31 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Council Directive 97/66, 1997 O.J. (L24) 1.

39. Council Directive 95/46/EC, *supra* note 38, art. 1, at 38.

persons, and in particular their right to privacy with respect to the processing of personal data."[40]

The DPD also requires that all companies' personal information be protected by adequate security.[41] Data subjects have the right to obtain copies of information collected, as well as the right to correct or delete personal data.[42] Software makers need to be mindful that consent must be obtained from the data subject prior to entering in to the license agreement or other contract.[43] Article 23 creates liability for companies that misuse or unlawfully process personal data.[44] A company may not transfer data to other countries without an "adequate level of protection."[45]

Companies targeting EU consumers must comply with EU privacy law. Google, for example, negotiated an agreement with the European Commission in 2008, agreeing to reduce the period in which it retains personally identifiable data to eighteen months.[46] Under the EU DPD, a company is required to get explicit consent from data subjects as to the collection of data on race, ethnicity, political opinions, union membership, physical health, mental health, sexual preferences, and criminal records.[47] Further, the company must implement adequate security to protect personal information.[48]

A "cultural lag" occurs where one element has not yet accommodated to developments in another.[49] Similar to a cultural lag, a "legal lag"

---

40. *Id.*

41. *Id.* art. 25(1), at 45.

42. *Id.* art. 12, at 42.

43. *Id.* art. 7, at 40.

44. "Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered." *Id.* art. 23, at 45.

45. *Id.* art. 25(3), at 46.

46. Drake Bennett, *Stopping Google*, BOS. GLOBE (June 22, 2008), http://archive.boston.com/bostonglobe/ideas/articles/2008/06/22/stopping_google/?page=full [https://perma.cc/8LBR-43XS].

47. Council Directive 95/46/EC, *supra* note 38, art. 8, at 40–41.

48. *Id.*

49. William Ogburn argues:

> [T]he various parts of modern culture are not changing at the same rate, some parts are changing much more rapidly than others; and that since there is a correlation and interdependence of parts, a rapid change in one part of our culture requires readjustments through other changes in the various correlated parts of culture.

occurs when laws fall behind disruptive societal developments, such as rapid technological change.[50] Recent technological advances in cyberspace have created a legal lag in EU data privacy protections.[51] The European data protection statutes are designed to keep up "with the fast pace at which IT-based services are developing and evolving."[52] The European Commission drafted the DPD of 1995 when the World Wide Web was in its infancy. Social networks, such as Facebook and Instagram, had not yet been invented.[53]

4. The General Data Protection Regulation

When scholars write the history of globalized data protection, they will commemorate May 25, 2018—the day the GDPR went into effect.[54] This legislation is the latest stage in a fifty-year EU effort to protect the

---

SOCIAL SCIENCE QUOTATIONS: WHO SAID WHAT, WHEN AND WHERE 175 (David L. Sills & Robert K. Merton eds., 2000) (reporting survey of American life commissioned by President Herbert Hoover and published during Franklin Delano Roosevelt's presidency).

50. Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 78 (2003).

51. In a book review of the *E-Business Legal Handbook*, Jerry Cohen stated:

> New technologies and new paradigms of commerce often outrun the law in the short term, but the law catches up. Catching up involves a common law reconsideration of classic legal constructs and legislative adjustments. The net result is a new branch of law with a more or less settled framework allowing for further growth of the new technology and new commercial paradigm. In retrospect, it appears that development of the new framework was inevitable. Often the sense of inevitability can be reinforced by studying precursors of current conflicts. Three diverse books reviewed here, taken together, show these trends for Internet-related businesses and social institutions.

Jerry Cohen, *Book Review*, 87 MASS. L. REV. 138, 138 (2003) (reviewing MICHAEL RUSTAD & CYRUS DAFTARY, E-BUSINESS LEGAL HANDBOOK (2003 ed.)).

52. *Proposal for an ePrivacy Regulation*, EUR. COMM'N, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation [https://perma.cc/Q3KQ-QHGS] (last updated Aug. 28, 2018).

53. Nicholas Carlson, *At Last – The Full Story of How Facebook was Founded*, BUS. INSIDER (Mar. 5, 2010), https://www.businessinsider.com/how-facebook-was-founded-2010-3 [https://perma.cc/8N2Q-PDGT] (reporting that Facebook was not released to the public until 2004).

54. A European *regulation* is a legal instrument binding in all of its part and, more importantly, it is self-executing, which means that it is immediately enforceable as law in all Member States. By contrast, a European *directive* is not self-executing, and it is binding on the Member States as to the result to be achieved but leaves to individual countries the choice of the form and method they adopt to realize the Community objectives within the framework of their internal legal order. Foreign Agric. Serv., *Difference Between a Regulation, Directive and Decision*, USDA: U.S. MISSION EUR. UNION, https://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision/ [https://perma.cc/5SSX-5UTB] (last updated Dec. 21, 2016).

personal data of EU consumers. The GDPR is a complex document consisting of eleven chapters, ninety-nine articles, and 173 recitals.[55] This Regulation is described as "the most contested law in the E.U.'s history, the product of years of intense negotiation and thousands of proposed amendments."[56] The GDPR defines personal data as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[57]

The GDPR recognizes that all "natural persons" have a "fundamental right[]" to "the protection of personal data."[58] The key provisions of the GDPR are: (1) an expanded jurisdictional reach applied to non-European companies processing the data of European consumers; (2) the duty to notify consumers of a data breach within twenty-four hours; (3) a requirement that companies obtain "specific, informed and explicit" consent before collecting personal data (opt-in provision); and (4) a company's duty to erase personal data upon demand (right to be forgotten).[59] The principal differences between the GDPR and its predecessor, the EU's DPD of 1995, are:

> 1. The definitions of personal data are much broader.
>
> 2. The scope of affected companies and organizations is also very broad and introduces the principle of extraterritoriality beyond the borders of the EU.

---

55. The eleven chapters of the GDPR are: (1) General Provisions, (2) Principles, (3) Rights of the Data Subject, (4) Controller and Processor, (5) Transfer of Personal Data to Third Countries or International Organizations, (6) Independent Supervisory Authorities, (7) Cooperation and Consistency, (8) Remedies, Liability and Penalties, (9) Provisions Relating to Specific Processing Situations, (10) Delegated Acts and Implementing Acts, and (11) Final Provisions. GDPR, *supra* note 4.

56. Julia Powle, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, NEW YORKER (May 25, 2018), https://www.newyorker.com/tech/elements/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy [https://perma.cc/7SMQ-WZWC].

57. GDPR, *supra* note 4, art. 4(1), at 33.

58. *Id.* art. 1(2), at 32.

59. Jeffrey M. Goetz, *A New World of EU Data Protection*, MARTINDALE (Feb. 2, 2012), https://www.martindale.com/corporate-law/article_Faegre-Baker-Daniels_1433012.htm [https://perma.cc/RGT7-NCUR] (emphasis omitted).

> 3. *The GDPR expands and builds the individual rights.* One of them is the right to be forgotten which came into effect a few years ago. Now individuals have several more rights like this one. Here they are:
>
> • *Right to be forgotten* – individuals can request to any company to delete all data it has for that individual
>
> • *Right to object* – individuals can prohibit certain uses of their data
>
> • *Right to rectification* – individuals can request incomplete data sets or incorrect data sets to be completed or corrected
>
> • *Right of portability* – individuals can request their personal data which has been stored by one company to be transferred to another
>
> • *Right of access* – individuals have the right to know what data is collected, how it's processed . . . .
>
> • *Right to be notified* – If a data [breach] occurs and it affects an individual's personal data in any way, this individual has a right to be informed within 72 hours of the organization first becoming aware from the breach. Authorities also have to be notified within that same time period.[60]

The GDPR applies to all U.S. and foreign business entities that either: (1) offer any goods or services in any of the thirty-one European Economic Area (EEA) nations[61] or (2) monitor the activities of data subjects within the EU.[62] Stringent new measures to protect European

60. *The Quick and Easy Guide for GDPR – Part 3 – GDPR in a Nutshell*, COURSEDOT (Mar. 15, 2018), https://blog.coursedot.com/index.php/2018/03/19/the-quick-and-easy-guide-for-gdpr-part-3-gdpr-in-a-nutshell/ [https://perma.cc/X2ZT-3SM9] (first emphasis added).

61. "Switzerland is neither an EU nor EEA member but is part of the single market - this means Swiss nationals have the same rights to live and work in the UK as other EEA nationals." *Countries in the EU and EEA*, *supra* note 9.

62. A U.S. company or any organization not established in Europe is subject to the GDPR "if it processes personal data of data subjects who are in the Union where the processing activities are related '*to the offering of goods or services*' (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or '*the monitoring of their behaviour*' (Article 3(2)(b)) as far as their behaviour takes place within the EU." DLA PIPER, DATA PROTECTIONS OF THE WORLD 2 (2017), https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=AT [https://perma.cc/U9E6-PBWK].

privacy on a global basis are justified on the grounds that technological advances have "resulted in the processing of EU residents' personal data outside the EU on a scale never seen before."[63]

The GDPR's aggressive extraterritorial scope contrasts with the EU's DPD of 1995, which asserts jurisdiction over non-EU entities only if these entities had an enterprise in Europe. Viviane Reding, the EU's Vice President and Justice Commissioner, maintained:

> [I]t would make no sense for the EU to assert fundamental rights for EU nationals, or a particular geographic region, but not for anyone else. Given the open nature of the internet, there had to be one data protection act to rule them all. It was a warning to US companies that they would not evade the reach of European law simply by being located in the US.[64]

Chapter 4, Section 1 of the GDPR establishes specific guidelines for data controllers and processors.[65] Section 2 imposes extensive rules for the security of personal data,[66] while Section 3 sets rules for data protection impact assessment and prior consultation.[67] Section 4 requires controllers and processors fulfilling certain requirements to designate data protection officers.[68] Article 39 specifies data protection officers' tasks, including regular and systematic monitoring of personally

63. Paul de Hert & Michal Czerniawski, *Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context*, 6 INT'L DATA PRIVACY L. 230, 230 (2016) (citing Lokke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 INT'L DATA PRIVACY L. 28 (2011)).

64. *See* Trevor Butterworth, *Europe's Tough New Digital Privacy Law Should Be a Model for U.S. Policymakers*, VOX (May 23, 2018, 6:46 AM), https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge [https://perma.cc/6T7W-SPUS] (quoting EU vice president and justice commissioner Viviane Reding).

65. Section 1 (Articles 24–28) spells out the duties of controllers. *See* GDPR, *supra* note 4, art. 24, at 47; *id.* art. 25, at 48; *id.* art. 26; *id.* art. 27, at 48–49; *id.* art. 28, at 49–50; *id.* art. 29, at 50; *id.* art. 30, at 50–51; *id.* art. 31, at 51.

66. *See id.* art. 32, at 51–52; *id.* art. 33, at 52; *id.* art. 34, at 52–53.

67. Section 3 of Chapter 4 of the GDPR titled, "Data protection impact assessment and prior consultation" consists of Article 35 (Data Protection Impact Assessment) and Article 36 (Prior Consultation). *See id.* arts. 35–36, at 53–55.

68. *See id.* art. 37, at 55 ("The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.").

identifiable data.[69] Section 5 regulates codes of conduct and certification.[70] Article 42 covers certification mechanisms as well as data protection marks and seals to assist the consumer in assessing the level of a website's security.[71]

All Member States must appoint independent public authorities to ensure compliance with the GDPR.[72] Article 56(1) of the GDPR provides that where a personal data controller or processor is established in more than one Member State, "the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."[73] Thus, all U.S. companies processing EU consumer data must identify their lead supervisory authority in order to comply with the GDPR.[74]

The GDPR provides for both greater centralization of data protection enforcement and a "consistency mechanism." This mechanism involves a new legal institution, the European Data Protection Board, which will closely study enforcement in Member States, to ensure the rules are uniform across the EEA countries.[75] "Articles 13(2)(f), 14(2)(g), and 15(1)(h) of the GDPR require data controllers to provide data subjects with information about the 'existence of automated decision-making, including profiling . . . .'"[76] Commentators read a right to explanation for automated processing into these provisions.[77] Doubts have been raised

69. *Id.* art. 39, at 56.

70. *Id.* § 5, at 56–60.

71. *Id.* art. 42, at 58–59.

72. *See id.* art. 51(1), at 61 ("[T]o be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').").

73. *Id.* art. 56(1), at 67.

74. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 173 (2015) (concluding that U.S. companies have enacted stronger privacy protections, in some respects, than European companies have).

75. *Proposal for a Regulation of the European Parliament and the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10 final (Oct. 1, 2017) [hereinafter *Eur. Comm'n Proposal*]; GDPR, *supra* note 4, art. 19, at 45.

76. Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIVACY L. 233, 233–34 (2017) (interpreting Articles 13–15 to only mandate limited information about automatic processing not an explanation of its logic or mechanics).

77. *Id.* at 235.

about "the legal existence and the feasibility" of a right to explanation of automated decision-making in the GDPR.[78]

On May 25, 2018, several U.S. media outlets[79] and other websites[80] went dark in Europe because these companies were not yet compliant with the GDPR data protection rules. When the authors attempted to access the *Chicago Tribune* from Europe on May 25, 2018, the following notice appeared:

> Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.[81]

---

78. Sandra W. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76, 76 (2017).

79. The Register reported:

> Folks trying to read the *NY Daily News*, say, or the *Chicago Tribune* – the third-biggest US daily newspaper – online from a location within the EU have been blocked from visiting the websites due to new data protection laws. Visitors in the bloc trying to load articles from the *Tribune*, or stablemates the *Los Angeles Times* – the fifth-biggest daily – and the *Orlando Sentinel* are shown the same error message from publisher Tronc[.]

Rebecca Hill, *U.S. Websites Block Netizens in Europe: Why are They Ghosting EU? It's Not You, It's GDPR*, REGISTER (May 25, 2018), https://www.theregister.co.uk/2018/05/25/tronc_chicago_tribune_la_times_gdpr_lock_out_eu_users/ [https://perma.cc/4TQU-UFSH].

80. Business World reported:

> Blanket blocking EU internet connections - which will include any U.S. citizens visiting Europe – isn't limited to newspapers. Popular read-it-later service Instapaper says on its website that it's "temporarily unavailable for residents in Europe as we continue to make changes in light of the General Data Protection Regulation." A&E Television Networks has narrowed its EU blockade to limit the damage to its audience. Websites for its History and Lifetime channels greet the European visitors with a message that its "content is not available in your area" . . . .

Tom Maguire, *U.S. Companies Block 500 Million Europeans Rather Than Deal with GDPR*, BUS. WORLD (May 27, 2018, 6:00 PM), https://www.independent.ie/business/world/us-companies-block-500-million-europeans-rather-than-deal-with-gdpr-36950038.html [https://perma.cc/HTY8-C5DW].

81. CHI. TRIB., http://www.tronc.com/gdpr/chicagotribune.com/ [https://perma.cc/6GXE-EHZF].

B. *An Overview of U.S. Privacy Law*

1. Sector-Specific Statutes

Data protection laws in the United States target only selected industries,[82] leaving Americans with significant gaps in data protection coverage. Examples of specific economic sectors in which federal laws address data privacy include the securities industry (SEC)[83], health care (HIPAA)[84], consumer financial services (GLBA)[85], and children's online privacy protection (COPPA).[86] One of the advantages of the U.S. approach is that its statutes are more granular and focused to the radius of the risk in a specific sector as opposed to Europe's one-size-fits-all approach to data privacy.[87] Data privacy and security must be tailored to the unique risks in an industry.[88]

2. The FTC's Role as a National Data Privacy Constable

The Federal Trade Commission (FTC) is the chief enforcer of federal privacy statutes, including the COPPA and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.[89] "In the United States legal landscape, sensitive information is accorded special recognition through a series of key privacy statutes."[90] The Federal Trade Commission Act (FTCA) prohibits unfair or deceptive practices and has been applied to both offline and online privacy and data security policies.[91] Health and Human Services' Office of Civil Rights (OCR) is

82. Many U.S. statutes target specific sectors. PRINCIPLES OF THE LAW: DATA PRIVACY intro. note at 2 (AM. LAW INST., Preliminary Draft No. 3, 2018) (listing Fair Credit Reporting Act, Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act, and Video Privacy Protection Act).

83. 17 C.F.R. pt. 248 (2018).

84. 45 C.F.R. pt. 160 (2017).

85. 15 U.S.C. § 6802 (2012).

86. 15 U.S.C. §§ 6501–06.

87. Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L. REV., no. 7, at 1, 4.

88. PRINCIPLES OF THE LAW: DATA PRIVACY § 13 cmt. b (AM. LAW INST., Preliminary Draft No. 3, 2018) ("Governance of data privacy and security cannot be one-size-fits-all. A major financial institution will require different privacy processes than an accountant with a solo practice. Small entities with personal data associated with high risk of harm need to take more measures than entities with personal data that poses a lesser risk of harm.").

89. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/3V4Q-MJ59] (last updated July 2008).

90. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 129 (2004).

91. The Federal Trade Commission has this description on its website:

responsible for enforcing the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule and Security Rule.[92] Enforcement and rulemaking responsibility for the Gramm-Leach-Bliley Act (GLBA)[93] privacy provisions was previously shared by eight federal agencies: the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Securities and Exchange Commission, and the Commodity Futures Trading Commission; however, at present, enforcement is delegated to the Consumer Financial Protection Agency.[94]

> The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector-specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.

Privacy & Data Security Update (2016), FED. TRADE COMM'N, https://www.ftc.gov/reports/privacy-data-security-update-2016 [https://perma.cc/XN8D-AY8Q] (last updated Jan. 2017).

92. The United States Department of Health and Human Services has this description on its website:

> HHS' Office for Civil Rights is responsible for enforcing the Privacy and Security Rules. Enforcement of the Privacy Rule began April 14, 2003 for most HIPAA covered entities. Since 2003, OCR's enforcement activities have obtained significant results that have improved the privacy practices of covered entities. The corrective actions obtained by OCR from covered entities have resulted in systemic change that has improved the privacy protection of health information for all individuals they serve. HIPAA covered entities were required to comply with the Security Rule beginning on April 20, 2005. OCR became responsible for enforcing the Security Rule on July 27, 2009. As a law enforcement agency, OCR does not generally release information to the public on current or potential investigations.

HIPAA Enforcement, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html [https://perma.cc/V6XC-SJM8] (last visited Nov. 14, 2018).

93. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

94. *WilmerHale Cybersecurity, Privacy and Communications Webinar: Financial Privacy Primer*, WILMERHALE (Mar. 23, 2017), https://www.wilmerhale.com/en/insights/events/2017-03-23-wilmerhale-cybersecurity-privacy-and-communications-webinar-financial-privacy-primer [https://perma.cc/XL2K-W8D6].

3. FTC Enforcement Actions

The FTC enforces privacy laws using its powers under Section 45 of the FTCA[95] to punish unfair and deceptive trade practices.[96] "[T]he FTC has stated that it is a violation of the FTC Act for a company to retroactively change its privacy policy without providing data subjects an opportunity to opt out of the new privacy practice."[97] The FTC's principal enforcement philosophy has been to sanction companies that break promises they made in their privacy notices.[98]

For example, the FTC filed a lawsuit against Wyndham Hotels "to provide reasonable and appropriate security for the personal information collected and maintained" exposing "consumers' personal data to unauthorized access and theft."[99] The FTC charged the hotel giant with failing to secure the personally identifiable information of its customers.[100] The FTC has entered into many additional settlements

95. Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended in scattered sections of 15 U.S.C.).

96. The Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45 (2012).

97. Jolly, *supra* note 16.

98. *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises [https://perma.cc/9UNV-QFV7].

99. First Amended Complaint for Injunctive & Other Equitable Relief at 10, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).

100. The FTC contended in its complaint against Wyndham:

> Since at least 2008, Defendants have disseminated, or caused to be disseminated, privacy policies or statements on their website to their customers and potential customers. These policies or statements include, but are not limited to, the following statement regarding the privacy and confidentiality of personal information, disseminated on the Hotels and Resorts' website[.]

Id. at 9. The hotel stated:

> Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by VeriSign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information – such as credit card numbers, online forms, and financial data – from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed.

Id. at 9–10. In reality, the Wyndham security was inadequate because it was improperly configured and implemented. *Id.*

requiring U.S. companies to change their practices.[101] "On June 13, 2014, for example, Sony settled for US$15 million a class action suit over a massive data breach for PlayStation users."[102] Between 2015 and 2017, the FTC employed its Section 5 powers in a large number of actions, including a $100 million penalty against LifeLock, after the identity protection company violated a 2010 order and failed to secure customers' personal data.[103] Aggrieved data subjects act as private attorneys general by filing tort lawsuits to supplement the enforcement of these statutes.[104]

4. Privacy-Based Torts

Louis Brandeis and his law partner, Samuel Warren, first proposed a new tort action for the invasion of privacy in an 1890 Harvard Law Review article.[105] The U.S. Supreme Court drew upon Warren and Brandeis in articulating the right to privacy as "the right to be let alone."[106] Courts and state legislatures began to recognize the right to

---

101. *See, e.g.*, *Electronic Toy Maker VTech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act*, FED. TRADE COMM'N (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated [https://perma.cc/FJ97-QAN7]; *Lenovo Settles FTC Charges it Harmed Consumers with Preinstalled Software on Its Laptops that Compromised Online Security*, FED. TRADE COMM'N (Sept. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled [https://perma.cc/ 4JDD-GJXT]; *Operator of Online Tax Preparation Service Agrees to Settle FTC Charges that It Violated Financial Privacy and Security Rules*, FED. TRADE COMM'N (Aug. 29, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges [https://perma.cc/SN62-RR6H]; *Privacy and Security Enforcement*, *supra* note 98.

102. Paul M. Schwartz, *Privacy and Security Law: What Korean Companies Need to Know*, PAUL HASTINGS, http://www.paulhastings.com/area/privacy-and-cybersecurity/privacy-and-security-law-what-korean-companies-need-to-know [https://perma.cc/N36N-HBZX].

103. *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges It Violated 2010 Order*, FED. TRADE COMM'N (Dec. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated [https://perma.cc/ALS7-4R74].

104. Congress has recognized private causes of action to supplement public recourse in many federal statutes:

> [A]s illustrated by civil and criminal penalties of the Racketeer Influenced and Corrupt Organizations Act (RICO), federal securities laws, antitrust law, and much of environmental law. This theme of private litigants uncovering misconduct involving and thereby benefiting the larger society is also found in civil forfeiture litigation, civil rights cases, and whistleblower actions.

Michael L. Rustad, *Torts as Public Wrongs*, 38 PEPP. L. REV. 433, 527 (2011).

105. *See generally* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (discussing a tort action based on the right to privacy).

106. Katz v. United States, 389 U.S. 347, 350 & n.6 (1967).

privacy shortly after this publication.[107] "It has been said that a 'right of privacy' has been recognized at common law in 30 states plus the District of Columbia and by statute in four States."[108]

Causes of action for invasion of privacy are comprised of four analytically distinct torts: (1) intrusion upon seclusion, (2) appropriation of name or likeness, (3) publicity given to private life, and (4) publicity placing person in false light.[109] Not all jurisdictions recognize all four forms of this privacy-based tort.[110] Some U.S. jurisdictions have enacted privacy statutes recognizing the common law torts.[111] Courts have been unwilling to find the publishing of disciplinary action on a website to be an invasion of privacy where the information is part of a public record.[112] Selling, transferring, transmitting, and manipulating personal data is the lifeblood of e-commerce and such activities are mostly beyond the reach of tort actions. Courts have largely been disinclined to stretch the tort of privacy to online surveillance and other Internet-related intrusions.[113]

5. The ALI's Data Privacy Principles Embody EU Privacy Norms

The American Law Institute (ALI) is a private organization of leading law professors and practitioners that proposes law reforms for legislative

---

107. The U.S. Supreme Court in *Time Inc. v. Hill*, 385 U.S. 374 (1967), noted how New York's statute was enacted a year after *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (N.Y. 1902). *Time, Inc.*, 385 U.S. at 380. The New York Court of Appeals traced the development of the right to privacy to a

> celebrated article of Warren and Brandeis, entitled The Right to Privacy . . . . The Court of Appeals, however, denied the existence of such a right at common law but observed that "[t]he legislative body could very well interfere and arbitrarily provide that no one should be permitted for his own selfish purpose to use the picture or the name of another for advertising purposes without his consent."

Id. at 380–81 (quoting *Roberson*, 64 N.E. at 443). The court observed that New York's privacy statute was a direct response to Warren and Brandeis' law review article. *Id.* at 381.

108. *Id.* at 383 n.7 (citing PROSSER, LAW OF TORTS at 831–32 (3d ed. 1964)).

109. Many states recognize four types of interests protected by a person's right to privacy: (1) unreasonable intrusions upon the seclusion of another, (2) appropriation of the other's name or likeness, (3) unreasonable publicity given to the other's private life, and (4) publicity that unreasonably places the other in a false light before the public. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977); *see also id.* § 652A (describing an invasion of privacy).

110. Colorado, for example, does not recognize false light privacy. *See* Shrader v. Beann, 503 F. App'x 650, 654 (10th Cir. 2012) (applying Colorado law).

111. *How U.S. State Law Quietly Leads the Way in Privacy Protection*, PRIVACILLA.ORG (July 2002), http://www.privacilla.org/releases/Torts_Report.html [https://perma.cc/47R2-7VNF].

112. *See* RESTATEMENT (SECOND) OF TORTS § 652B.

113. *See id.*

enactment.[114] The ALI's project, Principles of the Law: Data Privacy, "aims to provide a framework for regulating data privacy and for duties and responsibilities – best practices – for entities that process personal data."[115] The ALI's data privacy principles are aligned with the GDPR in its individual notice, consents, confidentiality, use limitation, access and correction rights, data retention and disposal duties, data portability, data security, and onward transfer rules.[116]

The ALI's data privacy project is neither a statute nor a restatement. Rather, it is a law reform project composed of policy recommendations addressed to "legislatures, administrative agencies, or private actors . . . where an area is so new that there is little established law."[117] The ALI proposal "is expected to include three Chapters: Purpose, Scope, and Definitions; Data Privacy Principles; and Accountability and Redress."[118] The ALI's Council has approved Sections of Chapters 1 and 2, including "Purpose and Scope of the Data Privacy Principles; Definitions; Transparency Statement; and Individual Notice."[119]

The ALI Reporters assembled many sectoral statutes restricting "secondary use of data," which closely parallel the GDPR's data minimization principle.[120] The ALI proposes recognizing data privacy principles such as individual notice, consent, confidentiality, data minimization, access and rectification, data retention and disposal, data portability and data security rights, thereby aligning much of U.S. privacy law with that of the European Union.[121] The ALI's concept of "accountability" in U.S. information privacy law was imported from the Organization for Economic Cooperation and Development (OECD),[122] reflecting the growing affinities between U.S. and EU privacy law. This

114. "[The American Law Institute] is the leading independent organization in the United States producing scholarly work to clarify, modernize, and otherwise improve the law." AM. L. INST., https://www.ali.org/ [https://perma.cc/S8XZ-HXML].

115. *Principles of the Law: Data Privacy*, AM. L. INST., https//www.ali.org/projects/show/adata-privacy/ [https://perma.cc/FRR7-K99L].

116. PRINCIPLES OF THE LAW: DATA PRIVACY ch. 2 (AM. LAW INST., Preliminary Draft No. 3, 2018).

117. *Id.* at xi ("Principles are primarily addressed to legislatures, administrative agencies, or private actors. They can, however, be addressed to courts when an area is so new that there is little established law. Principles may suggest best practices for these institutions.").

118. PRINCIPLES OF THE LAW: DATA PRIVACY, *supra* note 116.

119. *Id.*

120. Among the key provisions are: Privacy Act, 5 U.S.C. § 552(a)(e)(3)(B) (2012); Fair Credit Reporting Act, 15 U.S.C. § 1681b (2012); Driver's Privacy Protection Act, 18 U.S.C. § 2722(a) (2012); Cable Communications Policy Act, 47 US.C. § 551(e) (2012); Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(c); and the Video Privacy Protection Act, 18 U.S.C. § 2710(e).

121. PRINCIPLES OF THE LAW: DATA PRIVACY §§ 4–11.

122. *Id.* § 13 reporters' note 2.

common origin of U.S. and EU privacy law is evidence for the authors' thesis that EU and U.S. law are not so different after all.

II. EVIDENCE OF A BRUSSELS EFFECT ON U.S. DATA PRIVACY LAW

U.S. industry advocates have argued the GDPR is pushing the United States and Europe apart by impermissibly placing Europeans in the data protection driver's seat.[123] American conservative public policy think tanks contend that the GDPR intensifies the transatlantic conflict in data protection standards. For example, a Heritage Foundation senior research fellow views the GDPR as a form of EU "imperialism" that is hostile to U.S. free market principles:

> Together with an EU directive governing the processing of personal information by government authorities, the GDPR will mark the beginning of another phase in a long-running struggle between the U.S. and the EU over the handling of individual data by U.S. corporations and the U.S. government.
>
> . . . .
>
> . . . [T]he EU has persistently and hypocritically raised the bar in its demands on the U.S.—and only on the U.S. The EU sees no problem when European data is transferred to China or Russia . . . . The U.S. has approached the EU as a friend, but it has been treated worse than China. It is therefore time for the U.S. to stop being played for a fool, to recognize the EU's hostility, and—before the GDPR takes effect—to take measures that will force the EU to recognize that the U.S. will not stand by as the EU exerts legal authority over U.S. firms that have the temerity to be commercially successful.[124]

Critics charge that the "GDPR creates serious, unclear legal obligations for both private and public sector entities, including the U.S. government. We do not have a clear understanding of what is required to comply. That could disrupt transatlantic co-operation on financial

123. "For now, GDPR, which replaces previous EU mandates on data collection and use, differs significantly from U.S. law, pushing the two regions further apart in their approaches to regulating the digital economy." Larry Downes, *GDPR and the End of the Internet's Grand Bargain*, HARV. BUS. REV. (Apr. 9, 2018), https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain [https://perma.cc/P9LH-K5HQ].

124. Theodore Bromund, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*, HERITAGE FOUND. (Jan. 9, 2018), https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism [https://perma.cc/268U-X3W6].

regulation, medical research, emergency management co-ordination, and important commerce."[125] Another commentator notes that the "United States and the European Union not only have different notions of what personal data includes, but also operate under two very different definitions of privacy more generally . . . ."[126]

U.S. privacy law imposes "fewer restrictions on how much personal data may be collected, how such data may be used, and how long that data may be kept."[127] European data protection[128] is criticized for driving up the price tag of goods and services through unwarranted regulations.[129] Critics dismiss the GDPR as another example of "more protectionism from the EU, which has challenged American tech platforms on antitrust and privacy grounds with expensive consequences."[130] The GDPR is said to create fundamentally clashing data privacy rules, potentially fragmenting the globalized Internet into a "splinternet."[131]

---

125. Scott Bicheno, *GDPR Seems to Benefit Silicon Valley but Harm U.S. Relations*, TELECOMS.COM (May 31, 2018, 6:03 PM), http://telecoms.com/490036/gdpr-seems-to-benefit-silicon-valley-but-harm-us-relations/ [https://perma.cc/2245-WFZX].

126. Emily Linn, *A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement*, 50 VAND. J. TRANSNAT'L L. 1311, 1315 (2017).

127. Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 LAW & CONTEMP. PROBS. 231, 236 (2015); *see also* Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L REV. 1966, 1967 (2013) ("As an initial matter, the EU is skeptical regarding the level of protection that U.S. law actually provides. Moreover, despite the important role of the United States in early global information privacy debates, the rest of the world has followed the EU model and enacted EU-style 'data protection' laws.").

128. Europeans use the term "protection" as opposed to the U.S. where it is the "right to privacy." Data Protection "reflects the modern concept of privacy protection that emerged in the 1970s as computer systems were increasingly used to process information on citizens." SOLOVE & SCHWARTZ, *supra* note 11, at 870. However, a "concept of privacy, sometimes referred to as that of private life or the private domain, continues to play an important role in the European conception of information privacy." *Id.*

129. It is a long-standing stereotype that the EU Commission has created unnecessary and costly privacy regulations. *Ministers to Scythe Down Forest of Outdated Laws,* EVENING STANDARD (LONDON), Nov. 18, 1994, at 35 ("'Unnecessary regulations push up industry's costs,' concluded Forsyth [UK Home Minister]. . . . Forsyth attacked the growth of regulations being issued by the European Union and said the proposed Data Protection Directive would cost business an estimated £2.4 billion to implement."); *see also Death by Footnote for Privacy Law*, INDEP. (LONDON) (June 23, 1995), https://www.independent.co.uk/news/world/death-by-footnote-for-privacy-law-1587829.html [https://perma.cc/24A5-QN72] (expressing opposition to data retention rules of the Data Protection Directive of 1995).

130. Nitasha Tiku, *Europe's New Privacy Law Will Change the Web, and More*, WIRED (Mar. 19, 2018, 6:00 AM), https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/ [https://perma.cc/AGH3-BCE7].

131. L.S., *What is the "Splinternet"? The Internet Is at Risk of Breaking up into National and Regional Networks*, ECONOMIST (Nov. 22, 2016), https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [https://perma.cc/6EC2-C39K].

In Professor Anu Bradford's article, "The Brussels Effect," she argues that "rules and regulations originating from Brussels have penetrated many aspects of economic life within and outside of Europe through the process of 'unilateral regulatory globalization.'"[132] According to Bradford, "Unilateral regulatory globalization is a development where a law of one jurisdiction migrates into another in the absence of the former actively imposing it or the latter willingly adopting it."[133]

Bradford notes that the EU Commission externalizes its privacy norms "outside its borders through market mechanisms."[134] Jurisdictions around the globe are in the process of enacting new legislation conforming to the EU's new privacy laws.[135] California's Consumer Rights Privacy Act of 2018 provides the latest example of the Brussels Effect.[136] U.S. multinationals find it easier to apply the strongest data protection standards worldwide, rather than to have multiple rules for protecting privacy. Conforming to the GDPR may be easier than it first appears because U.S. data privacy policy has strongly influenced the EU's new data protection laws.

A. *U.S. Companies Are Complying with the GDPR*

Under the threat of being assessed catastrophic fines or ceasing offering sales or services to EU consumers, U.S. online companies need to align their data protection policies with the requirements of the GDPR. "For U.S. organisations with business operations in Europe, the European Union (EU) approach to regulation of data privacy or 'data protection' can seem like a logistical quagmire."[137] Some question whether the panic

132. Bradford, *supra* note 17, at 3.

133. *Id.* at 4.

134. *Id.* at 3.

135. Jeffrey Ritter et al., *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87, 87 (2001).

136. Dom Nicastro, *What Is the California Consumer Privacy Act of 2018 and How Does It Affect Marketers?*, CMS WIRE (Aug. 28, 2018), https://www.cmswire.com/customer-experience/what-is-the-california-consumer-privacy-act-of-2018-and-how-does-it-affect-marketers/ [https://perma.cc/AH8E-YZJE].

137. Kenneth Mullen, *EU Data Protection Reform—What Does it Mean for US Organisations?* WITHERSWORLDWIDE (Oct. 22, 2015), https://www.withersworldwide.com/en-gb/insight/eu-data-protection-reform-what-does-it-mean-for-us-organisations [https://perma.cc/Z56Y-NV6L]. It is noted that:

> There will be one GDPR although the regime of different national data supervisory authorities to enforce the regulation will remain in place. At the same time US data controller organisations with multiple business establishments Europe will have a 'lead' regulatory authority in the EU state where their main operations takes place to supervise their data processing activities.

Id.

over the GDPR, similar to Y2K, is "all hype, no consequence."[138] However, shortly after the effective date, internet users received complicated pop-ups "because the GDPR wants specific consent for specific purposes, not blanket acceptances. For example, OneTrust's consent utility has sections for strictly necessary cookies (needed for the site to work), performance and analytics cookies, functional cookies (for extra services, such as live chat), and targeting/marketing cookies."[139]

The GDPR has led to "'three levels of denial' from companies, including avoiding compliance, rebranding policies or playing the 'wait and see' game."[140] In the immediate aftermath of the GDPR's effective date, "users around the globe found their inboxes flooded with privacy policy updates."[141] An empirical study of leading information technology companies demonstrated the length of and the reading level needed to understand privacy policies increased:

> Surprisingly, given that GDPR aimed to increase transparency around privacy policies, many reading levels increased — the average change in reading level was up almost 4 percent. eBay clocked in with the highest reading level, at 20.
>
> - Lowest reading level (before GDPR): Facebook; 11
> - Lowest reading level (after GDPR): Reddit; 12
> - Highest reading level (before GDPR): eBay; 18
> - Highest reading level (after GD[P]R): eBay; 20
>
> Overall, Wikipedia clocked in with the largest update (word count increase) and eBay came in with the highest reading level (20).[142]

138. Trevor Butterworth, *Europe's Tough New Digital Privacy Law Should be a Model for US Policymakers*, VOX (May 23, 2018, 6:45 AM), https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge [https://perma.cc/6HZ3-D5C3].

139. Jack Schofield, *What Should I Do About All the GDPR Pop-ups on Websites?*, GUARDIAN (July 5, 2018, 11:01), https://www.theguardian.com/technology/askjack/2018/jul/05/what-should-i-do-about-all-the-gdpr-pop-ups-on-websites [https://perma.cc/Q3FU-NRK2].

140. Samantha Ann Schwartz, *No Company Wants to Become the 'Guinea Pig' of GDPR*, CIO DIVE (June 6, 2018), https://www.ciodive.com/news/no-company-wants-to-become-the-guinea-pig-of-gdpr/524916/ [https://perma.cc/V6FU-QHBB].

141. Sheeraz Raza, *How GDPR Has Changed Privacy Policies at Google, Facebook, Reddit, Amazon, Wikipedia, Yahoo, Twitter, eBay, Instagram & Netflix*, VALUEWALK (July 18, 2018, 12:31 PM), https://www.valuewalk.com/2018/07/privacy-policy-updates-gdpr/ [https://perma.cc/GK2A-E3LZ].

142. *Id.*

As the GDPR applies to all businesses, irrespective of location, that offer goods or services in the EU or monitor the activities of EU citizens, the GDPR, in effect, creates a statutorily protected consumer privacy bill of rights throughout the Eurozone.[143] All U.S. companies could either comply with the GDPR or cease offering sales and services to EU consumers.[144] While this may formally be a free choice, there is no real alternative for most major U.S. companies.[145]

Chart One reveals that U.S. information industry titans are pledging to change their companies' operations to achieve GDPR data privacy compliance. As predicted by the Brussels Effect, it is more cost-effective for a multinational entity to satisfy a single legal standard rather than multiple divergent standards that sometimes conflict.[146] Some smaller U.S. companies perceive the Brussels Effect as so onerous that they are blocking European users in order to avoid the costs and burden of complying with the GDPR.[147]

Chart One: Technology-Leading Companies Agree to Implement GDPR

U.S. Company	*Company Position on Compliance with the GDPR*	*What Company Is Doing to Comply with the GDPR*
Amazon Web Services	"AWS is committed to offering services and resources to our customers to help them comply with GDPR requirements that may apply to their activities."[148]	"This announcement confirms we have completed the entirety of our GDPR service readiness audit, validating that all generally available services and features

143. *Id.*

144. The definition of a Hobson's choice is "free choice when there is no real alternative." *Hobson's Choice*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/Hobson's%20choice [https://perma.cc/7ZP2-G4S3].

145. *Id.*

146. "As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based." *2018 Reform of EU Data Protection Rules*, EUR. COMM'N, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en [https://perma.cc/XXB8-RL4J].

147. Mike Masnick, *Companies Respond to the GDPR by Blocking all EU Users*, TECHDIRT (May 10, 2018, 3:26 AM), https://www.techdirt.com/articles/20180509/14021739811/companies-respond-to-gdpr-blocking-all-eu-users.shtml [https://perma.cc/BEB9-MHY3] (stating that Tunngle, Drawbridge, and Steel Root have blocked EU access to avoid compliance with the General Data Protection Regulation (GDPR)).

148. *General Data Protection Regulation (GDPR) Center*, AWS, https://aws.amazon.com/compliance/gdpr-center/ [https://perma.cc/E62K-3C7M].

		adhere to the high privacy bar and data protection standards required of data processors by the GDPR. We completed this work two months ahead of the May 25, 2018 enforcement deadline in order to give customers and APN partners an environment in which they can confidently build their own GDPR-compliant products, services, and solutions."[149]
eBay	"We embrace the GDPR as an opportunity to demonstrate and deepen our commitment to protecting your data."[150]	"eBay is making enhancements to its processes, products, contracts, and documentation to help support the company's, and our partner's, compliance with the GDPR."[151]
Google Cloud	"You can count on the fact that Google is committed to GDPR compliance across G Suite and Google Cloud Platform services. We are also committed to helping our customers with their GDPR compliance journey by providing them with robust privacy and security protections we have built into our services and contracts over the years."[152]	"G Suite and Google Cloud Platform customers will typically act as the data controller for any personal data they provide to Google in connection with their use of Google's services."[153]

149. Chad Woolf, *All AWS Services GDPR Ready*, AWS: SECURITY BLOG (Mar. 26, 2018), https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/ [https://perma.cc/LWD7-7N54].

150. *eBay's Commitment to GDPR*, EBAY, https://www.ebayinc.com/our-company/privacy-center/gdpr/ [https://perma.cc/Z4VZ-6DRS].

151. *Id.*

152. *Id.*

153. *Google Cloud & the General Data Protection Regulation (GDPR)*, GOOGLE, https://www.google.com/intl/en_ca/cloud/security/gdpr/ [https://perma.cc/J7ZR-GTE6] (footnote omitted).

Facebook	"[Mark] Zuckerberg indicated during his congressional testimony and in subsequent statements that Facebook would voluntarily extend GDPR-like protections such as informed consent to users worldwide — not only to those in the EU."[154]	"At Facebook, preparations are well underway to ensure that our products and services comply with the GDPR. Facebook and its affiliates, including Instagram, Oculus and WhatsApp, will all comply with the GDPR. . . . We are also meeting with regulators, legislators, experts and academics from around the world to seek feedback."[155]
Twitter	"Twitter has users and advertisers that span the globe, so we are working to ensure that our services comply with GDPR, and that advertisers around the world can continue to use our advertising products and services after GDPR takes effect on 25 May 2018. . . . Additionally, Twitter International Company has Data Transfer and Processing Agreements with Twitter, Inc., in the U.S., and its affiliates, which allow Twitter, Inc., to process personal data. Twitter, Inc., is also certified under the Privacy Shield . . . framework."[156]	"Twitter's controller and processor activities are determined by the terms governing your use of our advertising services and our Privacy Policy . . . , both of which will be updated accordingly before 25 May 2018, and will be made available for your review prior to that date. . . . Twitter is the controller of data it receives through the Twitter pixel and through mobile app conversion tracking partners. Twitter requires advertisers to have notice and consent mechanisms in place in connection with their use of this program, as

154. Joseph V. Moreno & Keith M. Gerver, *United States: Will Facebook Firestorm Yield Tougher U.S. Data Privacy Standards?*, MONDAQ (Apr. 27, 2018), http://www.mondaq.com/unitedstates/x/696436/data+protection/Will+Facebook+Firestorm+Yield+Tougher+US+Data+Privacy+Standards [https://perma.cc/43CT-R9PQ].

155. *Facebook's Commitment to Data Protection and Privacy in Compliance with the GDPR*, FACEBOOK (Jan. 29, 2018), https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr [https://perma.cc/ VD4B-5PKX].

156. *Twitter for Business FAQ*, TWITTER (2019), https://gdpr.twitter.com/en/faq.html [https://perma.cc/C2E6-E44Y].

		described in our Conversion Tracking Program T&Cs."[157]
Microsoft	"The GDPR represents one of the most complex compliance-focused engineering efforts ever undertaken at Microsoft. Regulatory, compliance, legal, HR, operations, business, and engineering teams have to work together to orchestrate cross-company activities."[158]	"To ensure we are compliant by May 25, 2018, we needed to verify our compliance during the implementation phase and establish mechanisms for ongoing verification of compliance."[159]

In April of 2018, Facebook's CEO, Mark Zuckerberg, testified before the Senate Judiciary Committee and the Senate Commerce, Science, and Transportation Committee, responding to questions about Facebook's data privacy practices in the aftermath of the company's Cambridge Analytica scandal.[160] In his prepared testimony, Zuckerberg took personal responsibility for not sufficiently overseeing Facebook's privacy practices.[161] Zuckerberg acknowledged that lax supervision led to the widespread misuse of the personally identifiable information of millions of Facebook users:

> But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake.[162]

157. *Id.*

158. *Journey to GDPR Compliance*, MICROSOFT 14, https://clouddamcdnprodep.azureedge.net/asm/1736412/Original [https://perma.cc/TT65-BE2K].

159. *Id.* at 11.

160. Zuckerberg acknowledged that Cambridge Analytica used personal data from 87 million Facebook users to influence the U.S. Presidential Election and other elections around the world. *Mark Zuckerberg Testimony to House Commerce Committee—As It Happened*, CBS NEWS (Apr. 11, 2018, 3:50 PM), https://www.cbsnews.com/live-news/mark-zuckerberg-testimony-to-house-commerce-committee-live-updates/ [https://perma.cc/672H-LEJ8].

161. *See id.*

162. *Testimony of Mark Zuckerberg Chairman and Chief Executive Officer, Facebook: Hearing Before the U.S. H.R. Comm. on Energy and Commerce*, 115th Cong. 1 (2018).

Shortly before his congressional testimony, Zuckerberg promised to extend GDPR privacy protections to Facebook users "in spirit."[163] A U.S. senator asked Zuckerberg whether he believed the GDPR "should be applied here in the U.S."[164] In explaining how Facebook would comply with the GDPR worldwide, Zuckerberg stated, "So I think it's certainly worth discussing whether we should have something similar in the U.S. But what I would like to say today is that we're going to go forward and implement that, regardless of what the regulatory outcome is . . . ."[165] In the House Commerce Committee Hearing, Zuckerberg stated that Facebook is compliant with most GDPR requirements: "The GDPR requires a few more things, and we'll make that available around the world," he promised.[166]

Similarly, Microsoft and Google both agreed to become GDPR compliant. Microsoft took out a full-page advertisement in the *New York Times*, contending the GDPR was going to give them a competitive advantage in engendering consumer trust:

> It may seem to some that the European Union reforms — and other data privacy protections popping up worldwide — are yet another regulatory burden for which companies must absorb the cost. But that doesn't have to be the case. Data privacy compliance can provide a distinct competitive advantage and business opportunity . . . .
>
> By choosing the right tools to protect customer privacy, companies can reshape their data practices in ways that reap cascading benefits. Compliance provides a way to win customer trust. And tackling inventory and discovery in a strategic manner can improve firms' agility and efficiency.[167]

---

163. David Ingram & Joseph Menn, *Exclusive: Facebook CEO Stops Short of Extending European Privacy Globally*, REUTERS TECH. NEWS (Apr. 3, 2018, 4:39 PM), https://www.reuters.com/article/us-facebook-ceo-privacy-exclusive/exclusive-facebook-ceo-stops-short-of-extending-european-privacy-globally-idUSKCN1HA2M1 [http://perma.cc/6A9S-VKP4].

164. Wayne Rash, *Social Media Data Regulation Appears Likely After Zuckerberg Testimony*, EWEEK (Apr. 11, 2018), http://www.eweek.com/security/social-media-data-regulation-appears-likely-after-zuckerberg-testimony [https://perma.cc/TG3V-BPLT].

165. *Id.* (responding to question asked by Sen. Maria Cantwell (D-Wash.)).

166. *Id.* (responding to question asked by Rep. Al Green (R-Tex.)).

167. Microsoft, *There's a Data Crackdown Coming. Why It's Good for Customers and Business*, N.Y. TIMES, https://paidpost.nytimes.com/microsoft/theres-a-data-crackdown-coming.html?tbs_nyt=2018--nytnative_hpmod&cpv_dsm_id=20174233 [https://perma.cc/B5YX-MAAT].

In May of 2018, Microsoft announced it was going to "extend the rights that are at the heart of GDPR to all of our consumer customers worldwide."[168] Microsoft declared, "We are committed to GDPR compliance across our cloud services and provide GDPR related assurances in our contractual commitments."[169] Microsoft's Data Subject Rights "include the right to know what data we collect about you, to correct that data, to delete it and even to take it somewhere else."[170] Similarly, Google committed to compliance with the GDPR specifically in its cloud computing activities.[171] U.S. companies are also acceding to the GDPR rules for transferring EU citizens' personally identifiable data to third countries.[172] These are clear examples of the power of the Brussels Effect in shaping company privacy practices.

B. *U.S. Compliance with EU Data Transfer Rules*

The GDPR makes it clear that complying with the data processing obligations is mandatory for any transfers of personal data to third countries or international organizations, including onward transfers.[173] Article 44 of the GDPR sets forth the general standard for data transfers to third countries:

> Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are

168. Wayne Rash, *How Enterprises Can Make GDPR a Global Data Privacy Standard*, EWEEK (May 29, 2018), http://www.eweek.com/security/how-enterprises-can-make-gdpr-a-global-data-privacy-standard [https://perma.cc/YE4T-LQ9U].

169. *Preparing for a New Era in Privacy Regulation*, MICROSOFT, https://www.microsoft.com/en-us/trustcenter/privacy/gdpr [https://perma.cc/6RJQ-KFUV]. "We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. We want to help you focus on your core business while efficiently preparing for the GDPR." *GDPR - Impact & Getting Compliant*, MICROSOFT, https://info.microsoft.com/WE-GDPR-WBNR-FY18-11Nov-11-GDPRimpactandgettingcompliant-MCW0002601_02OnDemandRegistration-ForminBody.html?wt.mc_id=AID652299_QSG_SCL_230915 [https://perma.cc/X428-8RKU].

170. Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT: MICROSOFT ON ISSUES (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ [https://perma.cc/383U-ENGJ].

171. "Google is committed to complying with the EU General Data Protection Regulation (GDPR) . . . for G Suite and Google Cloud Platform services." *Standards, Regulations & Certifications*, GOOGLE, https://cloud.google.com/security/compliance/gdpr/ [https://perma.cc/4T7V-8LP7].

172. *Id.*

173. GDPR, *supra* note 4, art. 44, at 60.

> complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.[174]

As with the DPD, onward transfers of EU personal data cannot be completed without a finding that the recipient country has adequate data protection:

> 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
>
> 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States;

174. *Id.*

and

> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.[175]

The GDPR adopts more specific rules for data transfers to third countries,[176] strengthening the provisions pioneered by Article 25 of the DPD of 1995. Transfers of personal data are subject to appropriate safeguards.[177] Article 25 of the former Directive only required data controllers to assess whether a receiving state has implemented an "adequate level of protection."[178] The GDPR relies in large part upon binding corporate rules approved by supervisory authorities to ensure that safeguards are in place before EU personal data transfers are permitted o third countries.[179] Together, Articles 44–50 of the GDPR constitute a comprehensive framework to govern EU personal data transfers to third countries or international organizations.[180]

1. Safe Harbor 1.0

Under the DPD of 1995, the European Commission concluded that European personal data could not be transferred to America because the United States lacked sufficient privacy standards outside of a few industries.[181] To avert this potential financial disaster, in 2000, the United States Commerce Department and the European Commission agreed to Safe Harbor 1.0.[182] Under Safe Harbor 1.0, U.S. companies receiving consumer data from Europe needed to self-certify that they complied with

175. *Id.* art. 45, at 61.

176. *Id.* arts. 44–50, at 60–65. Chapter V of the General Data Protection Regulation is titled "Transfers of personal data to third countries or international organisations." *Id.* at 60.

177. *Id.* art. 46, at 62.

178. Council Directive 95/46/EC, *supra* note 38, art. 25, at 45–46.

179. GDPR, *supra* note 4, art. 47, at 62.

180. *Id.* arts. 44–50, at 60–65. Chapter 5 Transfers of personal data to third countries or international organizations are governed by GDPR Articles 44 to 50: Article 44 (General principle for transfers); Article 45 (Transfers on the basis of an adequacy decision); Article 46 (Transfers subject to appropriate safeguards); Article 47 (Binding corporate rules); Article 48 (Transfers or disclosures not authorised by Union law); Article 49 (Derogations for specific situations); and Article 50 (International cooperation for the protection of personal data). *Id.*

181. Council Directive 95/46/EC, *supra* note 38, art. 25, at 45–56.

182. *Information for EU Residents Regarding the U.S. – EU Safe Harbor Program*, FED. TRADE COMM'N (Feb., 2015), https://www.ftc.gov/tips-advice/business-center/guidance/information-eu-residents-regarding-us-eu-safe-harbor-program [https://perma.cc/95WF-MCZ9].

the principles of the DPD of 1995.[183] Companies could join a self-regulatory privacy program by pledging to conform to EU privacy policies.[184]

"To participate . . . , a company must self-certify annually to the Department of Commerce that it complies with the seven privacy principles required to meet the EU's adequacy standard: notice, choice, onward transfer, security, data integrity, access, and enforcement."[185] U.S. companies that received consumer data from Europe had to certify that they complied with DPD principles.[186] "The U.S.-EU Safe Harbor

183. *Id.*

184. *Id.*

185. *FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework*, FED. TRADE COMM'N (Apr. 7, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international [https://perma.cc/XJ5E-47PK] [hereinafter *FTC Settles*].

186. *Id.* The Safe Harbor Principles are:

> 1. An organization must provide notice to data subjects about the purposes for their information's collection and use, contact information for any inquiries or complaints, types of third parties to which the organization discloses the data, and the choices and means the organization offers for limiting use and disclosure.
>
> 2. The organization must offer a choice to opt out from a disclosure of personal data to a third party or use of such data for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized. (Opt-in requirements may apply to certain information deemed especially sensitive).
>
> 3. Subject to (1) and (2), while transferring personal data to a third-party agent, an organization must ensure such agent subscribes to the Safe Harbor principles or is subject to the E.U. Directive or another adequacy finding. Alternatively, the organization may enter into a written agreement with such agent requiring the agent to provide at least the same level of privacy protection required by the relevant principles.
>
> 4. Data subjects must have access to their personal information and be able to correct, amend, or delete that information where it is inaccurate (though certain exceptions may apply).
>
> 5. Organizations must take "reasonable precautions" to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.
>
> 6. In accordance with item (1), organizations must use the personal information only for the intended purposes and "should take reasonable steps" to ensure that data are reliable for the intended use, accurate, complete, and current.
>
> 7. Finally, organizations' policies must include: (i) readily available and affordable independent recourse mechanisms to investigate complaints by data subjects, resolve disputes, and award damages, where applicable; (ii) procedures for verifying that the Safe Harbor principles have been implemented at the

Framework provides a method for U.S. companies to transfer personal data outside of Europe that is consistent with the requirements of the European Union Directive on Data Protection . . . ."[187] Safe Harbor 1.0 relied almost completely on self-policing and no empirical evidence demonstrated that U.S. companies actually complied with the Safe Harbor 1.0 principles.[188] In 2013, Google was the target of an investigation by the UK's Information Commissioner's Office and five other data protection authorities (DPAs) because of changes to its privacy policy that did not conform to EU and domestic regulations.[189]

2. The ECJ's Reversal of Safe Harbor 1.0

Europe previously expressed more concern with "the state of data privacy and regulation than their American counterparts for quite some time, but the immediate origins of the new data protection law can be traced to the fury over the extent of US surveillance in the years after 9/11."[190] During the George W. Bush presidency, the U.S. government clandestinely engaged in national security-related surveillance activities in violation of Safe Harbor 1.0.[191] The National Security Agency

---

> organization; and (iii) obligations to remedy problems arising out of a failure to comply with the principles.

Vadim Schick, *Data Privacy Concerns for U.S. Healthcare Enterprises' Overseas Ventures*, 4 J. HEALTH & LIFE SCI. L. 173, 185–86 (2011) (footnotes omitted).

187. Catherine Schmierer, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, 17 RICH. J.L. & TECH. 1, 52–53 (2011) (quoting Complaint, *In re* Progressive Gaitways LLC, No. 092-3141 (F.T.C. Oct. 6, 2009), 2006 WL 3239633, at *1).

188. It is noted that:

> This program relies heavily on the self-policing practices of participating entities and has a limited deterrent effect because the Federal Trade Commission (FTC), charged with Safe Harbor enforcement, has limited jurisdictional reach. The basic punishment for violating the Safe Harbor principles is being de-listed from the Safe Harbor program's participant list. However, the FTC still may bring a claim against a violator of the Safe Harbor provisions under the FTC Act. Furthermore, failure of a repeated violator to notify the Department of Commerce of such violations is actionable under the False Statements Act.

Schick, *supra* note 186, at 186–87 (footnotes omitted); *see also FTC Settles*, *supra* note 185 (noting that there are several companies that did not comply with the Safe Harbor regulations).

189. *Google Facing Regulatory Action in Six EU Countries over Privacy Policy Issues*, OUT-LAW.COM (Apr. 3, 2013), https://www.out-law.com/articles/2013/april/google-facing-regulatory-action-in-six-eu-countries-over-privacy-policy-issues/ [https://perma.cc/4RRN-8RLP].

190. Butterworth, *supra* note 64.

191. *See How It Works: NSA Spying*, ELEC. FRONTIER FOUND., https://www.eff.org/nsa-spying/how-it-works [https://perma.cc/PRG3-LHQQ]; *No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy*, ELEC. FRONTIER FOUND. (Oct. 5, 2015),

(NSA),[192] relying upon the U.S. Patriot Act, collected the records of millions of cell phone users without the knowledge and the consent of the data subjects.[193]

Google, Facebook, Apple, and other Internet moguls were cooperative in the NSA's secretive PRISM program, which monitored cyberspace.[194] The NSA invested billions of dollars to fund projects, such as supercomputers, used to crack encryption and digital scrambling in its classified program, called Bullrun.[195] PRISM, the NSA's program, was an "Internet surveillance program [that] collect[ed] data from online providers including e-mail, chat services, videos, photos, stored data, file transfers, video conferencing and log-ins."[196] The NSA,[197] relying upon the U.S. Patriot Act, routinely collected the phone records of millions of cell phone users.[198]

Based upon these disclosures of widespread surveillance, the Court of Justice of the European Union (CJEU) held that the U.S. did not qualifying as having an adequate level of protection.[199] This CJEU action

---

https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance [https://perma.cc/S4PG-LSWZ].

192. The National Security Agency (NSA) formed in 1952 as a separately organized agency within the Department of Defense. *Critical Skills for National Security and the Homeland Security Federal Workforce Act—S. 1800: Hearing Before the Int'l Sec., Proliferation & Fed. Servs. Subcomm. of the S. Comm. on Governmental Affairs*, 107th Cong. 11 (2002) (testimony of Harvey A. Davis, Associate Director, Human Resources Services, National Security Agency). The NSA has two identified missions: (1) the Signals Intelligence (SIGINT) mission, to "collect[], process[], and disseminate[] intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations" and (2) the Information Assurance mission, to "confront[] the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information." *The Intelligence Community*, UNM: NAT'L SECURITY STUD. PROGRAM, http://nssp.unm.edu/ic-info/index.html [https://perma.cc/3YW3-RP4G].

193. Charlie Savage et al., *U.S. Confirms that It Gathers Online Data Overseas*, N.Y. TIMES (June 6, 2013), https://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html [https://perma.cc/ZQ6D-4YP8].

194. *Id.*

195. Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html [https://perma.cc/2DZE-SKJJ] (stating that an N.S.A. memorandum confirmed that the agency spent billions to "break widely used Internet encryption technologies").

196. Savage et al., *supra* note 193.

197. *See supra* note 192 and accompanying text.

198. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/VHY7-9MH3].

199. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'n, 2015 E.C.R. ¶¶ 83, 88, 97, 107.

prompted the cross-border data transfer Safe Harbor to be renegotiated.[200] In October 2015, CJEU invalidated the Safe Harbor agreement between U.S. Commerce Department and the European Commission in *Schrems v. Data Protection Commissioner* (Case C–362/14).[201] The CJEU concluded U.S. data privacy "provisions were not stringent enough to adequately protect the privacy of EU citizens in line with EU privacy standards."[202]

3. Privacy Shield

On February 29, 2016, the European Commission published the EU-U.S. Privacy Shield (Privacy Shield), an amended framework to enable cross-data flows.[203] Under this "Safe Harbor 2.0," U.S. companies handling Europeans' personal data must commit to strong rules on how personal data is processed while ensuring that individual rights are guaranteed.[204] Many privacy advocates expressed dissatisfaction with this pragmatic agreement. Viviane Reding, the EU's Vice President and Justice Commissioner, contended that the agreement might not actually be safe at all, because U.S. privacy standards continue to be inadequate: "[W]e kicked the tyres and saw that repairs are needed. For the Safe Harbour to be fully roadworthy[,] the U.S. will have to service it. . . . Safe Harbour has to be strengthened or it will be suspended."[205]

Safe Harbor 2.0 grants European citizens protection with redress possibilities because "any company handling human resources data from Europe has to commit to comply with decisions by European DPAs."[206] This Safe Harbor agreement is in danger of collapse because of widespread European dissatisfaction with U.S. privacy policy. European privacy advocates call for the elimination of Safe Harbor 2.0, enabling transatlantic data transfers, because of U.S. spying on electronic

200. *Max Schrems v. Data Protection Commissioner (CJEU – "Safe Harbor")*, EPIC.ORG, https://www.epic.org/privacy/intl/schrems/ [https://perma.cc/BGZ8-DL2D].

201. *Id.*

202. Bryce Baschuk & Michael Scaturro, *U.S., EU Privacy Spat Might Shift to World Trade Organization*, BLOOMBERG L. (Feb. 2, 2016), https://www.bna.com/us-eu-privacy-n57982066852/ [https://perma.cc/5A85-UQLB].

203. MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1 (2016).

204. *Id.*

205. Viviane Reding, Vice-President, Eur. Comm'n, EU Justice Comm'r, Speech/14/62, A Data Protection Compact for Europe 3 (Jan. 28, 2014), http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm [https://perma.cc/HJ7P-SVVH] (emphasis omitted).

206. Press Release, Eur. Comm'n, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm [https://perma.cc/WL6L-4NB7].

communications.[207] "On July 5, the European Parliament passed a non-binding resolution, [requesting] the European Commission . . . to suspend the [EU-U.S.] Privacy Shield framework."[208]

4. Brussels Effect in the United States

On June 28, 2018, Governor Jerry Brown signed The California Consumer Privacy Act of 2018 (CCPA) into law.[209] The CCPA consists of three major components: "It gives consumers the right to ask companies to disclose what data they have collected on them; the right to demand that they not sell the data or share with third parties for business purposes; and the right to sue or fine companies that violate the law."[210] "The legislation, which will go into effect in January 2020," like the EU GDPR, "give[s] individuals more control over their personal data, restrict[s] what organizations can do with data, and give[s] regulators the power to fine non-compliant organizations."[211]

---

207. For example, Max Schrems, the Austrian law student who filed an action before the European Court of Justice (ECJ) invalidating Safe Harbor 1.0, argues that the U.S./EU agreement (Safe Harbor 2.0) should also be invalidated by the ECJ. *See* Jennifer Baker, *Why Safe Harbor 2.0 Will Lose Again*, ARS TECHNICA (Feb. 2, 2016, 1:00 PM), https://arstechnica.com/tech-policy/2016/02/interview-safe-harbour-2-0-will-lose-again-argues-max-schrems/ [https://perma.ca/M9SG-p2Z7] ("Schrems is adamant that those lobbying in favour of so-called Safe Harbour 2.0 are trying to blur the lines 'by saying we have this little change here, this little change there. But none of these are substantial changes of surveillance techniques that the US has. They have not even changed their own national system to a level that would be compliant with European law.'").

208. Chris Cwalina et al., *The European Parliament Asks for the Suspension of the Privacy Shield*, DATA PROTECTION REP. (July 17, 2018), https://www.dataprotectionreport.com/2018/07/european-parliament-asks-for-suspension-privacy-shield/ [https://perma.cc/7XXX-3W8F]; *see also id.* ("The Parliament's resolution cites a number of reasons for asking the Commission to suspend the Privacy Shield pending US compliance, including the recent reauthorization and amendment of Section 702 of the Foreign Intelligence Surveillance Act ('FISA') which allows US intelligence agencies to collection information on non-US persons located outside of the US and the March 2018 Clarifying Overseas Use of Data ('CLOUD') Act, which allows US law enforcement agencies to access personal data stored abroad. The resolution also cites the improper use of 2.7 million EU citizens Facebook data by Cambridge Analytica, and the failure of the US to appoint a sufficiently independent ombudsperson as required by the Privacy Shield . . . .").

209. Assemb. B. 375, 2018 Assemb. (Cal. 2018).

210. Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html [https://perma.cc/9CKP-9HZW].

211. Luke Irwin, *California's 'GDPR-Like' Privacy Law Passes: What You Need to Know*, IT GOVERNANCE USA BLOG (July 16, 2018), https://www.itgovernanceusa.com/blog/californias-gdpr-like-privacy-law-passes-what-you-need-to-know/ [https://perma.cc/8ZC6-WMGQ].

The CCPA requires businesses[212] to post "a 'clear and conspicuous link' on their website's homepage titled 'Do Not Sell My Personal Information.' The link would take users to a page where they can opt out of having their data sold or shared."[213] The CCPA adopts a principle of data minimization, closely resembling the European approach.[214] The CCPA contains both disclosure and data subject access rules similar to the GDPR; however, the California statute does not include many other GDPR rules.[215] For example, like the GDPR, the CCPA enacts remedies such as presumed statutory damages for security breaches,[216] but California has not adopted the GDPR's wealth-based fines.

---

212. *See* CAL. CONSUMER PRIVACY ACT, https://www.caprivacy.org/facts/hold-big-corporations-accountable [https://perma.cc/EV6H-HWFQ] ("A business is 1798.106 (b): a sole-proprietorship, partnership, limited-liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) has annual gross revenues in excess of $50,000,000, as adjusted pursuant to paragraph (5) of subdivision (a) of section 1798.115; or (B) annually sells, alone or in combination, the personal information of 100,000 or more consumers or devices; or (C) derives 50 percent or more of its annual revenues from selling consumers' personal information.").

213. Laura Sydell, *Do Not Sell My Personal Information: California Eyes Data Privacy Measure*, NPR: ALL TECH CONSIDERED (May 28, 2018, 9:26 AM), https://www.npr.org/sections/alltechconsidered/2018/05/28/614419275/do-not-sell-my-personal-information-california-eyes-data-privacy-measure [https://perma.cc/HG7N-CH8P].

214. *See* CAL. CONSUMER PRIVACY ACT, *supra* note 212 ("1798.101. Right to Know Whether Personal Information is Sold or Disclosed and to Whom. 1798.101. (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer: (1) the categories of personal information that the business sold about the consumer and the identity of the third parties to whom such personal information was sold, by category or categories of personal information for each third party to whom such personal information was sold; and (2) the categories of personal information that the business disclosed about the consumer for a business purpose and the identity of the persons to whom such personal information was disclosed for a business purpose, by category or categories of personal information for each person to whom such personal information was disclosed for a business purpose.").

215. *See* Philip N. Yannella, *Using the GDPR to Comply with the California Consumer Privacy Act*, BALLARD SPAHR LLP: CYBERADVISER (July 19, 2018), https://www.cyberadviserblog.com/2018/07/using-the-gdpr-to-comply-with-california-consumer-privacy-act/ [http://perma.cc/5MHR-HWLH] ("Substantively the GDPR contains many provisions that are absent from the CCPA, including: requirements for lawful processing; data and storage limitations; provisions for the appointment of data protection officers, local representatives, and performing a data protection impact analysis; specific requirements for data processors (service providers under the CCPA), business process mapping and documentation generally, and a draconian civil penalty structure. That being said, there is some overlap between the two privacy laws, particularly regarding disclosure requirements and subject access rights.").

216. David Caplan, *Momentum Building for California's Consumer Right to Privacy Act Ballot Initiative*, ALSTON & BIRD: PRIVACY & DATA SECURITY BLOG (June 4, 2018),

The CCPA's enactment is likely to create a "California Effect," a term used in political science to refer to the tendency of the other states to follow California's lead in areas such as consumer rights and environmental standards.[217] The state's enormous size and robust economy gives California significant advantage in encouraging large companies to adopt its regulations nationwide.[218] U.S. companies are likely to revise their privacy policies for all states to avoid having one standard for California that conflicts with privacy policies in other states.

C. *Against the Brussels Effect: Areas of Divergence*

1. The Right to Be Forgotten & U.S. Privacy Law

Article 17 of the GDPR gives data subjects in the twenty-eight countries of the European Union a statutory "right to be forgotten" (RTBF).[219] Commentators often point to the RTBF as the most significant difference between U.S. and EU data protection law.[220] The European Union's RTBF takes three forms: (1) the right to have information deleted after a preset period, (2) the right to have a clean slate, and (3) the right to be connected to current information and delinked from outdated information.[221] Article 17 of the GDPR further specifies the right of erasure provided for in Article 12(b) of the DPD of 1995.[222] It provides the conditions of the right to be forgotten, including the obligation of the controller that made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data.[223]

In 2014, the CJEU ruled that Google was a data processor subject to the EU's DPD of 1995 in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos* (*Google Spain v. AEPD*) (Case C-

---

https://www.alstonprivacy.com/momentum-building-for-californias-consumer-right-to-privacy-act-ballot-initiative/ [https://perma.cc/7KQW-7XJC].

217. *See* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 259 (1995).

218. *See* DYNAMICS OF REGULATORY CHANGE: HOW GLOBALIZATION AFFECTS NATIONAL REGULATORY POLICIES 9 (David Vogel & Robert A. Kagan eds., 2004).

219. GDPR, *supra* note 4, art. 17, at 43.

220. Charles Arthur, *Explaining the 'Right to be Forgotten' - The Newest Cultural Shibbileth*, GUARDIAN (May 14, 2014, 1:42 PM), https://www.theguardian.com/technology/2014/may/14/ explainer-right-to-be-forgotten-the-newest-cultural-shibboleth [https://perma.cc/53PM-Q96D].

221. *See* Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice*, 8 SCRIPTED 229, 236 (2011).

222. GDPR, *supra* note 4, art. 17, at 43.

223. *Id.*

131/12).[224] The CJEU ruling required Google and other search engines to delink information at the data subject's request if the search results "appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."[225] The court rejected Google's argument that removal requests were the province of the website publisher, not the search engine.[226]

Europe's highest court determined that Google, as the preeminent search engine, was far more likely to interfere with a consumer's right to privacy than was the original publisher.[227] Requiring Google and other search engines to implement the RTBF is not about deleting or forgetting content; rather, it is about making it more difficult to find personal information.[228] Links that Google removes from EU search results will remain in searches made from non-EU domains, although Europeans are now attempting to pressure other countries to comply with delinking requests as well.[229] Early takedown requests include "a British politician who's trying to make a comeback, someone convicted of possessing child abuse images and a doctor who doesn't want negative reviews from patients to be searchable."[230]

Article 17 establishes a methodology for determining when a data subject can exercise the right of erasure, data controllers' obligation to erase links to third-party websites, and how to exercise that right.[231] A data subject has the right to erase links to data relating to him or her if the information is:

---

224. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, 2014 E.C.R. ¶ 83.

225. *Id.* at ¶ 93.

226. *Id.* at ¶ 63, 88.

227. *Id.* at ¶ 99.

228. *Id.* at ¶ 88.

229. The GDPR will have the right to expunge or erase personal data that is subject to the right of expression:

> The proposed provisions on the "right to be forgotten" are very clear: freedom of expression, as well as historical and scientific research are safeguarded. For example, no politician will be able to have their earlier remarks deleted from the web. This will thus allow, inter alia, news websites to continue operating on the basis of the same principles.

Questions and Answers – General Data Protection Regulation, EUR. COMM'N (Jan. 24, 2018), http://europa.eu/rapid/press-release_MEMO-18-387_en.htm [https://perma.cc/3R2A-ETZV] (emphasis omitted).

230. *See* David Mitchell, *The Right to Be Forgotten Will Turn the Internet into a Work of Fiction*, GUARDIAN (July 5, 2014, 7:05 PM), http://www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google [https://perma.cc/LQJ4-98DZ].

231. GDPR, *supra* note 4, art. 17, at 43.

> no longer necessary in relation to the purposes for which [it was] collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation.[232]

The strongest case for a right of erasure applies to (1) personal data collected while a data subject was a child and (2) information that is no longer considered relevant. Here, the child is not likely to be cognizant "of the risks involved by the processing, and later wants to remove such personal data, especially on the Internet."[233] Article 17(3) makes it clear the RTBF is not an absolute right because the following exceptions apply:

> (a) for exercising the right of freedom of expression and information;
>
> (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
>
> (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
>
> (e) for the establishment, exercise or defence of legal claims.[234]

Commentators contend that the RTBF has never been explicitly recognized in the United States because the RTBF conflicts with the First Amendment's right of expression.[235] However, there is a clear parallel

232. *Id.* at 12.

233. *Id.* at 13.

234. *Id.* art. 17, at 43–44.

235. *See, e.g.*, Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012) (describing the right to be forgotten "as the biggest threat to free speech on the Internet in the coming decade"); *see also* Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten are Incompatible With Free Speech*, 18 COMM. L. & POL'Y 91, 93 (2013) ("[T]he European Union's proposed right to be forgotten -- and

between the RTBF and the U.S. tort action for "public disclosure of private facts."[236] The Restatement (Second) of Torts recognized this tort, which has a clear parallel to the RTBF.[237]

Section 230 of the Communication Decency Act (CDA Section 230) states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[238] CDA Section 230 has given rise to commercial websites such as the mugshot and revenge pornography industries that hide behind the First Amendment.[239]

Websites have the discretion to take down or restrict access to third party content that the provider regards as "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[240] Nevertheless, they have no takedown duty and they are shielded from liability for all third-party content. The chief benefit of CDA Section 230 is that it shields providers from liability for third party content. [241]

In one of the first U.S. RTBF cases, the plaintiff contended that Google, Yahoo!, Bing and other defendants operating internet search engines "harmed his reputation by indexing websites that describe him in negative terms, and that Defendants have profited therefrom."[242] The court granted the search engine companies' motion to dismiss on CDA Section 230 grounds.[243]

---

the obscurity model, generally -- is impermissibly antithetical to the American right of free speech and established First Amendment theories.").

236. *See* W. Gregory Voss & Celine Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the 'Right to Be Forgotten': A Study on the Convergence of Norms*, 14 COLO. TECH. L.J. 281, 285 (2016) (citing Franz Werro, *The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash*, *in* HAFTUNGSRECHT IM DRITTEN MILLENNIUM [LIABILITY IN THE THIRD MILLENNIUM] 285, 292 (Aurelia Colombi Ciacchi et al. eds., 2009)).

237. *Id.*

238. 47 U.S.C. § 230(c)(1) (2012).

239. AMY GAJDA, THE FIRST AMENDMENT BUBBLE: HOW PRIVACY AND PAPARAZZI THREATEN A FREE PRESS 128–32, 206–21 (2015).

240. 47 U.S.C. § 230(c)(2)(A) (2018).

241. *See* Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 397 (2015).

242. Manchanda v. Google, 16-CV-3350, 2016 WL 6806250, at *1 (S.D.N.Y. Nov. 16, 2016).

243. *Id.* at *2–3 (reasoning that the CDA gives the search engines broad immunity from these claims and that service providers are not liable for third party postings) ("This immunity attaches regardless of the specific claim asserted against the search engine, so long as the claim arises from the publication or distribution of content produced by a third party and the alleged injury involves damage to a plaintiff's reputation based on that content.").

The EU's right of erasure, in sharp contrast, applies to "every photo, status update, and tweet,"[244] a policy which "[c]ould precipitate a dramatic clash between European and American conception of the proper balance between privacy and free speech."[245] The proper line between protecting individual privacy and the public's right to know is extremely difficult to draw. An overly broad right to be forgotten may lead to censorship of the Internet or the improper suppression of historical truths.[246]

2. The Right to Rectification

Article 15 of the GDPR gives all data subjects a right of access to their personal data.[247] Controllers must inform data subjects of the length of the data storage period. Additionally, controllers must inform data subjects of their rights to rectify, to erase, and of their rights to lodge a complaint.[248] Rectification is a data subject's right to correct inaccurate information.[249] In the United States, sectoral statutes often give data subjects the right to correct information in their records.[250]

---

244. Rosen, *supra* note 235.

245. *Id.*

246. Rustad & Kulevska, *supra* note 241, at 372–73.

247. GDPR, *supra* note 4, art. 15, at 43.

248. *Id.*

249. The data subject's right to rectification under the GDPR is imported from Article 12(b) of the EU's DPD of 1995. Article 16 states: "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her." *Id.* art. 16, at 43.

250. The Family Educational Rights and Privacy Act (FERPA) grants the following rights:

> Parents or eligible students have the right to inspect and review the student's education records maintained by the school. . . .
>
> Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

Family Educational Rights and Privacy Act (FERPA), U.S. DEP'T EDUC., https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html [https://perma.cc/ZZL4-2WJY] (last updated Mar. 1, 2018); *see also Your Medical Records*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html [https://perma.cc/V245-MFHQ] (last updated June 16, 2017) ("If you think the information in your medical or billing record is incorrect, you can request a change, or amendment, to your record. The health care provider or health plan must respond to your request. If it created the information, it must amend inaccurate or incomplete information. If the provider or plan does not agree to your request, you

3. EU Consumers Have Rights Just Beginning to Evolve in the United States

The GDPR introduces the data subject's right to data portability—the right to transfer information from one electronic processing system to another—free from opposition by the controller.[251] A few U.S. federal statutes recognize the right of data portability.[252] The GDPR also provides the right to obtain one's data, in a commonly used electronic format, from the controller on request.[253] Additionally, EU data subjects have a right to object to the use of their data for direct marketing.[254]

EU data subjects have a specific right to be informed, free of charge, before their personal data are first disclosed to third parties or are used for direct marketing. Data subjects may also object to such use.[255] Article 21(1) gives data subjects a right to object unless the "controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject."[256]

EU citizens have a right to object to profiling.[257] The GDPR defines profiling as:

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's

---

have the right to submit a statement of disagreement that the provider or plan must add to your record.").

251. The GDPR states:

> The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
>
> (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
>
> (b) the processing is carried out by automated means.

GDPR, *supra* note 4, art. 20, at 45. A few U.S. federal statutes recognize the right of data portability. *See, e.g.*, 47 U.S.C. § 251(b)(2) (2012) (providing for number portability and stating "[t]he duty to provide, to the extent technically feasible, number portability in accordance with requirements prescribed by the Commission").

252. *See, e.g.*, 47 U.S.C. § 251(b)(2).

253. GDPR, *supra* note 4, art. 15, at 43.

254. *Id.* art. 21, at 45.

255. *Id.* at 12.

256. *Id.* art. 21(1), at 45.

257. *Id.* art. 21, at 45.

> performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements . . . .[258]

The GDPR posits exceptions in certain cases, such as contract performance, express authorization by EU or Member State law, or with a data subject's consent.[259] In contrast, the United States has not yet adopted a comprehensive data privacy rule addressing portability or profiling.[260] However, some states have adopted limited rights such as California's "eraser button" law allowing juveniles to delete their regretted postings.[261]

The GDPR adopts the "principle of accountability" and describes, in detail, the controller's obligation to demonstrate compliance by adopting of internal policies and mechanisms for ensuring such compliance.[262] The United States has yet to enact a comprehensive statute governing data transfer, portability, or profiling.[263]

III. THE "D.C. EFFECT" ON EUROPEAN DATA PROTECTION

The United States is often portrayed as a country with a weak or nonexistent privacy regime. The following section provides many illustrations of how EU Data Privacy Law imported privacy rights and remedies first recognized in the United States. European privacy law has lofty aspirations, but no meaningful methods of enforcement. The GDPR imported the U.S style model of public regulation supplemented by strong private enforcement. The GDPR also adopted data subject consent as a fundamental right, which was a concept first recognized in the U.S. The next section explains how the EU adopted damages lawsuits by the data subjects and representative actions, similar to class actions that originated in the United States.

A. *How the United States Shapes EU Data Privacy Law*

The notion that the GDPR is unilaterally driving U.S. privacy law is an overly deterministic interpretation of the Brussels Effect. U.S. privacy law already aligns well with GDPR privacy doctrines. Key principles found in the European Union's omnibus privacy law were present in U.S. privacy law decades prior to the GDPR's effective date. It is more

258. *Id.* art. 4, at 33.

259. *Id.* art. 6, at 36–37.

260. *See* Naula O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL., https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/M8ZF-E56J].

261. *See* S. 568, 2013 Leg., Reg. Sess. (Cal. 2013).

262. GDPR, *supra* note 4, at 15.

263. *See* O'Connor, *supra* note 260.

accurate to say that the United States and the European Union share fundamental principles while allocating enforcement to different legal institutions. The rights afforded to data subjects under U.S. sectoral statutes parallel the rights afforded to data subjects under the GDPR.

This part of the Article provides evidence of a "D.C. Effect" on the GDPR, as illustrated by the EU Commission's extensive borrowing of concepts from U.S. law. The evolving global standard is actually a hybrid, combining some of the most effective enforcement features of U.S. tort law (D.C. Effect) with the more stringent privacy principles of EU law (Brussels Effect). The Trump Administration is developing its own "consumer data privacy policies, and the Commerce Department is meeting with big companies like Facebook Inc., Comcast Corp. and Alphabet Inc. as it looks to eventually seeing the policies enshrined in legislation."[264]

1. Consent as a Common Cornerstone

The GDPR requires data controllers to document verifiable consent.[265] Data processors must present written requests for data subject consent "in a manner which is clearly distinguishable from the other matters."[266] Article 7 of the GDPR requires data processors to obtain data-subject consent prior to the processing of personal data.[267] Article 7(3) allows data subjects to withdraw their consent at any time.[268] The DPD also permitted the processing of personal data only when "the data subject has unambiguously given his consent."[269] Similarly, the ePrivacy Regulation incorporates the GDPR principles of consent while including Privacy by Design requirements for facilitating consent:

> 1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.
>
> 2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate

264. David Shepardson, *Trump Administration Working on Consumer Data Privacy Policy*, REUTERS (July 27, 2018, 5:36 PM), https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK [https://perma.cc/44W6-YTP8].

265. GDPR, *supra* note 4, art. 7, at 37.

266. *Id.*

267. *Id.*

268. *Id.*

269. Council Directive 95/46/EC, *supra* note 38, art. 7, at 40.

> technical settings of a software application enabling access to the internet.
>
> 3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.[270]

The principle of consent is also a cornerstone of U.S. privacy law.[271] For example, the Fair Credit Reporting Act (FCRA) is a federal statute that compels credit-reporting agencies to ensure that the information they gather and distribute is a fair and accurate summary of a consumer's credit history.[272] The FCRA arms consumers with strong consent provisions if credit reports are used for employment purposes.[273] A credit-reporting agency may share credit reports when it has "reason to believe" that there is "a legitimate business need for the information."[274]

Similarly, HIPAA's Privacy Rule, also referred to as Standards for Privacy of Individually Identifiable Health Information, established national standards for the protection of certain health information.[275] HIPAA's Privacy Rule requires a covered entity to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations.[276] The HIPPA Rule states that protected patient data cannot be disclosed without "authorization."[277]

2. Data Minimization

The GDPR restricts personal data processing to data "collected for specified, explicit and legitimate purposes and not further processed in a

---

270. *Eur. Comm'n Proposal*, *supra* note 75, art. 9.

271. *See generally* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 152–56 (2017) (discussing consent in the context of U.S. privacy law).

272. 15 U.S.C. § 1681(b) (2012).

273. *Id.* § 1681b(b)(2)(B).

274. *Id.* § 1681b(a)(3)(F).

275. "The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically." *The HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/JL5M-DJHG].

276. 45 C.F.R. § 164.508(a)(2)(i) (2018); *see also The HIPPA Privacy Rule*, *supra* note 275 (stating that the HHS's HIPAA Privacy Rule is found "at 45 CFR Part 160 and Subparts A and E of Part 164").

277. 45 C.F.R. § 164.508(a)(1).

manner that is incompatible with those purposes."[278] Under the GDPR, "businesses will be able to collect and process data only for a well-defined purpose. They will have to inform the user about new purposes for processing."[279]

More than four decades before the GDPR was proposed, the United States recognized use limitations on personal data. In 1973, the U.S. Department of Health, Education and Welfare released its report (HEW Report) calling for safeguards against data being collected and processed for one purpose and "used or made available for other purposes."[280] The HEW Report proposed the following safeguards to protect consumer privacy:

> • There must be no personal-data record-keeping systems whose very existence is secret.
>
> • There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> • There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.[281]

The American Law Institute's proposed Principles of the Law of Data Privacy propose a "use limitation" that provides, "Personal data shall not be used in data activities unrelated to those stated in the notice to

278. GDPR, *supra* note 4, art. 5, at 35; *see also id.* art. 6, at 36 ("Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) 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, in particular where the data subject is a child.").

279. *A New Era for Data Protection in the EU—What Changes After May 2018*, EUR. COMM'N, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf [https://perma.cc/TD6X-9EJY] (emphasis omitted).

280. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, & THE RIGHTS OF CITIZENS 41 (1973).

281. *Id.*

individuals pursuant to Principle 4 without the consent of the individuals."[282]

The ALI Reporters cite numerous U.S. statutes that reflect the GDPR norm of data minimization including the federal Privacy Act, Fair Credit Reporting Act, Driver's Privacy Protection Act, Cable Communications Policy Act, Gramm-Leach-Bliley Act and the Video Privacy Protection Act.[283] Similarly, the FTC report on privacy issues in the Internet of Things adopts data minimization as a salient principle:

> Commission staff also recommend that companies consider data minimization – that is, limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely. The report notes that data minimization addresses two key privacy risks: first, the risk that a company with a large store of consumer data will become a more enticing target for data thieves or hackers, and second, that consumer data will be used in ways contrary to consumers' expectations.[284]

The Gramm-Leach-Bliley Act (GLBA) has already incorporated a data minimization principle restricting information from being used for other purposes.[285] HIPAA applies to health care providers and medical

---

282. PRINCIPLES OF THE LAW: DATA PRIVACY § 7(1) (AM. LAW INST., Preliminary Draft No. 3, 2018).

283. *Id.* § 7 reporters' note 2.

284. *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FED. TRADE COMM'N (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices [https://perma.cc/P9DU-KTWB]. "The report takes a flexible approach to data minimization. Under the recommendations, companies can choose to collect no data, data limited to the categories required to provide the service offered by the device, less sensitive data; or choose to de-identify the data collected." *Id.*

285. 15 U.S.C. § 6802 (2012). The GLBA § 6802(c) is titled: "Limits on reuse of information" and places limitations on whether financial information may be transferred to third parties:

> Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

Id.

information. The HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164) has also adopted data minimization principles.[286]

The OECD's Collection Limitation and Use Limitation Principles first recognized data minimization as a basic right: "[T]he 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."[287] The OECD's Use Limitation Principle requires the processor to disclose what personal data is gathered and to make it available to the data subject.[288] The OECD's Purpose Specification Principle states that:

> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.[289]

Data minimization "is actually in stark contrast with things data-driven CEOs like Jeff Bezos at Amazon believed when he said 'We never throw away data.'"[290] Observers deride the United States' expansive approach to information privacy as "data maximization" versus Europe's strict data minimization policy. The widespread sharing of personal information with third parties, without the knowledge of data subjects, has led to calls for better control of personally identifiable data in the United States.[291] Nevertheless, data minimization originated in U.S. law

---

286. *See How May the HIPAA Privacy Rule's Minimum Necessary Standard Apply to Electronic Health Information Exchange Through a Networked Environment?*, U.S. DEP'T HEALTH & HUM. SERVS. (Dec. 15, 2008), https://www.hhs.gov/hipaa/for-professionals/faq/545/how-may-hipaas-minimum-necessary-standard-apply-to-electronic-information/index.html [https://perma.cc/XHQ2-6UYF] ("[HIPAA's] Privacy Rule generally requires covered entities to take reasonable steps to limit uses, disclosures, or requests (if the request is to another covered entity) of protected health information (PHI) to the minimum necessary to accomplish the intended purpose.").

287. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/Z5FX-J5UU] (last updated 2013).

288. *Id.*

289. *Id.*

290. Bernard Marr, *Why Data Minimization Is an Important Concept in the Age of Big Data*, FORBES (Mar. 16, 2016, 3:24 AM), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#55ee7fd71da4 [https://perma.cc/2B4B-9ZD8].

291. Kirsten Korosec wrote about the personal data that Facebook collects and stated:

> But the important step to remember is to stop and really read through what you're agreeing to—even if sometimes it's contained in a lengthy legalese agreement—before casually hitting the "continue" to log in using Facebook button. Typically,

decades before it was recognized in Europe.[292] The United States may have pioneered the concept of data minimization, but the United States severely under enforces the principle.

Seven out of ten smart phone applications share personally identifiable data with "third-party tracking companies like Google Analytics, the Facebook Graph API or Crashlytics."[293] Data minimization will grow in importance as "organizations are faced with more and more ways to collect more and more kinds of data, including and especially private, personally identifiable data."[294] The ALI's Proposed Principles of the Law of Data Privacy adopt a "use limitation" provision like the GDPR's Article 6, Section 7 "Use Limitation" provides:

> Personal data shall not be used in data activities unrelated to those stated in the notice to individuals pursuant to the Notice Principle (Principle 4) or otherwise disclosed to individuals, Personal data shall not be subject to an unrelated secondary use to which the individual has not consented unless there is a compelling reason to do so specifically authorized or required by law.[295]

3. Privacy by Design

The EU Data Protection Supervisor stated that "[d]ata protection by design aims to build data protection and privacy into the design of processing operations and information systems, in order to comply with

---

> these apps want access to names, genders, and locations. But many apps dig deeper into personal preferences and friend networks. From here, all it takes is for the third-party app to sell the data to someone else, like behavior research firm Strategic Communication Laboratories, which is affiliated with Cambridge Analytica, the data firm that worked for Trump's campaign. Facebook has cut down on the information it shares with third party apps. However, it has not been eliminated altogether.

Kirsten Korosec, *This Is the Personal Data that Facebook Collects—and Sometimes Sells*, FORTUNE (Mar. 21, 2018), http://fortune.com/2018/03/21/facebook-personal-data-cambridge-analytica/ [https://perma.cc/8XAX-FEFP].

292. *See supra* notes 271–77 and accompanying text.

293. Narseo Vallina-Rodriguez & Srikanth Sundaresan, *Internet Privacy: 7 out of 10 Smartphone Apps are Sharing Your Data, New Study Reveals*, NEWSWEEK (June 1, 2017, 7:22 AM), http://www.newsweek.com/online-privacy-data-driven-companies-facebook-and-google-have-access-7-out-10-618782 [https://perma.cc/5WDS-7TYE].

294. Marr, *supra* note 290.

295. PRINCIPLES OF THE LAW: DATA PRIVACY § 7 (AM. LAW INST., Preliminary Draft No. 3, 2018) (use restrictions).

data protection principles."[296] The GDPR requires companies "to take into account the protection of the rights of individuals, both before and during their processing activities, by implementing the appropriate technical and organization measures to ensure that they fulfil their data protection obligations."[297] In 2010, eight years before the GDPR adopted this preventive data protection strategy, the FTC rolled out its "Privacy by Design" rules.[298] "Privacy by Design" was first advanced by the Information & Privacy Commissioner of Ontario, Canada.[299]

The FTC contends that Privacy by Design is critical to U.S. data protection and consumer privacy comparable to the GDPR.[300] "The FTC has adopted [Privacy by Design] in the context of enforcement, as has the European Commission."[301] The FTC's Privacy by Design strategy paved the way for the adoption of numerous GDPR principles, including: consent, data minimization, reasonable security, and substantive privacy.[302]

The FTC's underlying jurisprudence is to encourage an entity's software engineers and website designers to implement Privacy by Design rather than to place this responsibility in the hands of data protection officers.[303] For example, "Apple's Safari browser blocks third-party tracking cookies by default. This feature is automatically turned on, making it easier for consumers to prevent unwanted tracking of their activity across websites."[304] Additionally, "Google, Twitter, and Mozilla, now offer SSL encryption by default in some of their online products and services."[305]

---

296. *Privacy by Design*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/our-work/subjects/privacy-design_en/ [https://perma.cc/F2RT-GFJK].

297. *Id.*

298. *See* Edith Ramirez, Comm'r, *Fed. Trade Comm'n, Remarks at the Privacy by Design Conference: Privacy by Design and the New Privacy Framework of the U.S. Federal Trade Commission* 2 (June 13, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf [https://perma.cc/S743-DYHE].

299. ANN CAVOUKIAN, INFO. & PRIVACY COMM'R OF ONT., PRIVACY BY DESIGN 1 (2009), http://www.ontla.on.ca/library/repository/mon/23002/289982.pdf [https://perma.cc/7PHE-T6Q5].

300. *See* Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1335 (2013).

301. Jeff Scarpitti, *Privacy by Design*, INSIDE COUNSEL, June 2015, at 44.

302. *See* Ramirez, *supra* note 298.

303. *See id.* at 2 ("But privacy by design cannot be reduced to hiring a chief privacy officer, mandating employees to watch a privacy training video or fill out a checklist, or inserting a privacy policy into an app. . . . It must be something that an engineer or website developer instinctively thinks about when writing code or developing a new product.").

304. *Id.* at 3.

305. *Id.* at 3.

Article 25 of the GDPR imports the data protection principle of Privacy by Design from the United States.[306] Under the GDPR, data controllers "shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."[307]

B. *"U.S.- Style" Remedies Imported into the GDPR*

Many of the fundamental principles of the GDPR originated in U.S. law. "In 1973, the U.S. Department of Health, Education, and Welfare . . . laid out five principles for data protection, known as the 'Fair Information Practices' ('FIPs')."[308] These core principles prefigured EU data protection law and are emblematic of the way data protection law are congruent.

> 1. There must be no personal data record-keeping systems whose very existence is secret.
>
> 2. There must be a way for a person to find out what information about the person is in a record and how it is used.
>
> 3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
>
> 4. There must be a way for a person to correct or amend a record of identifiable information about the person.
>
> 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[309]

---

306. GDPR, *supra* note 4, art. 25(1), at 48 ("Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.").

307. *Id.* art. 25(2).

308. Griffin Drake, Note, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 167 (2017).

309. *The Code of Fair Information Practices*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/consumer/code_fair_info.html [https://perma.cc/W5SA-V2Q2].

The FIPs identified by HEW were later incorporated into the OECD Principles that Europe relied upon in developing its data protection law:[310]

> The EU legal framework for data protection developed based on the Council of Europe's Convention 108 that was elaborated in parallel with the OECD Guidelines. The Convention is a benchmark for 41 states in Europe and offers protection to nearly 800 million people. The OECD Guidelines are mostly relevant as a global framework for interactions with partners around the world.[311]

1. The GDPR Imports "U.S.-Style" Enforcement

In the European Union, Privacy by Design is proactive but has rarely been reflected in compliance actions.[312] The GDPR's strengthened enforcement mechanisms further align U.S. and EU Privacy by Design law. EU privacy reform empowers data subjects to file private lawsuits seeking damages against controllers and processors who violate their privacy rights.[313] Prior to the GDPR, the European Union had no equivalent to the FTC's hybrid public/private enforcement efforts. The GDPR strengthens enforcement by importing U.S. tort law concepts,

---

310. Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY F., https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ [https://perma.cc/UYF9-CVSL] (last updated Dec. 19, 2007) ("In 1980, the Organization for Economic Cooperation and Development (OECD) used these core HEW fair information principles and built upon them to create a set of eight Fair Information Practices codified in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The OECD has historically created internationally-agreed upon codes, practices, decisions, recommendations, and policy instruments. . . . These OECD guidelines form the basis of many modern international privacy agreements and national laws, and these eight principles from 1980 are referred to by the U.S. Government Accountability Office as key principles for privacy protection." (endnotes omitted)).

311. Peter Hustinx, Eur. Data Prot. Supervisor, Speech at the Joint ICCP-WPISP Roundtable: 30 Years After: The Impact of the OECD Privacy Guidelines 1 (Mar. 10, 2010), http://www.oecd.org/internet/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm [https://perma.cc/DL27-ZGJV] (click on "Speech" hyperlink next to "Peter Hustinx, European Data Protection Supervisor" under "Session 3" heading).

312. A 2011 FTC settlement with Google over its deceptive privacy policies also incorporated Privacy by Design with similar fines as in the Facebook Settlement. *See* Ramirez, *supra* note 298, at 8 (discussing Complaint, *In re* Google, Inc., No. 102 3136 (F.T.C. Oct. 24, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf [https://perma.cc/FT39-6Q9D] and Agreement Containing Consent Order, *In re* Google, Inc., No. 102 3136 (F.T.C. Mar. 30, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf [https://perma.cc/S5Z8-L5VV]).

313. *See* GDPR, *supra* note 4, art. 82, at 81.

including the right to pursue individual damages lawsuits, class actions, and wealth-based fines modeled on U.S. punitive damages law.

Private enforcement of privacy laws was a concept that originated in the U.S.[314] The principal difference between the U.S. and EU concepts of Privacy by Design is the FTC's role in enforcement as seen in a 2011 action against Rite Aid, a company with 4,900 retail pharmacy stores in the U.S.[315] From late 2006 through 2008, Rite Aid "discarded materials containing personal information in clear readable text (such as pharmacy labels and employment applications) in unsecured, publicly-accessible trash dumpsters used by Rite Aid pharmacies on numerous occasions."[316]

Under the GDPR, European data subjects have, for the first time, gained the right to make complaints and seek the equivalent of punitive damages.[317] For more than two hundred years, the wealth of a defendant has been considered a relevant basis for setting the amount of punitive damages in the United States. Wealth-sensitive fines can teach even multi-billion-dollar information-age companies, like Facebook, Instagram, or Google, that violating EU data protection law does not pay.[318]

Article 78 of the GDPR recognizes the right of data subjects to pursue a judicial remedy against a supervisory authority,[319] and Article 79 of the GDPR recognizes the right to a judicial remedy against a controller or processor.[320] The benefit of U.S. privacy law lies in its robust record of enforcement, whereas, prior to the GDPR, Europe had strict data privacy rules with almost no enforcement.[321]

The EU DPD of 1995[322] allowed individual data subjects to seek monetary damages.[323] However, there was no role for data controllers' enforcement as is found in the GDPR.[324] One of the most innovative

314. *See* Alan Charles Raul et al., *United States*, *in* THE PRIVACY, DATA PROTECTION, AND CYBERSECURITY LAW REVIEW 268, 268 (Alan Charles Raul ed., 2014).

315. *See* Complaint at 1, *In re* Rite Aid Corp., No. 072-3121, (F.T.C. Nov. 22, 2010), https://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaidcmpt.pdf [https://perma.cc/2YA7-4EJ3].

316. *Id.* at 3

317. *See* GDPR, *supra* note 4, art. 82, at 81.

318. *See id.* (permitting data subjects whose privacy was infringed to file suit against data controllers and processors seeking monetary damages).

319. *Id.* art. 78, at 80.

320. *Id.* art. 79.

321. *See Cases Tagged with Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/terms/249 [https://perma.cc/EB67-2V3S] (enumerating FTC enforcement actions between 2000 and 2018).

322. Council Directive 95/46/EC, *supra* note 38.

323. *Id.* art. 23, at 45.

324. Article 24 of the GDPR states:

aspects of the GDPR's emphasis on enforcement is the creation of supervisory authorities in each country, which are tasked with investigation and enforcement.[325] "Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union."[326] The FTC's role overseeing privacy is the closest analogue to national supervisory authorities under U.S. law.

2. Data Security Breach Notification

The GDPR's data breach notification framework was largely imported from the United States.[327] The United States recognized this right more than a decade ahead of the European Union. "The data-breach notification provisions of the GDPR were inspired by federal and state data-breach notification laws."[328] "All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security

---

> 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
>
> 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
>
> 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

GDPR, *supra* note 4, art. 24, at 47.

325. Article 51 of the GDPR states:

> Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Id. art. 51(1), at 65.

326. *Id.* art. 51(2).

327. Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 795 n.317 (2016).

328. *Id.*

breaches of information involving identifiable information."[329] These data security laws:

> typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc[.]); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).[330]

The GDPR obliges the controller and the processor to implement appropriate measures for the security of processing in ways that may be at variance with U.S. law.[331] For example, under EU law, controllers have the duty to notify the supervisory authority within seventy-two hours of a security breach.[332] The U.S. data breach notification laws, in contrast, generally employ the standard of reasonableness rather than a specific time period. A rigid rule may be inappropriate because it does not allow the law to accommodate to technological developments that may impact an entity's ability to recognize that the data breach has occurred.

The U.S. data breach notification statute governing customer's financial information (GLBA) provides more comprehensive protection than the GDPR's provisions. Under the GLBA, financial institutions must conduct an audit and identify foreseeable risks to the security of customer

---

329. *Security Breach Notification Laws*, NCSL, (Sept. 29, 2018) http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/2347-2XPM].

330. *Id.*

331. *See* GDPR, *supra* note 4, art. 30, at 50–51.

332. Article 33 of the GDPR states:

> 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
>
> 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Id. art. 33(1)–(2), at 52.

data.[333] HIPPA's Security Rule requires physical safeguards for facility access controls, facility security plans, and other safeguards for workstations and record-keeping.[334]

3. The United States Pioneered Laws Protecting Children's Privacy

The GDPR promulgates specialized rules governing the lawfulness of processing children's personal data relating to information society services offered directly to them.[335] The Clinton Administration first expressed "concern[] about the use of information gathered from children, who may lack the cognitive ability to recognize and appreciate privacy concerns."[336] In 1998, Congress enacted The Children's Online Privacy Protection Act (COPPA),[337] making it illegal for companies to harvest personally identifiable information from children without the consent of a parent. The COPPA Rule:

> applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13.[338]

The amended COPPA Rule, which took effect on July 1, 2013, also protects the privacy of children by making it illegal for companies to harvest personally identifiable information without their parents' consent.[339] COPPA applies only to websites or online services that target children 13 or younger.[340]

---

333. *See* 16 C.F.R. § 314.4(b)(2) (2018) ("Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations . . . .").

334. 45 C.F.R. § 164.310 (2018) (physical safeguards).

335. GDPR, *supra* note 4, art. 8, at 37.

336. *The Task Force's Report*, WALL ST. J. (July 1, 1997), https://www.wsj.com/articles/SB867789071879645500?ns=prod/accounts-wsj [https://perma.cc/A9W8-AXCJ] (reproducing the Clinton Administration's report).

337. 15 U.S.C. § 1605 (2012).

338. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions [https://perma.cc/NQ94-JWKZ].

339. 16 C.F.R. 312.3(b) (2018).

340. "[T]he Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, *et seq.*,) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet." *Id.* § 312.1.

4. Collective Redress Under the GDPR

The Achilles heel of pre-GDPR EU privacy law was the fact that the European Commission's detailed rules lacked an effective enforcement mechanism. An academic critic states European data protection law has traditionally been overly broad, outdated, and under-enforced:

> Take data security breaches, for example: the broad, omnibus information requirements under existing European data protection laws have arguably always required companies to inform data subjects of security breaches, however, in practice European companies have rarely disclosed breaches. . . . In general, the European Union considers its own privacy law regime so deficient and outdated that it has recently proposed a complete overhaul, specifically referencing a need to update the rules on personal data in social media. Thus, it seems a myth that the European Union is somehow ahead of the U.S. in terms of social media privacy protections.[341]

Under the GDPR, EU data subjects are now armed with the ability to seek collective redress and to initiate investigations of data processors' privacy practices.[342] The preamble to the GDPR states a subsidiary purpose is to strengthen the rights and remedies of data subjects:

> Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.[343]

The GDPR will bring European enforcement practices closer to the more vigorous mechanisms of private class action litigation used in the United States to advance the public interest in an efficient manner.[344] Class action litigation permits data subjects with functionally equivalent

---

341. Determann, *supra* note 87, at 5 (footnotes omitted).

342. *See* GDPR, *supra* note 4, art. 77, at 80 (setting forth right to lodge complaints with supervisory authorities for infringement of the data subject's rights); *see also id.* art. 79 ("Right to effective judicial remedy against a controller or processor.").

343. *Id.* ¶ 11, at 3.

344. "The key institution is the plaintiff in the role of private attorney general who seeks civil recourse but also fulfills a broader purpose of identifying and punishing reckless corporate defendants who had previously evaded the attention of the public authorities." Rustad, *supra* note 104, at 440; *see also* THOMAS H. KOENIG & MICHAEL L. RUSTAD, IN DEFENSE OF TORT LAW 1–2 (2001) (discussing that many tort remedies are under siege).

complaints against a company to join in either a class action or representative action where a federal court consolidates the complaints into a single proceeding. In 2010, the European Data Protection Supervisor recommended that class actions be adopted as a way of strengthening enforcement. However, no action was taken at the time:

> Empowerment of data subjects requires, among others, the improvement of redress mechanisms: more options for the data subject to execute and enforce his rights, including the introduction of class action procedures, more easily accessible, and more effective and affordable complaints procedures and alternative dispute resolutions.[345]

Article 80 of the GDPR provides for representation through lawsuits filed by not-for-profit associations to protect data subjects' privacy rights.[346] The GDPR gives European data subjects the right to lodge a complaint with a supervisory authority for misuses of their data. In addition, Article 77 indicates that data subjects can choose to apply personally rather than be represented by a non-profit organization under Article 80. By permitting private lawsuits, the GDPR may fill the European Union's large enforcement gap.[347]

Prior to the GDPR, the European Union had not recognized class actions or other collective redress remedies of any kind. For example, in 2018, the European Court of Justice (ECJ) ruled that an Austrian law student could not initiate class action against Facebook on behalf of other data subjects.[348] The ePrivacy Regulation does not explicitly recognize a

---

345. Hustinx, *supra* note 311, at 3 (arguing that "[e]mpowerment of data subjects requires, among others, the improvement of redress mechanisms: more options for the data subject to execute and enforce his rights, including the introduction of class action procedures") (emphasis omitted).

346. GDPR, *supra* note 4, art. 80, at 81.

347. Article 82 of the General Data Protection Regulations gives data subjects to right to sue for monetary damages against controllers or processors:

> 1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
>
> 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Id. art. 82.

348. Patrick Kane, *GDPR—Collective Actions Under the Privacy Banner*, WSGR DATA ADVISOR (Mar. 26, 2018), https://www.wsgrdataadvisor.com/2018/03/gdpr-collective-actions/

mechanism for collective redress, but the Regulation incorporates through reference all rights and remedies granted under the GDPR. [349]

The Explanatory Memorandum for the proposed GDPR stated that only "bodies, organisations or associations which may lodge a complaint on behalf of the data subject or, in case of a personal data breach, independently of a data subject's complaint."[350] However, this language is not found in the adopted GDPR, meaning that EU data subjects now have private and public enforcement mechanisms in the form of the ability to file (1) individual complaints and (2) complaints through data protection authorities. Commentators have generally overlooked the European Union's recognition of a data subject's right to seek monetary damages against controllers and processors[351] through proceedings which closely parallel U.S. class actions.

Within hours of the enactment of the GDPR, a European data protection advocacy group, led by privacy activist Max Schrems, filed functionally equivalent data protection lawsuits against Facebook,[352]

[https://perma.cc/5U2M-XJCG] ("On January 25, 2018, the Court of Justice of the European Union (CJEU) ruled that Maximilian Schrems could not lead a collective-action lawsuit in his home country of Austria against Facebook. Schrems' suit claims that Facebook committed numerous violations of applicable data protection provisions. The CJEU ruled that in a collective action, the plaintiff assigned the claims cannot benefit from the EU consumer forum rule, which would have allowed Schrems to bring the case in his home country, when the other members of the class are not themselves a party to the contract in question." (footnotes omitted)); *see also EU Top Court Dismisses Class Action Suit Against Facebook*, DW (Jan. 25, 2018), http://www.dw.com/en/eu-top-court-dismisses-class-action-suit-against-facebook/a-42298391 [https://perma.cc/33WB-FMFR] (discussing the class actions against Facebook).

349. "Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679." *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, art. 21(1), COM (2017) 10 final (Oct. 1, 2017).

350. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 14, COM (2012) 11 final (Jan. 25, 2012).

351. *See* GDPR, *supra* note 4, art. 82, at 81 ("Right to Compensation and Liability").

352. *See* Complaint under Article 77(1) GDPR at 1, https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf [https://perma.cc/ZXP6-UG4Y] (complaint against Facebook Ir. Ltd. regarding Facebook).

Google,[353] Instagram,[354] and WhatsApp,[355] claiming these U.S. social media giants violated the mandatory consent provisions of the GDPR.[356] Contrary to the GDPR, these class actions each named an advocacy organization, noyb.eu, as class representative, seeking redress for coerced consent.[357] The noyb.eu describes the four complaints as follows:

> The GDPR prohibits such forced consent and any form of bundling a service with the requirement to consent (see Article 7(4) GDPR). Consequently access to services can no longer depend on whether a user gives consent to the use of data. On this issue a very clear guideline of the European data protection authorities has already been published in November 2017 . . . .
>
> Separation of necessary & unnecessary data usage. An end of "forced consent" does not mean that companies can no longer use customer data. The GDPR explicitly allows any data processing that is *strictly* necessary for the service – but using the data additionally for advertisement or to sell it on needs the users' free opt-in consent. With this complaint we want to ensure that GDPR is implemented in a sane way: Without just moving towards "fishing for consent".
>
> Putting an end to annoying pop-ups. If the complaints of *noyb.eu* are successful, it will also have a very practical effect: Annoying and obtrusive pop-ups which are used to claim a user's consent, should in many cases be a thing of the past.[358]

---

353. *See* Complaint under Article 77(1) GDPR at 1, https://noyb.eu/wp-content/uploads/2018/05/complaint-android.pdf [https://perma.cc/XNZ4-9PNP] (complaint against Google).

354. *See* Complaint under Article 77(1) GDPR at § 1.1, https://noyb.eu/wp-content/uploads/2018/05/complaint-instagram.pdf [https://perma.cc/AJ3F-PGWV] (complaint against Facebook Ir. Ltd. regarding Instagram).

355. *See* Complaint under Article 77(1) GDPR at 1, https://noyb.eu/wp-content/uploads/2018/05/complaint-whatsapp.pdf [https://perma.cc/Q4T8-RXGS] (complaint against WhatsApp Ir. Ltd.).

356. "Very similar complaints were filed with four authorities, to enable European coordination. In addition to the four authorities at the residence of the users, the Irish Data Protection Commissioner . . . will probably get involved in the cases too, as the headquarter of the relevant companies is in Ireland in three cases." *GDPR: noyb.eu Filed Four Complaints over "Forced Consent" Against Google, Instagram, WhatsApp and Facebook*, NOYB (May 25, 2018), https://noyb.eu/4complaints/ [https://perma.cc/L7SQ-3KJE] [hereinafter *noyb.eu Complaints*].

357. *See* Derek Scally, *Max Schrems Files First Cases Under GDPR Against Facebook and Google*, IRISH TIMES (May 25, 2018, 8:03 AM), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177 [https://perma.cc/R5S6-LKX8].

358. *noyb.eu Complaints*, *supra* note 356.

The class action complaint against Facebook "asks the regulator to impose 'effective, proportionate and dissuasive' fines as foreseen by GDPR, which in Facebook's case could run to €1.3 billion ($1.5 billion)."[359] Allowing data subjects to seek monetary damages in class actions is the most significant instance of the D.C. Effect on EU data privacy law. Unlike the United States, the European Union has not traditionally imposed wealth-based fines nor have they previously recognized the right of data subjects to file individual complaints through data protection authorities. However, both the GDPR and the ePrivacy Regulation impose wealth-based punishment to deter infringers.[360]

5. Privacy Enforcement & Wealth-Based Punishment

Companies in violation of the GDPR's data privacy rules face wealth-based fines of up to four percent of annual profits or €20 million euros, whatever amount is greater.[361] Evidence of a defendant's financial circumstances is permitted in order to calibrate the most efficient level of deterrence.[362] The European Union's $5.1 billion dollar fine against Google for antitrust violations, issued in July 2018, demonstrates that the threat of enormous GDPR fines must be taken seriously by corporate entities.[363]

Most U.S. states permit the admissibility of the financial condition or wealth of a defendant to set the level of punishment necessary to achieve optimal deterrence.[364] Punitive damages can be calibrated according to the wealth of the wrongdoer, as well as the actual or potential harm caused by the wrongdoing.[365] Tort reforms, often championed by large corporate defendants,[366] have resulted in significant limitations on the use

---

359. Reuters, *Data Privacy Activist Wastes No Time in Filing GDPR Complaints Against Facebook, Google, Instagram, and WhatsApp*, BUS. INSIDER (May 25, 2018, 6:19 AM), http://www.businessinsider.com/max-screms-gdpr-complaints-facebook-google-2018-5 [https://perma.cc/F59W-LH5U].

360. GDPR, *supra* note 4, art. 83(6), at 83.

361. *See id.* ("Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.").

362. *See id.* art. 83(2)(k), at 82.

363. *See* Allison Schiff, *After Google's $5B Antitrust Fine, Will GDPR Enforcement Be Next?*, AD EXCHANGER (July 18, 2018, 1:10 PM). https://adexchanger.com/privacy/gdpr-enforcement-what-we-know-so-far/ [https://perma.cc/KJ3J-JS8Z].

364. *See* Michael L. Rustad, *Unraveling Punitive Damages: Current Data and Further Inquiry*, 1998 WIS. L. REV. 15, 42–48 ("Punitive damages are based upon the wealth of the defendant in the vast majority of states . . . .").

365. Punitive damages awards may be calibrated to factors such as the wealth of the defendant, the potential harm of the defendant's course of conduct, the degree of bad faith of the defendant's actions, and any "larger pattern of fraud, trickery, and deceit." TXO Prod. Corp. v. All. Res. Corp., 509 U.S. 443, 444, 462 (1993) (citing Pac. Mut. Life Ins. v. Haslip, 499 U.S. 1, 21–22 (1991)).

366.

> Tort reformers seek to decouple corporate wealth from the punitive damages equation. They seek a system of punitive sanctions that treats everyone equally:

of a defendant's financial circumstances in setting the level of punitive damages throughout the United States.[367] Chart Two, below, reveals the maximum fines available against Facebook, Google, Instagram, and WhatsApp, based on the awards allowed by the GDPR in the cases discussed above.

Chart Two: GDPR Maximum Fines in nyob.eu Actions[368]

U.S. Company	Data Authority Where Action Was Filed	Maximum Penalties[369]
Facebook	DSB (Austria)	€ 1.3 Mrd
Google	CNIL (France)	€ 3.7 Mrd
Instagram	DPA (Belgium)	€ 1.3 Mrd
WhatsApp	HmbBfDI(Hamburg)	€ 1.3 Mrd

Fines for violating data protection orders could easily exceed the multi-billion-dollar awards imposed for violating EU competition law. In 2009, for example, the Commission imposed a €1.06bn fine against Intel

---

> the punitive damages paid by a drunk driver should be the same as those paid by a Fortune 500 company. . . .
>
> Wealth-sensitive punitive damages serve a deterrent function because that level of award that would punish an impoverished person would not 'sting' a wealthy person or company.

Michael L. Rustad, *The Closing of Punitive Damages' Iron Cage*, 38 LOY. L.A. L. REV. 1297, 1319–20 (2005) (documenting rules on limitations of wealth and financial condition of the defendant in punitive damages litigation across fifty-one jurisdictions).

367. *See, e.g.*, CAL. CIV. CODE § 3295(d) (West 2018) (California); MD. CODE ANN., CTS. & JUD. PROC. § 10-913(a) (LexisNexis 2018) (Maryland) ("In any action for punitive damages for personal injury, evidence of the defendant's financial means is not admissible until there has been a finding of liability and that punitive damages are supportable under the facts."); MONT. CODE ANN. § 27-1-221(7) (2018) (Montana); NEV. REV. STAT. § 42.005(4) (2018) (Nevada); N.D. CENT. CODE § 32-03.2-11(3) (2018) (North Dakota); OR. REV. STAT. § 30.925(2)(f) (2018) (Oregon); S. Life & Health Ins. Co. v. Whitman, 358 So. 2d 1025, 1026–27 (Ala. 1978) (Alabama).

368. Complaint under Article 77(1) GDPR, *supra* note 352, at 18 (Facebook); Complaint under Article 77(1) GDPR, *supra* note 353, at 15 (Google); Complaint under Article 77(1) GDPR, *supra* note 354, § 3.3 (Instagram); Complaint under Article 77(1) GDPR, *supra* note 355, at 16 (WhatsApp).

369. *Tutorial: Symbols and Abbreviations*, EUROSTAT (Mar. 15, 2017), http://ec.europa.eu/eurostat/statistics-explained/index.php/Tutorial:Symbols_and_abbreviations [https://perma.cc/6NA2-TT5A] ("EUR (or €) is the measuring unit. In English, 'EUR' (or the euro sign '€') is placed before the figure, separated by a (non-breaking) space, e.g. EUR 30. In French and German the order is reversed, e.g. 30 EUR. Note also that English uses the singular of terms such as million if they relate to a currency such as EUR 10 million. In French 10 Mio EUR and 10 Mrd EUR (without full stop) are used while German uses 10 Mio. EUR and 10 Mrd. EUR (with full stop). Try to avoid the term billion in all languages and replace it, if possible, by 1000 million, because the term means something different in (American) English (109) compared to German and French (1012). If it cannot be avoided, 'bn' may be used as an abbreviation for billion, but 'mn' should be avoided for million, as it has another meaning in the ISO system.").

for abusing its dominant position in the x86 CPU market.[370] In 2017, the European Commission imposed a €2.2bn fine against Google for "its abuse of its dominance of the search engine market in building its shopping comparison service."[371] Similar to U.S. punitive damages, Article 83(6) of the GDPR imposes fines based upon the wrongdoer's annual turnover:

> Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[372]

In 2017, Amazon's revenue was $178 billion dollars, up from $135.99 billion dollars in 2016 (approximately €152.3bn).[373] Four percent of €152.3bn is €6.1bn, which is Amazon's potential exposure for violating EU data protection law.

IV. TOWARDS A GLOBAL DATA PRIVACY STANDARD

A. *The GDPR as a Global Privacy Standard*

Most U.S. law school coverage about privacy is U.S.-centric, with almost no discussion of foreign or international developments. The Internet, by definition, is a global institution without territorial borders.[374] Professor David Post notes that:

> we talk about [the Internet] as if it were [a place], and we experience it as if it were; we "visit" websites and then we "leave" them and "go to" others; we meet people "on the Internet," we talk of "entry" and "access," "portals" and

370. European Commission Press Release IP/09/745, Antitrust: Commission Imposes Fine of €1.06bn on Intel for Abuse of Dominant Position; Orders Intel to Cease Illegal Practices (May 13, 2009), http://europa.eu/rapid/press-release_IP-09-745_en.htm [https://perma.cc/AG78-D84Z].

371. Daniel Boffey, *Google Appeals Against EU's €2.4bn Fine over Search Engine Results*, GUARDIAN (Sept. 11, 2017, 2:03 PM), https://www.theguardian.com/technology/2017/sep/11/google-appeals-eu-fine-search-engine-results-shopping-service [https://perma.cc/34PS-XWS3].

372. GDPR, *supra* note 4, art. 83(6), at 83.

373. *Net Sales Revenue of Amazon from 2004 to 2017 (in Billion U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/266282/annual-net-revenue-of-amazoncom/ [https://perma.cc/5YXL-V7PA].

374. Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J.L. & TECH. ¶ 5 (1997), http://vjolt.org/wp-content/uploads/2017/Articles/vol1/issue/vol1_art3.html [https://perma.cc/N2VL-6NCU].

> "trapdoors," logging in and logging on, home pages and site maps.[375]

The rapid expansion of the global consumer marketplace creates inevitable clashes between diverse legal traditions about legal norms.[376]

The Internet, by its very nature, is international, yet there is no uniform legal infrastructure protecting data wherever it resides or travels. The paradox is that the open Internet is one that disregards privacy. "Surveillance cameras, data brokers, sensor networks, and 'supercookies' record how fast we drive, what pills we take, what books we read, what websites we visit."[377] The misuse of Internet-based surveillance tools threatens our society as much as telephone wiretaps in the first decades of the twentieth-century when the tort of privacy was first recognized.

The architecture of the Internet makes the location of the server irrelevant. "Access doesn't depend on geography."[378] "[G]eographic indeterminacy is simply part of the network's normal operation."[379] The GDPR is rapidly emerging as the core of a de facto global policy standard of creating rights that are recognized wherever data is transferred or processed. The GDPR's rules for: (1) data minimization, (2) data rectification, storage, and processing limitations, (3) integrity, (4) confidentiality, (5) consent, and (6) a user's right to be forgotten, are being adopted around the world as described in this Part.

1. African Data Privacy Law is Generally Undeveloped

South Africa's data protection law, the Protection of Personal Information Act of 2013 (POPIA), and the GDPR are functional equivalents in many respects, but there are significant differences in specific data security rules.[380] Angola has enacted data protection rules

375. DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 3 (2009).

376. In 2017, the nation of Libya was ranked first in the Business Software Alliance's global survey of intellectual property violations with 90% of software pirated, followed by Venezeula and Zimbabwe with an 89% piracy rate. BUS. SOFTWARE ALL., GLOBAL SOFTWARE SURVEY 10 (2018), https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. [https://perma.cc/2BZ9-L2TY]. This worldwide piracy is valued at $46.3 billion. *Id.* at 12. The highest aggregate piracy losses outside the U.S. were found in China, India, and Finland. *Id.* at 10.

377. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3 (2015).

378. LAWRENCE LESSIG, CODE VERSION 2.0, at 16 (2006).

379. Burk, *supra* note 374, ¶ 18.

380. A legal commentator notes most of the definitions of South Africa's POPIA Act are close to the GDPR as are many provisions:

for sensitive data and transfers of data.[381] However, the nation currently lacks any effective enforcement mechanism.[382] Ghana's data privacy law protects personal data and has special statutory provisions for children's data.[383] It requires organizations to appoint data protection officers and limits what personal information can be collected.[384] Ghana also enacted a compulsory data breach notification statute requiring data processors to implement reasonable and appropriate security.[385]

Many African countries have not taken significant steps toward compliance with the GDPR. For example, in Nigeria, "only a small number of companies appear interested in setting up GDPR compliance processes."[386] Africa has the largest number of the least-developed countries in the world, so it is not unexpected that the GDPR's gravitational pull has been less than on other continents.[387] Much of Sub-

---

> The problem is that they are slightly different in some very important ways. For example, regards security . . . .
>
> > The GDPR does not protect legal entities. It also does not create such serious penalties for failing to protect an account number. It exempts some SMEs from having to keep records. . . . The GDPR also makes it obligatory for some organisations to have a data protection officer, whereas POPIA provides that every organisation has an information officer by default. And the GDPR deals with the right to be forgotten and data portability. The GDPR has a definition of genetic data and requires data controllers to do data protection impact assessments. The fines are much bigger in the GDPR but there no criminal offences in the GDPR.

John Giles, *What Does the GDPR Mean for the POPI Act? GDPR v. POPIA*, MICHALSONS (May 13, 2016), https://www.michalsons.com/blog/gdpr-mean-popi-act/19959 [https://perma.cc/2N52-UDX4].

381. *See* DLA PIPER, *supra* note 62, at 8–12.

382. *See id.* at 10 ("[T]he competent authority for the enforcement of Data Protection Law is the APD. However, considering that the APD is not yet created, the level of enforcement is not significant at this stage.").

383. *See id.* at 199.

384. *See id.* at 200.

385. *See id.* at 201.

386. Enyioma Madubuike, *GDPR: 7 Types of Nigerian Companies that Should Comply*, TECHPOINT.AFRICA (May 31, 2018), https://techpoint.ng/2018/05/31/gdpr-compliance-nigeria/ [https://perma.cc/D7M7-T8NS].

387. The United Nations includes the following African countries on its list of the least developed countries: Angola, Benin, Burkina Faso, Burundi, Cape Verde, Central African Republic, Chad, Comoros, Congo (Dem. Republic of the), Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Guinea, Guinea-Bissau, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mozambique, Niger, Rwanda, Sao Tome and Principe, Senegal, Sierra Leone, Somalia, Sudan, Tanzania, Togo, Uganda, and Zambia. *Least Developed Countries (LDCs)*, ONE WORLD NATIONS ONLINE, http://www.nationsonline.org/oneworld/least_developed_countries.htm [https://perma.cc/8WWR-HRN3].

Saharan Africa, for example, lacks wired broadband access, so there will be little need to update their privacy law to comply with the GDPR.[388]

2. Most Asian Countries Align With the GDPR

Asian countries have been scrambling to become GDPR compliant as many companies in Asia render goods or services to EU consumers. In 2018, China had 772 million Internet users, as compared to 312 million Americans with Internet access.[389] China enacted a cybersecurity law in 2017 that "requires critical information infrastructure operators (CIIOs) to store personal information and important data collected and generated within the territory of the PRC."[390] China's new cybersecurity statute proposes to define "personal data as information that identifies a natural person either by itself or in combination with other information. The term includes a person's name, address, telephone number, date of birth, identity card number and biometric identifiers."[391]

Under China's cybersecurity statute, data controllers must obtain consumers' consent to transfer their personal information outside of China. This rule applies even where the transfer is to an affiliate or to an overseas storage facility, for example, in connection with the use of offshore cloud storage.[392] China does not recognize a right to be forgotten but gives Chinese data subjects the right to erase personal information posted on the Internet that violates their legal rights.[393]

---

388. *See* Arturo J. Carri, *Having Your Cake and Eating It Too? Zero-rating, Net Neutrality and International Law*, *in* TOWARDS AN INTERNET FREE OF CENSORSHIP II: PERSPECTIVES IN LATIN AMERICA 81, 108–09 (Agustina del Campo ed., 2017), https://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf [https://perma.cc/H5TV-ZC6N] ("This helps explain why the wired broadband access in Zambia is less than 1 percent of the population; even in South Africa, the richest country in Sub-Saharan Africa, barely above 3 percent of the population is connected in this way.").

389. *See Top 20 Countries with the Highest Number of Internet* Users, INTERNET WORLD STATS (Dec. 31, 2017), https://www.internetworldstats.com/top20.htm [https://perma.cc/2L9Y-4UQ7].

390. Sara Xia, *China Data Protection Regulations (CDPR)*, CHINA L. BLOG (May 20, 2018), https://www.chinalawblog.com/2018/05/china-data-protection-regulations-cdpr.html [https://perma.cc/3E64-ZNDX].

391. Richard Bird, *Where Are We Now with Data Protection Law in China?*, FRESHFIELDS BRUCKHAUS DERINGER (Sept. 13, 2018), https://digital.freshfields.com/post/102f217/where-are-we-now-with-data-protection-law-in-china [https://perma.cc/EA36-88B3].

392. *Id.*

393. *See id.*; *see also* Nathan Jubb, *Chinese Have No Right to Be Forgotten, Court Rules*, SIXTH TONE (May 5, 2016), http://www.sixthtone.com/news/814/chinese-have-no-right-be-forgotten-court-rules [https://perma.cc/ZJ3E-AV86] ("Wei Yongzheng, a retired professor from the Shanghai Academy of Social Sciences and an expert in mass media law, [stated] that China does have something called a 'right to erase . . . .' If citizens find their personal identity is revealed, private information is spread, or if other information that encroaches on their legal rights is found

Asia-Pacific region exporters such as Japan, Hong Kong, and the Philippines have been particularly active in adapting to the GPDR.[394] Japan's new data protection statute went into effect on May 30, 2017, making Japan the first country to be recognized as an EU "white listed" jurisdiction.[395] Japan and the European Union have recently announced a GDPR safe harbor agreement, which is, in effect, an EU approval of Japan's data protection regime.[396] Recently, the Supreme Court of Japan "issued its very first decision citing conditions for allowing for the deletion of information from internet search results, although its ruling made no mention of the 'right to be forgotten.'"[397]

Japan's data protection law differs in some respects from the GDPR. For example, unlike the strong extraterritorial provisions of the GDPR, Japan's "[Act on the Protection of Personal Information (APPI)] does not have express provisions dealing with jurisdiction and territoriality." [398] Japan does not recognize the institutions of data controllers and data processors.[399] Japan and the European Union "will continue their cooperation and aim by early 2018 to recognize each other as having adequate levels of personal data protection."[400] Hong Kong's PDPO is the Office of the Privacy Commissioner for Personal Data (PCDP), which has primary responsibility for ensuring compliance with the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO).[401]

In South Korea, "[a]s of July 25, 2016, as a result of an amendment to PIPA, in instances Personal Data breaches caused by the Data Handler's intentional act or negligence, the Data Handler may be liable for three

---

on the Internet, they have the right to request the network service provider to erase the relevant information . . . .").

394. Matthew Pokarier, *The EU General Data Protection Regulation and What It Means for Australian Business*, CLYDE&CO (June 27, 2018), https://www.clydeco.com/insight/article/the-eu-general-data-protection-regulation-and-what-it-means-for-australian [https://perma.cc/C72H-YTFL].

395. Kensaku Takase, *GDPR Matchup: Japan's Act on the Protection of Personal Information*, IAPP (Aug. 29, 2017), https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/ [https://perma.cc/P9VR-8M5U].

396. Correspondent, *European Union and Japan Agree to Create World's Largest Area of Safe Data Flows*, EUREP. (July 20, 2018), https://www.eureporter.co/frontpage/2018/07/20/european-union-and-japan-agree-to-create-worlds-largest-area-of-safe-data-flows/ [https://perma.cc/4YK5-PTXK].

397. *Court Decision May Fire Up 'Right to be Forgotten' Debate*, JAPAN TIMES (Feb. 2, 2017), https://www.japantimes.co.jp/news/2017/02/02/national/crime-legal/court-decision-may-fire-right-forgotten-debate/#.W2YI2k2WyUk [https://perma.cc/T4ZP-DVRB].

398. Takase, *supra* note 395.

399. *Id.*

400. *Id.*

401. Personal Data (Privacy) Ordinance, (2018) Cap. 486, 2-2, § 5 (H.K.).

times the damages suffered."[402] "Singapore is planning to review its personal data protection laws to keep up with the changing technology landscape, such as the growing adoption of the Internet of Things where seeking consent from consumers for the collection and use of personal data may not be practical."[403]

India protects personal information "through Section 43-A and Section 72-A of the Information Technology Act (2000) and the IT Rules (2011)."[404] India's Information Technology Act addresses:

> reasonable security practices and laws regulating the use and collection of personal data. The laws primarily regulate the processing of sensitive personal data or information (SPDI) which includes, among other things, financial information, medical information and sexual orientation. Non-SPDI is subject to very little regulation.
>
> Further reducing these protections, the IT Rules only protect data collected at the first stage, i.e., when the data is collected from the individual to the entity doing the collection. Subsequent transfers from the original controller are not governed by the IT Rules.[405]

In 2011, India's Ministry of Communication and Information Technology released a press note clarifying this and stating that India is in the process of bringing itself closer to compliance with the GDPR's "gold standard" of data privacy protection[406] by updating its data protection rules[407] to meet its policy goal of Digital India.[408] "India has bee[n] in dire[ct] need of a data protection law. The [proposed statute]

402. DLA PIPER, *supra* note 62, at 532.

403. Aaron Tam, *Singapore to Review Personal Data Protection Rules*, COMPUTER WKLY. (July 28, 2017, 5:33 AM), https://www.computerweekly.com/news/450423530/Singapore-to-review-personal-data-protection-rules [https://perma.cc/UY3N-B6MC] (considering new rules for notifying consumers of data breaches).

404. Jasdeep Singh, *Cross-Border Data Transfers in Privacy-Driven India*, IAPP (Mar. 27, 2018), https://iapp.org/news/a/cross-border-data-transfers-in-privacy-driven-india/ [https://perma.cc/ZG92-3EKC].

405. *Id.*

406. Nicolaj Nielsen, *GDPR: A Global 'Gold Standard'?*, EU OBSERVER (May 31, 2018, 2:49 PM), https://euobserver.com/justice/141906 [https://perma.cc/6UQJ-X5KA] ("EU officials and lawmakers like to say the [GDPR] is setting a new global standard.").

407. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India) (amending the Information Technology Act of 2000).

408. News Staff, *Srikrishna Panel Submits Data Protection Bill to MEITY; No Word on Aadhaar*, TECH2 (July 27, 2018, 7:37 PM), https://www.firstpost.com/tech/news-analysis/srikrishna-committee-finally-submits-personal-data-protection-bill-to-meity-4836631.html [https://perma.cc/2EK3-GPV8].

aims to protect the digital rights of Indian citizens and addresses issues such as consent, protecting children's rights in the digital age and . . . empower[] citizens to fight for their digital rights."[409]

India's rules for the transfer of personal data to other countries, similar to the GDPR, provide: "The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under the Privacy Rules."[410]

India's data breach notification law also closely parallels those requirements of the GDPR and provides:

> The Government of India, has established and authorised the Indian Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.
>
> The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain 'cyber security incidents.'[411]

In July of 2018, India proposed a data protection statute with a right to be forgotten, security breach notification rules, and rules for the processing and storage of data, congruent with the GDPR.[412] "Indian IT/ITeS companies earn close to 30% of their revenue from European market," and must adhere to the GDPR.[413]

---

409. *Id.*

410. DLA PIPER, *supra* note 62, at 255.

411. *Id.* at 256.

412. Sunetra Ravindran & Sohini Chatterjee, *Data Protection Bill: How the Draft Law Has Circumvented Undesirable Private Regulation by Data Fiduciaries*, TECH2 (Aug. 3, 2018, 7:28 PM), https://www.firstpost.com/tech/news-analysis/data-protection-bill-how-the-draft-law-has-circumvented-undesirable-private-regulation-by-data-fiduciaries-4888261.html [https://perma.cc/3MAQ-SWEV] ("The draft law equips data principals with a right to be forgotten. It has been criticised for not including the right to erasure. Here, erasure refers to the permanent deletion of personal data from its source. As the report highlights, the relevant distinction to be drawn is between a restriction on disclosure (like delinking from a search engine) and permanent removal from the fiduciary's storage.").

413. *India Getting GDPR Ready*, 17 BANKING FRONTIERS 10, 11 (2018).

A human rights organization, Bytes for All, concludes that "Pakistan is now in urgent need of data protection legislation that is not only intelligible but also fit for purpose."[414] "[Their] report recommends incorporating principles of individual's consent for processing data in any new legislation[,] emphasising that it is crucial to state [this right] in an unambiguous and intelligible manner. Moreover, the requirement of consent and consent withdrawal should be part of any data collection process."[415]

Privacy International, another human rights organization, describes the key attributes of Pakistan's current data protection laws:

> 1. Constitutional privacy protections: Article 14(1) of the Constitution of the Islamic Republic of Pakistan states that "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable."
>
> 2. Data protection laws: Pakistan does not at present have direct data protection legislation.
>
> 3. Data protection agency: Pakistan does not at present have a data protection authority.

---

414. *Pakistan Needs Laws Which Protect the Public's Data*, EXPRESS TRIB. (Jan. 31, 2018), https://tribune.com.pk/story/1622506/1-pakistan-needs-laws-protect-publics-data/ [https://perma.cc/2M53-CGLK] (quoting BYTES FOR ALL ET AL., ELECTRONIC DATA PROTECTION IN PAKISTAN 39 (2017), http://digitalrightsmonitor.pk/wp-content/uploads/2018/01/Data_Protection_in_Pakistan.pdf [https://perma.cc/47AN-5TZP]) ("The 'Electronic Data Protection in Pakistan' report, based on findings from Bytes for All — a human rights organisation and a research think tank with a focus on information and communication technologies . . . ." The Report called for best practices on data protection, using Pakistan as a case study:

> "At a time, when digital surveillance promotes Orwellian, STASI like oppression, there is a dire need for pro-people, human rights-based principles and practices, which protect citizens online and offline. This is particularly important in the case of Pakistan, where different citizens' databases and safe city projects pose a serious threat to civil liberties," . . . .
>
> The research underscores the need of establishing a system of accountability for data breaches applicable to big data repositories such as the National Database and Registration Authority (NADRA) and the Safe City projects, which are the largest repositories of biometric and facial imprints of Pakistani citizens.

Id.

415. *Id.*

> 4. Recent scandals: Interception across Pakistani networks is pervasive; some of it is also unlawful, according to investigative and media reports.
>
> 5. ID regime: Pakistan has one of the world's most extensive citizen registration regimes. This is run by the National Database & Registration Authority (NADRA).[416]

Privacy International and Bytes for All express particular concern about widespread government surveillance:

> Pakistan has a deplorable track record on internet issues, as it continues to carry out widespread mass surveillance, filtering and censorship of cyberspace. In recent months, researchers have found active presence of Netsweeper, an internet firewall that resulted in a mass URL filtration in Pakistani cyberspace with dire consequences for many rights including freedom of expression. It has been over a year since YouTube was banned and more recently a secret censorship arrangement was also exposed between Facebook and the Government of Pakistan. The command and control servers for the digital surveillance technology FinFisher have been also found in Pakistan.[417]

The least developed Asian countries have either not enacted data protection laws or have privacy laws that are out of date.[418] "In Indonesia, as of the date of this publication there is no "general law on data protection... However, there are certain "regulations concerning the use of electronic data."[419] Inspired by the GDPR, the West-Asian nation of Turkey is currently in the process of instituting Privacy by Design and data minimization regulations paralleling the EU Directive.[420]

---

416. *State of Privacy Pakistan*, PRIVACY INT'L (Jan. 2018), https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan [https://perma.cc/9F2K-8BFX] (alteration in original).

417. Privacy Int'l & Bytes for All, *Online Surveillance Becomes a Priority for the Human Rights Council, as Pakistan Joins the Wrong Side of the Debate*, PRIVACY INT'L (Feb. 9, 2018), https://privacyinternational.org/press-release/1517/online-surveillance-becomes-priority-human-rights-council-pakistan-joins-wrong [https://perma.cc/MU4B-FM7A].

418. Afghanistan, Bangladesh, Bhutan, Cambodia, Lao PDR, Maldives, Myanmar, Nepal, Timor-Leste, and Yemen are classified as the least developed countries of Asia. *Least Developed Countries (LDCs)*, *supra* note 387.

419. DLA PIPER, *supra* note 62, at 212.

420. Nazli Gozde Cakmak & Susen Aklan, *Turkey: Privacy by Design and by Default Approach Under Turkish Data Protection Law*, MONDAQ (June 25, 2018), http://www.mondaq.com/turkey/x/712466/Data+Protection+Privacy/Privacy+By+Design+And+By+Default+Approach+Under+Turkish+Data+Protection+Law [https://perma.cc/EVW3-DHMV]

3. Central America's Data Protection Developments

Most Central American countries have not begun to revise their data protection laws or practices to comply with the GDPR, but there are a few exceptions. Mexico has made the greatest progress in strengthening its data protection. "[B]oth[] the Mexican Regulations to the Federal Data Protection Law Held by Private Parties and the EU GDPR, focus on when using new technologies is likely to result in a (high) risk to the privacy or to the rights and freedoms of natural persons."[421] Honduras's constitutional protection of habeas data, gives:

> individuals the right 'to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources.'[422]

Honduras recently enacted a statute that:

> enables the access of any person to all the information contained in public entities, except that which is classified as 'Confidential.' It also extends the Constitutional Protection of Habeas Data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economic damage to people.[423]

> The development of data privacy regulation in Costa Rica is divided among two laws (the "Laws"). The first law is Law No. 7975, *Undisclosed Information Law*, which makes it a crime to disclose confidential/personal information

("Article 12 of the Law numbered 6698 creates the infrastructure of the privacy by design and by default approach. Also, it is likely to find influences of such approach in guidelines and documents concerning the protection of personal data published by the Board. The regulations relating to the protection of personal data in Turkey are prepared based on the Directive, however the enactment of the GDPR will have a major impact on the existing regulations and practices. We anticipate that such kind of principles of the GDPR will be implemented in Turkey in the next periods.").

421. Miguel Recio, *GDPR Matchup: Mexico's Federal Data Protection Law Held by Private Parties and Its Regulations*, IAPP (June 8, 2017), https://iapp.org/news/a/gdpr-matchup-mexicos-federal-data-protection-law-held-by-private-parties-and-its-regulations/ [https://perma.cc/Y5F3-32P7].

422. DLA PIPER, *supra* note 62, at 188 (discussing Law for Transparency and for Access to Public Information (Article 3.5, Decree 170-2006)).

423. *Id.*

> without authorization. The second law is Law No. 8968, *Protection in the Handling of the Personal Data of Individuals*, and its by-laws were enacted regulate the activities of companies that administer databases containing personal information. Therefore, its scope is limited.[424]

4. Eastern and Central Europe

"Russia adopted its first data protection law in 2006 and amended it significantly in 2015."[425] These laws will probably be judged not GDPR compliant. "The notable highlight of these amendments is the requirement to store personal data of Russian citizens in databases physically located in Russia . . . ."[426] Critics contend that this is a major step away from data privacy. "In Russia, the security services can intercept any communications they like, from the biggest email service Mail.ru to the social network Vkontakte. Once the new law went into force, they would be able to do the same with international platforms."[427] Bulgaria, the Czech Republic, Croatia, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia are the members of the European Union where the GDPR is in effect.[428]

5. The GDPR is in Effect in Europe

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) went into effect on May 25, 2018 without requiring implementation by the EU Member States through national law.[429] The European Free Trade Association (EFTA) countries—Iceland, Lichtenstein, and Norway—have agreed to adopt the GDPR

---

424. *Id.* at 112.

425. Volha Samasiuk, *When the GDPR is Not Quite Enough: Employee Privacy Considerations in Russia, Belarus, and Ukraine*, IAPP (Mar. 27, 2018), https://iapp.org/news/a/when-the-gdpr-is-not-quite-enough-employee-privacy-considerations-in-russia-belarus-and-ukraine/ [https://perma.cc/P8GC-2YVX].

426. *Id.* (noting the combined effect of the requirement with "the increased power of the Federal Service for Supervision of Communication, Information Technology and Mass Media (Roskomnadzor), and its recent focus on enforcement activities").

427. Andrei Soldatov & Irina Borogan, *Putin Trolls Facebook: Privacy and Moscow's New Data Laws*, FOREIGN AFF. (Nov. 3, 2015, 12:00 AM), https://www.foreignaffairs.com/articles/russian-federation/2015-11-03/putin-trolls-facebook [https://perma.cc/9E5M-8AR4]. "In reality, the law had nothing to do with data protection. The real goal was to make international technology companies subject to Russian communications law, under which all Internet service providers and network hosts in the country must provide the Russian security services with direct and unrestricted access to their servers." *Id.*

428. *EU Member Countries in Brief*, EUR. UNION, https://europa.eu/european-union/about-eu/countries/member-countries_en [https://perma.cc/DA35-L6VT] (last updated Sept. 19, 2018).

429. DLA PIPER, *supra* note 62, at 25.

Regulation.[430] "All businesses in the Channel Islands will be affected as new Guernsey and Jersey laws have come into force to adopt the GDPR into domestic legislation."[431] Guernsey[432] recently enacted a GDPR compliant statute.[433] The Data Protection Law (DPL) implements provisions equivalent to those in the EU GDPR.[434]

6. Data Protection Development in the Middle East

Relatively few Middle Eastern countries, with the notable exception of Israel, target EU consumers, so the Brussels Effect is relatively insignificant in the Middle East. Most Middle Eastern countries do not have laws that regulate protection of personal data. In traditionalist Muslim countries, complying with the GDPR is problematic because *Shari'a* legal principles are based on the *Quran's* moral precepts. These religious principles can conflict with the more individualistic personal privacy rights valued in Western nations:

> *Shari'a* principles (that is, Islamic principles derived from the Holy *Quran* and the *Sunnah*, the latter being the witnesses' sayings of the Prophet Mohammed), which although not codified, are the primary source of law in the [Kingdom of Saudi Arabia (KSA)]. In addition to *Shari'a* principles, the law in the KSA consists of secular regulations passed by government, which is secondary if it conflicts with *Shari'a* principles.
>
> At this time, there is no specific data protection legislation in place in the KSA (although we understand that

430. *General Data Protection Regulation (GDPR) Entered into Force in the EEA*, EFTA (July 19, 2018), http://www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576 [https://perma.cc/QX76-MNS7].

431. *GDPR*, CAREY-OLSEN, https://www.careyolsen.com/services/regulatory/gdpr [https://perma.cc/GFH2-UEZN].

432. Under its Protocol 3 relationship with the EU, Guernsey is part of the customs territory which allows for the free movement of goods. Protocol No. 3 of the Treaty of Accession, art. 1, 1972 O.J. (L 73) 164 (EC), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1972:073:FULL&from=EN [https://perma.cc/9UWJ-5C9N]. For most purposes the islands are treated as third countries and outside of the EU. *Id.*

433. Data Protection (Bailiwick of Guernsey) Law, 2017, http://src.bna.com/zY1 [https://perma.cc/W7QG-J2CL].

434. The Data Protection (Bailiwick of Guernsey) Law, 2017 (DPL) is designed to implement provisions equivalent to those in the EU General Data Protection Regulation, which came into force on May 25, 2018. The DPL repealed Guernsey's previous data protection law, the Data Protection (Bailiwick of Guernsey) Law, 2001, along with its amending ordinances and related regulations. *See id.* § 113.

> a new freedom of information and protection of private data law is under review by the Shura Council).[435]

Israel has the most advanced data protection laws in the region. Numerous laws protect the privacy of citizens in Israel such as: "the Basic Law: Human Dignity and Liberty, 5752 - 1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the 'PPL') and the guidelines of the Israel Privacy Authority."[436] Israel recently enacted Data Security Regulations and updated Outsourcing Guidelines which expand protections for outsourced processing of personal data, "even prior to entering into a data transfer agreement between the database owner and the data recipient and the requirements to be included therein."[437]

Egypt does not have a data protection law, though "there are some piecemeal provisions in connection with data protection in different laws and regulations."[438] Egypt has proposed a number of statutes addressing "state surveillance and the transfer and processing of data, including (i) draft law regarding the combat of the electronic and information crimes; and (ii) draft law regarding cyber security."[439] Qatar recently enacted a data protection law that captures certain aspects of European-style data protection and privacy.[440]

7. GDPR Compliance in North America

Parts I and II of this Article have documented that many GDPR innovations such as security breach notification and wealth-based fines originated in the United States. The United States' fragmented privacy regime consists of approximately "20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories."[441] "The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data."[442]

A few states have enacted GDPR compliant statutes. California, for example, enacted "the 'Privacy Rights for California Minors in the

435. DLA PIPER, *supra* note 62, at 404.
436. *Id.* at 275.
437. *Id.* at 278.
438. *Id.* at 146.
439. *Id.* at 148.
440. *Id.* at 464.
441. *Id.* at 503.
442. *Id.*

Digital World' law, known as the 'eraser' law.'"[443] One commentator argues that this "law illustrates . . . strong political support (at least in some states) for enactment of Internet protections, which may include some form of the 'right to be forgotten.'"[444]

Canada's Personal Information Protection and Electronic Documents Act adopts GDPR standards for consent, transparency, and information security.[445] "With respect to openness/transparency, generally Canadian Privacy Statutes require organisations make information about their personal information practices readily available."[446] All Canadian Privacy Statutes require that personal data is accurate, especially if disclosed to another organization.[447] "While the Canadian Charter of Rights provides constitutional protection to fundamental freedoms such as freedom of expression, Canada has also adopted data protection laws, which are similar to the European Directive 95/46/EC."[448] The right to be forgotten is recognized in Canadian privacy law.[449]

8. Oceania Data Protection Development

Australia and New Zealand are the only countries in Oceania with advanced data protection statutes.[450] The least developed countries of Oceania, such as Fiji, Kiribati, Marshall Islands, Micronesia, Naru, Palau, Papua New Guinea, Samoa, and the Solomon Islands, have not enacted data protection statutes.[451] Australia is updating its data privacy regulations to become GDPR compliant. In 2018, Australia enacted breach notification laws that parallel the GDPR.[452] "There is currently no

443. Steven C. Bennett, *Is America Ready for the Right to Be Forgotten?*, 88 N.Y. ST. B. ASS'N J. 10, 12 (2016).

444. *Id.* at 13 (footnote omitted).

445. Timothy M. Banks, *GDPR Matchup: Canada's Personal Information Protection and Electronic Documents Act*, IAPP (May 2, 2017), https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/ [https://perma.cc/Y84J-ZK6M].

446. DLA PIPER, *supra* note 62, at 81.

447. *Id.*

448. Eloise Gratton & Jules Polonetsky, *Droit A L'Oubli: Canadian Perspective on the Global 'Right to Be Forgotten' Debate*, 15 COLO. TECH. L.J. 337, 337 (2017).

449. *See* Mike Wagner & Yun Li-Reilly, *The Right to Be Forgotten*, 72 ADVOCATE 823, 826 (2014) ("The right to be forgotten as a concept existed in fact, in Canadian legal thinking, long before the European court's ruling. The B.C. privacy commissioner has referred to the right to be forgotten more than once in support of decisions.").

450. *See* DLA PIPER, *supra* note 62, at 19–24, 403–08.

451. *See Data Protection Laws of the World*, DLA PIPER, https://www.dlapiperdata protection.com/ [https://perma.cc/V4FV-KCWT].

452. *See* Jim Lennon & Edward Odendaal, *Data Breach Notification to Become Mandatory in Australia from 22 February 2018*, DATA PROTECTION REP. (Feb. 7, 2018), https://www.dataprotectionreport.com/2018/02/data-breach-notification-to-become-mandatory-in-australia-from-22-february-2018/ [https://perma.cc/L8F3-GLRC].

obligation to report breaches to affected individuals or to the [Office of the Australian Information Commissioner (OAIC)], however, from February 22, 2018, entities with existing obligations to comply with the [Australian Privacy Principles (APPs)] under the Privacy Act must comply with mandatory reporting requirements under the mandatory data breach notification regime."[453]

New Zealand has strong "privacy laws that give individuals some power over how accessible their private information is to the public."[454] "The New Zealand privacy laws have been found 'adequate' by the European Union, though they are currently being reformed to become even more robust."[455] All Australian and New Zealand companies holding or processing the personal data of EU residents will be required to comply with the GDPR or to stop doing business in the world's largest single market.

9. Data Protection Reform in South America

Most South American countries do not have modern data privacy rules congruent with those of the European Union,[456] but there are exceptions. Argentina and Uruguay are the South American countries closest to compliance with the GDPR's "gold standard" of data privacy protection.[457] Argentina has adopted many GDPR principles, including rules for the transfer of personal data to third parties.[458] Argentina enacted the "Personal Data Protection Law Number 25,326 (the 'PDPL')" in October 2000.[459] The European Commission ruled in 2003 "that

453. DLA PIPER, *supra* note 62, at 23.

454. James Greenland, *Privacy Week 2016 - A "Right to be Forgotten"?*, N.Z. L. SOC'Y (May 12, 2016), https://www.lawsociety.org.nz/news-and-communications/latest-news/news/privacy-week-2016-a-right-to-be-forgotten2 [https://perma.cc/U8KF-3A6K].

455. Nathalie Morris, *What New Zealand Marketers Need to Know About the GDPR*, MARKETING ASS'N, https://www.marketing.org.nz/GDPR [https://perma.cc/H7PD-9RAT].

456. *See Data Protection Laws of the World*, *supra* note 451.

457. *See* Nielsen, *supra* note 406 ("EU officials and lawmakers like to say the general data protection regulation (GDPR) is setting a new global standard.").

458. Florencia Rosati et al., *Data Protection in Argentina: Overview*, THOMSON REUTERS: PRACTICAL L., https://us.practicallaw.thomsonreuters.com/3-586-5566 (last updated June 1, 2018) ("*Purpose proportionality*. Personal data collected for processing must be relevant and not excessive in relation to the scope and purpose for which it was obtained. *Data accuracy*. Personal data collected for processing must be correct and accurate. It must also be updated, corrected, or deleted as necessary; this is in addition to the data subjects' right to request this. *Purposes restriction*. Data collected for processing must not be used for any purpose other than the purpose it was collected for. *Confidentiality*. Those responsible or involved in any part of the data processing are bound by the duty of confidentiality. *Access right*. Data must be stored in a way that enables data subjects to exercise their right of access.").

459. Law No. 25.326, Oct. 4, 2000, [29.517] B.O. 1 (Arg.) (decreeing the Protection of Personal Data (Personal Data Protection Law, or PDPL)).

Argentina provides an 'adequate' level of protection of personal data, in line with the Data Protection Directive (95/46/EC)."[460]

Under the Argentine Data Protection Regulations (ADPR), "personal data is defined as any type of information of any kind that refers to individuals or legal entities, whether identified or identifiable by an associative process. The ADPR protects all personal data, not only sensitive data."[461] Argentine courts are predisposed to recognizing the right to be forgotten.[462] In Argentina, a large number of right to be forgotten requests have been litigated, but most have been reversed by its highest court:

> Although celebrity clients achieved several victories over Google and Yahoo, the Supreme Court of Argentina, in late 2014, struck a blow to the right to be forgotten when it decided against the model María Belén Rodriguez. The court held that search engines do not have a general obligation to obscure or hide search results linking individuals such as Rodriguez to objectionable websites. However, the court did allow that a search engine may be obligated, upon a specific request, to remove results that include child pornography or information that would facilitate criminal conduct. Leguizamón and his partner, Alejandro Arauz Castex, did not concede that the battle over the right to be forgotten was over, even after the Supreme Court decision.[463]

Although Brazil currently has no comprehensive data privacy law, Brazilian President Michel Temer signed into law *Lei Geral de Proteção de Dados* or LGPD (Law 13,709/2018) on August 14, 2018.[464] Brazil approved a new data protection law that incorporates the GDPR standard of data minimization.[465] Brazil is also working to enact a GDPR-inspired

460. DLA PIPER, *supra* note 62, at 14.

461. Rosati et al., *supra* note 458.

462. *See* Edward L. Carter, *Argentina's Right to Be Forgotten*, 27 EMORY INT'L L. REV. 23, 35 (2013) ("Argentina's courts appear willing at this point to grant celebrity plaintiffs an effective right to control use of their images online even if not broadly instituting a new right to be forgotten.").

463. Edward L. Carter, *The Right to Be Forgotten*, OXFORD RES. ENCYCLOPEDIA COMM. 12 (Nov. 2016), http://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189?print=pdf [https://perma.cc/7YVB-NYVU].

464. Lei No. 13.709, de 14 de Agosto de 2018, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] (Braz.) (enacting Geral de Proteção de Dados or LGPD).

465. *Brazil Approves New Data Protection Law*, LEADER'S LEAGUE (July 31, 2018), https://www.leadersleague.com/en/news/brazil-approves-new-data-protection-law [https://perma.cc/2K7N-TGJR]. ("[P]rivate and public entities may only collect and store data which is necessary for the provision of services. All parties will be subject to auditing by the newly created National Data Protection Authority and could face penalties reaching up to $50 million.").

online data protection law, including "a right to be forgotten" that would require the removal, upon request, of "links from Internet search engines that make reference to irrelevant or outdated data."[466]

In 2017, Chile began updating its outdated data protection law.[467] Chile's draft data protection law "provides rights for data subjects including access, rectification, cancellation, opposition and portability."[468] Chile's new data protection regime recognizes "[a] Personal Data Protection Agency . . . ensuring compliance with rules on personal data processing, and subject to the monitoring of the President of the Republic via the Department of the Treasury."[469]

Colombia, the third largest economy in Latin America,[470] "has passed and implemented various privacy laws and regulations, including Law 1581 in 2012, Decree 1377 in 2013, Resolution 20752 in 2013, Law 1712 in 2014 and Decree 886 in 2014."[471] "Further, Colombia is looking to fit into the global marketplace by establishing itself as a jurisdiction where data protection and privacy are taken seriously."[472]

In Uruguay, "the data processor should obtain prior documented consent from the individual or entity whose information is being processed."[473] "Personal data can only be transferred to a third party . . . for purposes directly related to the legitimate interests of the transferring party and the transferee; and . . . with the prior consent of the data subject. However, such consent may be revoked."[474] In 2001, the Venezuelan Supreme Court:

---

466. Albert Gidari, Jr., *My Vote for Privacy Person of the Year*, JD SUPRA (Dec. 3, 2014), https://www.jdsupra.com/legalnews/my-vote-for-privacy-person-of-the-year-97641/ [https://perma.cc/5PGQ-DXVC].

467. *See* Lucia Bobadilla & Paulina Silva, *The Proposed Revision of Chile's Data Protection* Act, IAPP, https://iapp.org/news/a/the-proposed-revision-of-chiles-data-protection-act/ [https://perma.cc/D2LU-K4LD].

468. *Id.*

469. *Id.*

470. *Latin America and Caribbean: Statistical Profile*, NATION MASTER, https://www.nationmaster.com/country-info/groups/Latin-America-and-Caribbean [https://perma.cc/633R-LPUN].

471. Joseph Mazzella, *Colombia: Is a Data Protection Officer Required for Compliance?*, IAPP, https://iapp.org/news/a/colombia-is-a-data-protection-officer-required-for-compliance/ [https://perma.cc/KD5B-6KXM].

472. *Id.*

473. Alec Christie et al., *Uruguay: Data Protection Laws of the World Handbook: Second Edition - Uruguay*, MONDAQ (Apr. 12, 2013), http://www.mondaq.com/Uruguay/x/231656/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Uruguay [https://perma.cc/J443-6ZD4].

474. *Id.*

> set forth an interpretation of Articles 28 (right to access official records) and 60 (right to the protection of privacy) of the Constitution. This leading decision (a) determined the privileged information that is protected under constitutional standards; and (b) established a habeas data process and the information that may be subject to such process.[475]

Governments in several countries in the region have been accused of using malware to spy on their citizens.[476]

10. Data Privacy in the Caribbean

The Caribbean "functions as a hub for the global financial industry, with citizens from all over the world investing and moving their money throughout the region."[477] The Caribbean Hotel and Tourism Association (CHTA) is emphasizing the importance of GDPR compliance because large numbers of EU consumers vacation in the region.[478] "Businesses throughout the Caribbean have paid very little notice to the GDPR, with few aware of the implications the new regulations may have on their organisation."[479]

> Additionally, the data subject must be informed of the purpose of the transfer, as well as of the identity of the recipient.
>
> However, the prior consent of the data subject is not necessarily required when the personal data to be transferred is limited to: name, surname, identity card number, nationality, address, and date of birth.

Id.

475. *Data Protection Enforcement in Venezuela*, GLOBAL COMPLIANCE NEWS, https://globalcompliancenews.com/data-privacy/data-protection-enforcement-in-venezuela/ [https://perma.cc/LSE4-CMP6] (describing the core principles of Venezuelan data protection law).

476. Daniel Álvarez Valenzuela & Francisco Vera Hott, *Cybersecurity and Human Rights in Latin America*, *in* TOWARDS AN INTERNET FREE OF CENSORSHIP II, *supra* note 388, at 31, 52 (footnotes omitted) ("As to the use of malware, some reports issued by Citizen Lab from the University of Toronto and by Derechos Digitales NGO, reveal that several States in the region (Chile, Ecuador, Paraguay, Venezuela, Mexico, Honduras, Colombia and Brazil) have acquired platforms from two companies (Hackin Team and Gamma Group), that are able to infiltrate malware into the digital devices of certain people to spy on the devices and the information captured by them.").

477. *How the GDPR Will Affect Organisations in the Caribbean*, CLOUD CARIB: BLOG, https://info.cloudcarib.com/blog/how-the-gdpr-will-affect-organisations-in-the-caribbean [https://perma.cc/4MJ9-KBZS].

478. *Id.*

479. *Id.*

B. *The Evidence for an Emerging Global Data Privacy Standard*

Our global data privacy survey reveals the rise of a GDPR-inspired privacy standard that is harmonizing data control practices in democratic-industrial countries, often described as the "First World." The GDPR is in effect in all twenty-eight countries of the European Union and the three EFTA countries.[480] This includes many of the former communist-socialist states—the "Second World" of developed nations.[481] North America is largely GDPR compliant, as is Japan.[482] Australia is bringing its data protection laws into alignment with the GDPR.

"Third World" countries generally have non-existent or weak data protection laws.[483] "The term Third World includes [] capitalist (e.g., Venezuela) and communist (e.g., North Korea) countries, as [well as] very rich (e.g., Saudi Arabia) and very poor (e.g., Mali) countries."[484]

The countries least involved in the world economy are unlikely to become GDPR compliant in the near future because they offer few goods or services to Europe or the United States.[485] "What is clear is that the World Wide Web is becoming more segmented, with different rules in different countries and regions that go far beyond the Chinese firewall or

480. *See supra* Section IV.A.5.

481. Bulgaria, Croatia, Czech Republic, Estonia, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia are members of the EU, where the GDPR is now in effect. *EU Member Countries in Brief*, EUR. UNION, https://europa.eu/european-union/about-eu/countries/member-countries_en [https://perma.cc/DA35-L6VT] (last updated Sept. 19, 2018).

482. "The term 'First World' refers to so called developed, capitalist, industrial countries, roughly, a bloc of countries aligned with the United States after World War II, with more or less common political and economic interests: North America, Western Europe, Japan and Australia." *First, Second and Third World*, ONE WORLD NATIONS ONLINE, http://www.nationsonline.org/oneworld/third_world_countries.htm [https://perma.cc/B3FU-AH57].

483. "The least developed countries (LDCs) are a group of countries that have been classified by the UN as 'least developed' in terms of their low gross national income (GNI), their weak human assets and their high degree of economic vulnerability." *See Least Developed Countries (LDCs)*, *supra* note 387. Less developed countries will generally have: (1) "Low-income criterion based on a three-year average estimate of the gross national income (GNI) per capita (under $750 for inclusion, above $900 for graduation)", (2) "Human resource weakness criterion involving a composite Human Assets Index (HAI) based on indicators of: (a) nutrition; (b) health; (c) education; and (d) adult literacy," and (3) "Economic vulnerability criterion based on indicators of the instability of agricultural production; the instability of exports of goods and services; the economic importance of non-traditional activities (share of manufacturing and modern services in GDP); merchandise export concentration; and the handicap of economic smallness." *Id.*

484. *First, Second and Third World*, *supra* note 482.

485. "Third World Countries classified by various indices: their Political Rights and Civil Liberties, the Gross National Income (GNI) and Poverty of countries, the Human Development of countries (HDI), and the Freedom of Information within a country." *Id.*

Iranian Internet isolation."[486] As a result, most of the world's least developed countries either have no data protection or have segmented data privacy rules unaligned with the synthesis of U.S. and EU data privacy law.

The evolving U.S. and EU hybrid global data standard is dual public-private enforcement. The vast majority of developed countries recognize the concept of data subject consent, and many countries specify even greater protections for sensitive data. Advanced countries generally provide data subjects with a mechanism for correcting or rectifying incorrect information. Countries are increasingly enacting statutory remedies such as wealth-based fines to deter organizations from misusing personal information. Wealth-based fines make even the most powerful company think twice before violating data subjects' privacy rights.

The emergent standard holds data processors responsible for ensuring data protection when collecting and processing personally identifiable data. Many developed countries use data protection supervisors, or their equivalent, to ensure compliance.[487] Data minimization obligations are widely recognized. This standard requires organizations to limit the use, retention, and disclosure of personal information to relevant purposes.

Google has voiced concern that the "right to be forgotten" (RTBF) is spreading from "Europe to other areas of the world."[488] The authors' survey of global data privacy developments found evidence that the RTBF is being adopted by countries outside of Europe, although the rate of acceptance is lower than that of other GDPR data subject rights. The Australian Law Reform Commission, for example, decided not to adopt this doctrine,[489] and American legal experts often reject it as a violation of the First Amendment. However, a recent study of U.S. privacy decisions found "a surprising number of modern cases from United States

---

486. Dan Lohrmann, *GDPR in the USA*: *What's Next?*, LOHRMANN ON CYBERSECURITY & INFRASTRUCTURE (May 27, 2018), http://www.govtech.com/blogs/lohrmann-on-cybersecurity/gdpr-in-the-usa-whats-next.html [https://perma.cc/5V84-DC8M].

487. *See* GDPR, *supra* note 4, art. 56(1), at 67.

488. Wendy Davis, *Google Warns Against Possible Expansion of "Right to Be Forgotten*," POL'Y BLOG (July 26, 2018), https://www.mediapost.com/publications/article/322815/google-warns-against-possible-expansion-of-right.html?edition=110222 [https://perma.cc/VS2N-JQ94] ("Google now says it's worried that the right to be forgotten could expand beyond the EU. 'We have done our best to comply responsibly, but we disagreed with the ruling in Europe and would have concerns about this principle being exported to other jurisdictions,' Google said in a recent filing . . . with the National Telecommunications and Information Administration.").

489. Angela Lavoipierre & Stephen Smiley, *The Nightmare of Mopping up Your Online Reputation and the "Right to be Forgotten*," ABC NEWS (July 23, 2018, 10:56 PM), https://www.abc.net.au/news/2018-07-24/the-nightmare-of-mopping-up-your-online-reputation/10027170 [https://perma.cc/UJ5S-GJFU] ("[T]he Australian Law Reform Commission had previously considered whether to recommend the introduction of a 'right to be forgotten' in Australia and decided against it.").

courts, including the nation's highest court, that support the idea that a [RTBF] exists on U.S. shores."[490]

U.S. courts are increasingly predisposed to removing posted information.[491] Professor Amy Gajda argues "that the [RTBF] must be cabined by presuming newsworthiness, a word defined in journalism's ethics codes in a way that parallels at least in some part the legal standard. Without such limitation, any [RTBF] will significantly erode freedom of the press."[492]

The right to be forgotten may yet achieve global acceptance. In 2017, the Karnataka High Court in India:

> passed a landmark order while hearing a writ petition, wherein the Court Registry was directed to ensure that an internet search made in the public domain would not bring up the applicant's name in a previous criminal order passed by the same High Court. The High Court observed . . . 'This is in line with the trend in western countries of "right to be forgotten" in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.' Internet footprints are all pervasive, and removal of content from the internet is often a technical impossibility.[493]

Nevertheless, the High Court's landmark approach suggests that the Indian judicial system is sympathetic to efforts "to recognise and assist in the upholding of an individual's right to privacy."[494]

The expression "right to be forgotten" also appeared in a 1992 court ruling in Colombia.[495] A 2017 report on freedom of expression by a team

---

490. Amy Gajda, *Privacy, Press, and the Right to Be Forgotten in the United States*, 93 WASH. L. REV. 201, 204 (2018).

491. *Id.*

492. *Id.*; *cf.* Julian Hattem, *Should the U.S. Have "Right to Be Forgotten?,"* HILL (May 15, 2014, 6:00 AM), https://thehill.com/policy/technology/206169-should-us-have-right-to-be-forgotten [https://perma.cc/Z5HR-P6QG] ("A U.S. version of what Europeans call the 'right to be forgotten' seems impossible in this country . . . ."); David Rodin, *There Is No "Right to Be Forgotten,"* HUFFINGTON POST (Feb. 10, 2015, 2:39 PM), https://www.huffingtonpost.com/david-rodin/there-is-no-right-to-be-f_b_6645776.html [https://perma.cc/DX3P-RR9Z] ("[T]here is no right to be forgotten. There is not even a right to be remembered fairly.").

493. Sugandha Kaur Borthakur & Sandeepan Borthakur, *Right to Be Forgotten: The Way Forward*, ASSAM TRIB., Feb. 28, 2017, at 6.

494. *Id.*

495.

> For a long time, the concept referred to the situation of people reported as debtors, people in arrears or individuals who had committed a crime. During the XX century, the subject was studied under the framework of the right to

of Latin American scholars urged the Latin American governments to consider the applicability of the European Union's right to be forgotten and recommended:

> (1) [that] governments in the Americas face these questions head-on; (2) that courts and authorities throughout the hemisphere work to apply the existing and hard-fought inter-American standards protecting the freedom of expression; (3) that a transatlantic dialogue be initiated to discuss the right to be forgotten online; and (4) that governments search for alternative legal and technological mechanisms to protect privacy so as to limit the tensions while taking into account the very real concerns that the right to be forgotten attempts to address.[496]

In short, this international survey confirms considerable movement toward a data protection consensus among the "First World" nations and many of their principal trading partners. The multinational effort to achieve GDPR compliance has the potential to create the basis for a truly global data privacy regime.

CONCLUSION

As technological advances enable the harvesting of ever larger quantities of personal data, sophisticated controls on the collecting, processing, and transfer of big data have become increasingly necessary. The GDPR was enacted to protect the personal privacy of EU residents against the threat posed by the collectors and disseminators of large-scale analytics.[497] In July 2018, the European Parliament passed a non-binding resolution to suspend the EU-U.S. Privacy Shield that permits U.S.

> information, reputation and human dignity in relation to individuals, credit risk entities and the State.
>
> Nonetheless, the debate in the early XXI century was enriched with new elements and circumstances. On the one hand, elements as Internet and freedom of expression were added.

Nelson Remolina Angarita, *Right to Be Forgotten in Cyberspace? International Principles and Considerations About Latin American Regulations*, *in* TOWARDS AN INTERNET FREE OF CENSORSHIP II, *supra* note 388, at 175, 175.

496. *Brief: Freedom of Expression—Paper Looks at 'Right to Be Forgotten' in Latin American Context*, INTELL. PROP. WATCH (Nov. 15, 2017), http://www.ip-watch.org/2017/11/15/freedom-expression-paper-looks-right-forgotten-latin-american-context/ [https://perma.cc/AGN7-PLZ9].

497. *See supra* note 58 and accompanying text.

organizations to transfer data between the world's two largest trading blocs.[498]

The Trump Administration is resisting EU pressure to enact policies that conform to the GDPR's privacy rules, viewing these European actions as unilateral impositions of foreign mandates on American corporations.[499] President Donald Trump's revised policies may make the compromise of data privacy solutions more difficult to achieve. Trump's FTC opposes the recognition of the right to be forgotten.[500] Nevertheless, even if the federal government weakens consumer privacy laws, the convergence between U.S. and EU law has a high probability of evolving over time into a global solution to divergent national privacy laws.

This Article has countered the Trump Administration's misperception, using empirical evidence demonstrate that the GDPR is actually a legal hybrid that borrows heavily from long established U.S. legal doctrine. Commentators who typecast the divide between the European Union and the United States as reflecting diametrically opposed legal approaches fail to recognize that convergent forces are harmonizing EU and U.S. data protection law. The extraterritorial impact of the GDPR is unlikely to lead to an all-out Transatlantic Data War because much of the GDPR originated in U.S. law and is clearly compatible with long-standing American privacy norms and remedies.

Most multinational private and public entities stand to benefit greatly from the efficiencies created by a globalized privacy protection policy. Without a unified data control standard, there is the specter of multiple cyberspace Checkpoint Charlies that could fragment the Internet into an inefficient "splinternet." In the past several months, major U.S. information companies have pledged to comply with the GDPR and, in some cases, extend the Resolution's protections to citizens around the world. The authors' global survey shows that at least twenty countries are currently updating their privacy laws to become GDPR compliant.

Many difficulties remain to be overcome, but the GDPR is rapidly evolving into the transnational gold standard of data protection, applicable to all domestic and cross-border transfers of personally identifiable data. The GDPR, as a bilateral synthesis of U.S. and EU privacy law, provides an important step toward the development of an international data control policy for the age of the Internet.

---

498. *See supra* note 208 and accompanying text.

499. *See supra* note 22 and accompanying text.

500. *FTC Commissioners Wary of Right to Be Forgotten*, TR DAILY (Sept. 18, 2015), 2015 WLNR 27832249 ("FTC Commissioners Terrell McSweeny, a Democrat, and Maureen Ohlhausen, a Republican, said they were both wary of any move in the U.S. toward 'right to be forgotten' rules that the European Union has embraced for online content, saying that the strong U.S. reliance on the First Amendment would make such rules unworkable.").