Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Indiana Law Journal

Volume 94 | Issue 1 Article 7

Winter 2019

Data Protection in an Increasingly Globalized World

Nicholas F. Palmieri III
Maurer School of Law - Indiana University, nicpalmi@iu.edu

DATA PROTECTION IN AN INCREASINGLY GLOBALIZED WORLD

NICHOLAS F. PALMIERI III*

INTRODUCTION

With the rise of the internet in recent decades, it has become increasingly easy for various enterprises—including retailers, advertising agencies, and service providers—to acquire, use, and even share the personal details of their users.[1] Such a trend is unlikely to decrease in the coming years; in fact, internet usage is only likely to increase as more and more people gain access to the internet.[2] In the wake

---

* J.D. Candidate, 2019, Indiana University Maurer School of Law.

1. *See, e.g.*, Aaron Brown, *The Amount of Data Facebook Collects from Your Photos Will TERRIFY You*, EXPRESS (Jan. 6, 2017, 12:12 PM), https://www.express.co.uk/life-style/science-technology/751009/Facebook-Scan-Photos-Data-Collection [https://perma.cc/NF5F-F5K9]; Todd Haselton, *How To Find Out What Google Knows About You and Limit the Data It Collects*, CNBC (Nov. 20, 2017, 11:50 AM), https://www.cnbc.com/2017/11/20/what-does-google-know-about-me.html [https://perma.cc/K3SQ-STM2]; 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/KQG8-WH8J]; Matt Smith, *How Much Does Google Really Know About You?*, MAKEUSEOF (June 17, 2014), https://www.makeuseof.com/tag/how-much-google-know-about-you/ [https://perma.cc/X8F3-HJPD].

2. *See generally* CHINA INTERNET NETWORK INFO. CTR., STATISTICAL REPORT ON INTERNET DEVELOPMENT IN CHINA (2017) (examining internet usage and access trends in the United States, the European Union, and China, respectively); *Internet Access and Use Statistics - Households and Individuals*, EUROSTAT (Jan. 30, 2017, 2:49 PM), http://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Internet_access_and_use_statistics_-_households_and_individuals [https://perma.cc/3BSZ-VCV4]; *Internet/Broadband Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/internet-broadband/ [https://perma.cc/GP3J-XZ9R].

of recent data breaches, including the now infamous breach of Equifax[3] as well as the scandal involving Facebook and Cambridge Analytica,[4] people are even more aware of the need for (and the risk of not having) adequate data protection laws. Luckily though, in the last few years there have been serious pushes across the globe to institute new data protection laws[5] that ensure private data is not used for nefarious purposes or given away frivolously.

This Note intends to outline the current data protection regimes in three large jurisdictions across the globe (the European Union, China, and the United States), to offer insight into the strengths and weaknesses of each regime, and to predict the path that data protection laws in the United States should take in upcoming years. As will be seen, both the European Union and China, with the institution of their newest data protection laws, use omnibus regimes, in contrast with the United States' current sector specific regime.[6] The United States should move from its current regime, in which there are only national laws for specific industries,[7] to a more omnibus regime, taking elements from both the European and the Chinese data protection regimes, which will help provide a minimum floor of protection applicable to all citizens whose personal data is being processed rather than allowing for varying levels of protection between states and industries.

I. A FRAMEWORK FOR DATA PROTECTION LAWS

Before being able to properly analyze the data protection laws of the jurisdictions mentioned above, it is important to first create a framework against which to analyze those regimes. For this purpose, this Note will adapt a five-element framework put forth by Professor Fred H. Cate.[8] Instead of using those five elements, which are

---

3. *See* AnnaMaria Andriotis, Michael Rapoport & Robert McMillan, *'We've Been Breached': Inside the Equifax Hack*, WALL ST. J. (Sept. 18, 2017, 8:04 AM), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318 [https://perma.cc/5THE-4R22]; Ron Lieber, *How To Protect Yourself After the Equifax Breach*, N.Y. TIMES (Oct. 16, 2017), https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html?_r=0 [https://perma.cc/4638-EPHR].

4. *See generally* Nellie Bowles, *After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So,'* N.Y. TIMES (Apr. 12, 2018), https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html [https://perma.cc/CE2V-SSU5]; Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/VE7R-3S76].

5. Such a push may not actually be a very new idea, but recent legislation certainly points to an increased push for data protection guaranteed by national (and sometimes international) law. *See* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 51 [hereinafter Treaty of Lisbon] (declaring in Article 16 B that "[e]veryone has the right to the protection of personal data concerning them").

6. *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 15–30 (2015).

7. *See, e.g.*, 5 U.S.C. § 552a (2012 & Supp. II 2015); Children's Internet Protection Act, Pub. L. No. 106-554, tit. XVII, 114 Stat. 2763, 2763A-335 to -352 (2000); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

8. Fred H. Cate, *Big Data, Consent, and the Future of Data Protection*, *in* BIG DATA IS

intended for use in the management of big data,[9] this Note will use a modified three-factor framework intended to apply to all instances of data processing and collection, not just those which can be classified as big data. The three elements of this framework consist of: (1) data stewardship, (2) a balance between harms and benefits, and (3) a system of transparency and redress. Individually, each element covers a different aspect of data processing. Data stewardship involves the proper collection and storage of personal data.[10] The balance between harms and benefits covers what a data processor can (and should) do once they have received personal data.[11] Finally, having a system of transparency and redress ensures that data subjects themselves can properly monitor their own data and have ways of ensuring that data processors are not violating anyone's rights and causing harm.[12]

A. Data Stewardship

Individual consent to the use of personal data by various websites and companies has, for a long time, been standard practice.[13] Consent to a website's "privacy policy" is often done automatically, with consumers assuming that a website will, naturally, "follow[] fair information practice principles."[14] Yet in reality, such consent is rarely truly informed or adequate,[15] usually for two reasons. First is the existence of a

---

NOT A MONOLITH 3 (Cassidy R. Sugimoto, Hamid R. Ekbia & Michael Mattioli eds., 2016). Professor Cate's frameworkes specifically on the management of Big Data, with the framework consisting of: (1) a focus on data stewardship, *id.* at 12; (2) a system of risk management, *id.*; (3) an increased focus on data uses, *id.* at 14; (4) a framework of harms, *id.* at 16; and (5) transparency and redress, *id.* at 17.

9. The Federal Trade Commission (FTC) defines big data as "a confluence of factors," including the collection of data from various sources, the plethora of available data storage mediums for low costs, and the presence of immense computing power to analyze that data and draw conclusions from it. EDITH RAMIREZ, JULIE BRILL, MAUREEN K. OHLHAUSEN & TERRELL MCSWEENY, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 1 (2016). Three characteristics (called the "three Vs") used to identify big data are volume (the sheer amount of data being analyzed), velocity (the speed at which a company can collect and analyze the data), and variety (referring to the variety, or "breadth," of data being collected). *Id.* at 1–2.

10. *See* Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 47–49 (2013).

11. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1890–92 (2013) (discussing how the harms and benefits of giving up personal data can change depending on the time, place, reason, etc. surrounding the use).

12. *See* Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365, 375 (2013).

13. *See* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 43–46 (2015) (discussing the "notice and choice" standard that has existed in the United States since the 1970s).

14. Patrick F. Gallagher, *The Internet Website Privacy Policy: A Complete Misnomer?*, 35 SUFFOLK U. L. REV. 373, 380 (2001); *see also* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 15 (2012).

15. *See* Thomas B. Norton, Note, *The Non-Contractual Nature of Privacy Policies and a*

"knowledge gap" between the consumer and the data processor.[16] The average consumer rarely knows, or even considers, the uses to which their personal data will be put,[17] whether it be due to the complexity of the terms, ignorance of the existence of the privacy policies, or simply an inability to process these lengthy notices.[18] The second failing of individual consent, as explained by Professor Paul Schwartz, is the so-called "consent fallacy,"[19] where individuals may not truly have a choice in whether or not to consent because they are seeking to use a necessary service or they fear reprisals of some sort.[20]

So rather than allowing companies to rely on the consent of individual data subjects, data protection laws should seek to require proper data stewardship by companies, allowing the data subjects to rely on companies to use personal data responsibly.[21] Thus the law should incentivize companies to look for and protect personal data from foreseeable harms so that individuals can feel safer in allowing personal data onto the internet or to be collected by various companies.[22] The exact structure of such incentives has not been codified, but several commenters have laid out potential solutions. For example, Professor Andrea Matwyshyn has laid out a data stewardship model that has been informed by and built from contract and trade law.[23] That model incorporates personal data use as part of a contract between the

---

New Critique of the Notice and Choice Privacy Protection Model, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 201 (2016); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 140–48 (2014). *But see* Pharmatrak, Inc. Privacy Litig. v. Pharmatrak, Inc., 329 F.3d 9, 19–21 (1st Cir. 2003) (suggesting that even cursory consent to an online privacy agreement is adequate in many, but not all, circumstances).

16. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1683–84 (1999).

17. *Id.*; *see also* Amanda Grannis, *You Didn't Even Notice! Elements of Effective Online Privacy Policies*, 42 FORDHAM URB. L.J. 1109, 1147–48 (2015); Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 133–37 (2003).

18. *See* Cate, *supra* note 8, at 6–8; Peppet, *supra* note 15, at 144–46 (discussing the weaknesses of privacy policies related to use of objects connected to the "Internet of Things"); Reidenberg et al., *supra* note 13, at 47–48; Solove, *supra* note 11, at 1884.

19. Schwartz, *supra* note 16, at 1684; *see also* George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 33–34 (2016).

20. Schwartz, *supra* note 16, at 1684; *see* Article 29 Data Protection Working Party, *Opinion 2/2017 on Data Processing at Work*, 17/EN WP 249 (June 8, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=45631 [https://perma.cc/95GQ-NZS3] [hereinafter DPWP] (recognizing that forcing employees to consent to broad uses of their personal data is not really voluntary consent).

21. *See* Cate, *supra* note 8, at 12; *see also* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 55–56 (2014) [hereinafter WHITE HOUSE BIG DATA REPORT].

22. Cate, *supra* note 8; *see also* Ashenmacher, *supra* note 19, 44–55 (discussing why it is so important to identify harms caused by breaches of personal data).

23. Matwyshyn, *supra* note 10. Professor Matwyshyn is not the only one who has identified parallels between data protection and contract law. *See, e.g.*, Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now Is the Time*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 22–23 (2009) (discussing why contract law is related to but falls short of

company and the consumers, which in turn would create "a new statutorily implied warranty of 'digital usability and quiet enjoyment.'"[24]

Another alternative, offered by Professor Jeff Kosseff, is the creation of various tax incentives for companies to properly invest in and maintain cybersecurity infrastructure.[25] In this case, rather than retroactively punishing companies for not properly protecting personal data, companies are proactively encouraged to establish adequate security measures with the knowledge that they can receive certain tax breaks or other benefits in return.[26]

In addition to incentivizing data processors to properly protect data, data protection laws should also provide guidance towards the proper use of personal data. The use of data in different contexts can often result in different levels of risk.[27] By providing some guidance as to how personal data should be used,[28] data protection laws can further push responsibility of data protection to the companies that collected the data rather than to the consumer whose data is being collected.[29] But it is important to note that just because the focus is shifted to use of collected data does not mean that there should be no regulations or responsibilities associated with data collection. Instead, businesses using personal data should focus on the risks or benefits associated with a particular use and should not just rely on the terms of collection of that data.[30] This element would help to eliminate the need for lengthy privacy policy notices and prevent businesses from simply putting consumers on notice of a broad, boilerplate list of *possible* uses of their data that a user must accept in order to use the product or service offered.[31]

---

providing for proper data protection); Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 855–57 (2005); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1057–63 (2000). *But see* Norton, *supra* note 15.

24. Matwyshyn, *supra* note 10, at 48.

25. Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 415–16 (2016).

26. *Id.*

27. *See* Cate, *supra* note 8, at 15 (discussing the use of personal data in the context of big data); WHITE HOUSE BIG DATA REPORT, *supra* note 21, at 49–51.

28. A complete enumeration of allowable uses would be almost impossible due to both the varying nature of personal data itself as well as the needs of various industries that would be using the personal data. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 7–9 (2014).

29. With these two elements in place, legal focus will not even start in earnest until the companies have collected the data (since they will be required to properly protect that data) and begin to use that data (as a result of the greater focus on uses rather than collection of data).

30. Cate, *supra* note 8, at 15.

31. *See* Schwartz, *supra* note 16, at 1685 (describing user acceptance of privacy statements as a "hollow ritual" of consent to access various content).

B. A Balance Between Harms and Benefits

Before a company can properly minimize the risk of harms from improper treatment of data (and before a consumer can properly consent to giving their information in light of those risks), the company must understand and identify those potential harms.[32] Commentators have identified various potential harms, but there has been little concerted effort to enumerate the harms resulting from the misuse of personal data.[33] While it is important to include a broad spectrum of possible harms,[34] including both tangible and intangible injuries, the real benefit of codifying specific harms is that it gives notice to consumers, who now understand what harms could result from giving up their personal data, and businesses, who must analyze those harms to determine how much risk they pose and determine if they wish to pursue the data processing.[35]

While it is important for data protection laws to enumerate broad potential harms and to recognize that "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions,"[36] it is also important for governments not to be overbroad in their classification of potential harms.[37] Laws that are too broad risk alienating both potential businesses (who will be unwilling to bear the burden of those potential harms)[38] and potential consumers (who are unwilling to submit their information to the risk of those potential harms). So, any

---

32. Cate, *supra* note 8, at 16.

33. *See, e.g.*, LYNSKEY, *supra* note 6, at 77 (recognizing a tangible harm (discrimination) and an intangible harm (the feeling of helplessness) that can result from misuse of personal data); Gallagher, *supra* note 14, at 385 (citing reputation harm as one potential harm of misuse of personal data); Scott J. Shackelford, Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna Gjonaj & Rachith Kavi, *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 440–41 (2017) (referencing a "myriad of ways" consumers can be harmed, including bad credit ratings); *see also* MARIA TZANOU, THE FUNDAMENTAL RIGHT TO DATA PROTECTION 21–24 (2017) (implicating the right of privacy as under threat from an abuse of personal data).

34. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 10–11 (2008) (creating sixteen categories of processing activities that can result in harm to individuals).

35. Cate, *supra* note 8, at 17; *see, e.g.*, WHITE HOUSE, *supra* note 14, at 19–21; Peltz-Steele, *supra* note 12, at 408; Schwartz, *supra* note 16, at 1645–47.

36. FED. TRADE COMM'N, *supra* note 28, at 8; *see also* WHITE HOUSE BIG DATA REPORT, *supra* note 21, at 51–53 (acknowledging that harms can range from tangible to intangible as well as affect both individuals and groups).

37. *See Dissenting Statement of Commissioner Orson Swindle*, *in* PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE; A REPORT TO CONGRESS 57 (2000) (criticizing the FTC's recommendation for "breathtakingly broad" legislation directed towards consumer-oriented websites).

38. *See, e.g.*, Manu J. Sebastian, *The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises?*, 31 SYRACUSE J. SCI. & TECH. L. 216, 235 (2015) (explaining one potential risk of overbroad data privacy laws: forcing enterprises to store all data pertaining to a certain subject or risk being unable to combat any legal action taken against them).

data privacy regime must carefully consider what effects, both social and economic, inclusion of particular harms would cause.[39]

But identifying only the potential harms of various processing activities leaves out another vital part of personal data processing—the benefits to be achieved by that processing.[40] As discussed earlier, vital to any proper data protection regime is the ability to contemplate and identify as many risks of a particular activity as possible, with the goal of reducing those risks and increasing "predictability, consistency, and efficiency in data protection."[41] But beyond just identifying the risks encompassed by a particular activity, data protection laws (and data processors in general) must be able to balance those risks against the benefits the activity may produce. For certain activities, the benefits of data processing can sometimes outweigh the risks posed by that processing.[42]

By creating a system that includes both risks and benefits in any overarching laws regarding data protection, governments will preempt varying interpretations by various companies and allow for consumers to properly set their expectations.[43] Naturally, any system of risk management will become a balancing act between the benefits and risks of any particular activity, which could lead to seemingly arbitrary distinctions between activity that is deemed beneficial enough to proceed as opposed to activity that is too risky to proceed.[44] However, by using a national law to inform companies and consumers about what risks are acceptable (and to what degree) nations will, at the very least, allow companies to properly tailor their behavior to fall within the confines of the law and allow consumers to have confidence that they know the uses to which their data will be put.[45] Additionally, such an approach allows

---

39. *See* CTR. FOR INFO. POLICY LEADERSHIP, THE ROLE OF RISK MANAGEMENT IN DATA PROTECTION 25 (2014) (quoting Jennifer Stoddart, *Auditing Privacy Impact Assessments: The Canadian Experience*, *in* PRIVACY IMPACT ASSESSMENT 430 (David Wright & Paul De Hert eds., 2012)) (discussing the use of social and economic analyses to develop programs and services to maximize the integration of risk management practices); DPWP, *supra* note 20, at 9–10 (discussing the balance between increased employee efficiency, protection of company assets, and collection of personal data); SIMON HEAD, THE RUTHLESS ECONOMY: WORK AND POWER IN THE DIGITAL AGE 100 (2005) (describing the "hyperefficiency" caused by "analysis, surveillance[,] and control"); *see also* LYNSKEY, *supra* note 6, at 79–81 (discussing economic factors and social factors as driving forces behind data protection regulation).

40. *See, e.g.*, HEAD, *supra* note 39, at 100; LYNSKEY, *supra* note 6, at 80.

41. *See* Cate, *supra* note 8, at 12–13; *cf.* CYNTHIA R. FARINA, SIDNEY A. SHAPIRO & THOMAS M. SUSMAN, ADMINISTRATIVE LAW OF THE EUROPEAN UNION: TRANSPARENCY AND DATA PROTECTION 139–41 (George A. Berman, Charles H. Koch, Jr. & James T. O'Reilly eds., 2008).

42. *See* McClurg, *supra* note 17, at 72–74 (discussing the "important benefits "on both individuals and society" that data collection and use can confer).

43. *See* CTR. FOR INFO. POLICY LEADERSHIP, *supra* note 39, at 13.

44. *Cf.* K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 11 n.28 (2003) (discussing "arbitrary distinctions" with permissible data uses based on whom the data relates or where the data was collected).

45. *See* CTR. FOR INFO. POLICY LEADERSHIP, A RISK-BASED APPROACH TO PRIVACY: IMPROVING EFFECTIVENESS IN PRACTICE 8–9 (2014) (suggesting a balance between likelihood of harm and severity of harm, which takes into account the risk aversion of various different

for governments to consolidate and resolve the "largely ad hoc, colloquial terms" that have developed around data protection to this day.[46] By establishing a proper system to balance the harms against the benefits of processing and allowing enterprises to perform even risky processing if it results in enough of a benefit, governments will be able to strike a balance between the protection of personal data and the well-being of society as a whole.[47]

C. Transparency and Redress

Despite the existence of various laws to incentivize proper data protection, it is almost inevitable that mistakes and data breaches will happen.[48] Therefore, data protection laws must have in place requirements not only for consumers to see what a business is doing with the personal data (transparency)[49] but also ways to effectively respond and correct them (redress).[50]

Transparency should allow for consumers not only to see what businesses are using their personal data for, but also give consumers the chance to correct any incorrect personal data.[51] In this way, consumers can retain confidence and trust that their personal data is not only being used appropriately but also that the data they have given is as accurate as possible.[52] While transparent behavior by businesses

---

kinds of businesses).

46. Cate, *supra* note 8, at 13; *see also* FED. TRADE COMM'N, *supra* note 28, at 38–39 (explaining that while a risk management standard should be "flexible," it must also provide businesses with "more concrete guidance").

47. *See* Ryan Moshell, *. . . And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH. L. REV. 357, 375–76 (2005) (showing how the Freedom of Information Act, 5 U.S.C.A. § 552 (2000), balances between the public's right of access and a data subject's right of privacy); Peltz-Steele, *supra* note 12, at 379–83 (briefly discussing the safeguards contained in European legislation designed to preserve freedom of expression); Scott J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures*, 49 AM. BUS. L.J. 125, 131 (2012) (comparing the balance between freedom of expression and personal privacy in several jurisdictions around the world).

48. Cate, *supra* note 8, at 18.

49. *See* Alan Toy, *Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy*, 25 N.Z.U. L. Rev. 938, 948 (2013) (defining transparency as the ability of consumers to see what a business does with disclosed personal data); *see also* FARINA, *supra* note 41, at 1–9 (discussing transparency as a citizen's ability both to gain access to information about "structure and function" of the government as well as access to documents "produced and accumulated" by the government).

50. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 11 (1998) [hereinafter FTC REPORT 1998] (suggesting that redress remedies should include both "right of the wrong" and "compensation for any harm suffered").

51. *See* Privacy Act of 1974, 5 U.S.C. § 552a (2012 & Supp. II 2015) (expressly allowing individuals the right to access and correct personal data in the context of data gathering by the U.S. government); Council Directive 95/46, 1995 O.J. (L 281) 31, 33 (EC) [hereinafter The 1995 Directive] (allowing individuals to request corrections and object to processing of personal data).

52. Such accuracy is especially important where information is being used for national security or criminal investigation purposes, since inaccurate information might not only open

allows for consumers to pick and choose which businesses to frequent,[53] transparency in and of itself is not enough to ensure proper regulation.[54] Regulation also needs a means of redress to be effective.[55]

With regard to redress, one of the first responses by any business is often sending notification to consumers that a breach of personal data has occurred.[56] In fact, such a requirement is already in effect in many places.[57] But just notifying consumers that a breach has occurred does little to help them—it essentially shifts the burden of caring for personal data back to the consumers and away from the businesses, which is counter to the data stewardship element discussed earlier.[58] A proper data protection regime must outline and address specific remedies available.[59] In this way,

---

up an individual to reprisals or investigation by government authorities but might also waste government resources tracking and investigating individuals who pose no threat (or even risk) to national security. *See* NAT'L AUDIT OFFICE, EFFICIENCY IN THE CRIMINAL JUSTICE SYSTEM, 2015–16, HC 852, at 19 (UK) (discussing the cost of investigations and hearings which end up being dropped); TRANSUNION, IMPROVING INVESTIGATION TECHNIQUES AND SAVING TIME USING ONLINE RESOURCES (2015) (discussing the importance of accurate information in any investigation); *see also* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 543 (2016) (discussing the tendency for groups to assume that any information stored within a database is accurate).

53. Users will be able to make informed decisions using information about the uses to which their personal data will be put, which helps to decrease the knowledge gap between consumers and businesses. *See* Schwartz, *supra* note 16, at 1683–84.

54. *See* Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES IN BUILDING GOVERNANCE MECHANISMS 105, 120 (Eric Brousseau, Tom Dedeurwaerdere, Pierre-André Jouvet & Marc Willinger eds., 2012) (discussing the shortcomings of allowing consumer "trust" to regulate certain resource regimes and suggesting that at least some monitoring, *ex ante*, is required to keep rule-breaking to a minimum).

55. FTC REPORT 1998, *supra* note 50, at 10 (stating that redress is a requirement for privacy protection regulations to be effective).

56. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2007); Alan Wehbé, *OPM Data Breach Case Study: Mitigating Personnel Cybersecurity Risk*, 26 B.U. PUB. INT. L.J. 75, 92 (2017). *But see* Editorial, *Have You Been Stolen?*, WASH. POST (June 30, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/06/29/AR2005062902576.html [https://perma.cc/THB2-WWEL] (criticizing the overabundance of breach notifications).

57. Shackelford et al., *supra* note 33, at 449 ("As of 2016, forty-seven states had data-breach-notification laws."); *Security Breach Notification Laws*, NAT'L CONFERENCE ST. LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/SG4F-Z38V] (explaining that as of 2018, all fifty states had data-breach-notification laws); The 1995 Directive, *supra* note 51, arts. 18–19 (obligating Member States to notify the supervisory authority, but not the consumers whose personal data was breached).

58. *See supra* Section I.A.

59. *Cf.* Steven M. LoCascio, *Forcing Europe To Wear the Rose-Colored Google Glass: The "Right to be Forgotten" and the Struggle to Manage Compliance Post* Google Spain, 54 COLUM. J. TRANSNAT'L L. 296 (2015) (suggesting an administrative and legal framework for enforcing a "Right to Be Forgotten" online, by analyzing privacy laws and enforcement in Europe and the United States).

enterprises are incentivized not only to protect personal data before a breach, but also to correct any breaches that occur and ensure that such breaches do not occur in the future.[60]

II. JURISDICTIONAL APPLICATION

This Part will analyze the data protection regimes of each jurisdiction[61] and compare them with the framework developed above. The order of analysis has been chosen based upon how long each jurisdiction has been developing its regional data protection laws. Therefore, the European Union, which is on its second iteration of a regional data protection law, has been analyzed first; China, which has recently developed and implemented its first national data protection law, will be analyzed second; and the United States, which does not yet have a national data protection law will be analyzed last, with the added benefit of being able to compare proposed or anticipated national U.S. laws to the previous two jurisdictions.

Each Section will also provide a brief background of data protection in each jurisdiction, which will provide brief but useful background material for determining how or why the regulations in each jurisdiction have been developed into what they are today.

A. The European Union

Unlike China and the United States, the European Union is currently undergoing its second iteration of a regional set of laws governing data protection—the General Data Protection Regulation (GDPR).[62] Thus, the European Union has a chance to learn from application of its first iteration,[63] as well as various cases that have further developed the concepts of both data protection and privacy.[64]

While now the right to data protection is considered a fundamental right within the European Union,[65] there was significant debate leading up to that designation.[66]

---

60. Such *ex post* analysis of the causes of a breach are vital to ensuring that the same breach does not occur in the future. *See* Schwartz & Janger, *supra* note 56, at 934–35.

61. The European Union, China, and the United States.

62. The General Data Protection Regulation came into force on May 25, 2018, two years after it was passed by the European Parliament. Regulation (EU) 2016/679, 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].

63. The 1995 Directive, *supra* note 51.

64. *See, e.g.*, Joined Cases C-293/12 & C-594/12, Digital Rights Ireland v. Minister for Commc'ns, ECLI:EU:C:2014:238 (GC Apr. 8, 2014); Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (GC Oct. 6, 2015); Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (GC May 13, 2014). For a more in-depth analysis of the case law behind European data protection laws than will be covered here, see MARIA TZANOU, THE FUNDAMENTAL RIGHT TO DATA PROTECTION (2017).

65. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU]; Charter of Fundamental Human Right of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 1 [hereinafter CFHR].

66. *See, e.g.*, Joined Cases C-465/00, C-138/01, & C-139/01Österrichischer Rundfunk

The need for data protection has been a concern of the European Parliament since at least 1975, when data processing was still in its infancy.[67] The European Parliament saw the need for data protection as so important that it passed its first regional data protection law—the 1995 Directive[68]—at a time when only 1% of EU citizens were using the internet.[69]

This first major iteration of data protection law in the European Union gives broad principles within which Member States "shall . . . determine more precisely the conditions under which the processing of personal data is lawful."[70] The 1995 Directive is classified as an "omnibus regime," meaning that is intended to be generally applicable to all sectors, with specific exceptions spelled out in its provision.[71] As such, it does not lay down any specific framework but provides certain criteria within which national laws must fall.[72]

Since the establishment of the 1995 Directive, the European Court of Justice has, in three important cases, recognized the right to data protection as a fundamental right, a backdrop against which the most recent data protection regime (the GDPR)[73] has been developed. In a major step, the European Court of Justice (ECJ) in *Digital Rights Ireland Ltd.*, recognized the right to data protection as separate from the right to privacy and discussed the need for "fair information principles" in the processing of any personal data.[74] In *Google Spain*, the ECJ sought the "fair balance" between two rights: the fundamental right of data protection and the legitimate interest of internet users to access certain information.[75] Although they recognized that data protection rights will "as a general rule" override the public interest in those cases, they did also recognize that under certain circumstances (e.g. where the data subject is a public official or exercises public authority) the public interest can outweigh the data subject's right to data protection.[76]

The *Schrems* case[77] showed a slight change from the court's previous jurisprudence. Although it acknowledges the existence of a right to data protection,

---

and Others, 2003 E.C.R. I-5014, ¶ 68 (declaring that the provisions of the 1995 Directive must be interpreted "in light of fundamental rights," suggesting that data protection itself might not be among those fundamental rights). *But see* The 1995 Directive, *supra* note 51, pmbl. ¶ 10 (claiming that the object of laws regarding the processing of personal data is to "protect fundamental rights and freedoms").

67. *See* Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing, 1975 O.J. (C 60) 48.

68. The 1995 Directive, *supra* note 51.

69. LYNSKEY, *supra* note 6, at 4.

70. *Id.* at 39.

71. *See* LYNSKEY, *supra* note 6, at 15–30. This is in contrast to the sectorial regime present in the United States, which will be discussed later.

72. As will be seen later, this approach is very similar to the current approach in the United States. *See infra* Section II.C.

73. GDPR, *supra* note 62.

74. Joined Cases C‑293/12 & C‑594/12, Digital Rights Ireland v. Minister for Commc'ns (2014), ¶¶ 39, 40.

75. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (2014), ¶ 81.

76. *Id.*

77. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-627.

as enshrined in Article 8 of the Charter of Fundamental Human Rights of the European Union (CFHR),[78] that right is viewed and analyzed as an extension of the right to privacy enshrined in Article 7 of the CFHR.[79] Importantly, the court in *Schrems* allowed for the invalidation of secondary legislation[80] that violated the rights of data protection and privacy declared in the CFHR,[81] showing that EU courts are willing to enforce recognized fundamental rights rather than allowing the legislature to encroach on those rights.

As can be seen above, the European Union's data protection regimes have arisen in the past as a necessary extension of the fundamental rights of privacy and data protection. In the face of such developments, though, the 1995 Directive has been shown to be deficient. First, as a directive, many of the details were left up to EU Member States, resulting in a variety of different laws among Member States.[82] In addition, Member States, individually responsible for enforcement of their laws, took various approaches. Some focused on more proactive approaches, while others remained more reactive in their enforcement.[83] As a result of such fragmentation among Member States, the European Parliament, in April 2016, enacted the General Data Protection Regulation, which finally took effect on May 25, 2018,[84] in order to "ensure a consistent and high level of protection of natural persons."[85]

1. The General Data Protection Regulation

Building off the assumption that data protection (and privacy) is a fundamental right to which all persons are entitled and with an intent not to unduly inhibit cross-border transfers of information, the European Parliament set out to develop a

---

78. CFHR, *supra* note 65, art. 8.

79. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-627, ¶¶ 177, 179. *But see* PAUL DE HERT & SERGE GUTWIRTH, *Privacy, Data Protection & Law Enforcement. Opacity of the Individual and Transparency of Power*, *in* PRIVACY AND THE CRIMINAL LAW 61, 80 (Erik Claes, Antony Duff & Serge Gutwirth eds., 2006) (suggesting that European Courts have been using a broad interpretation of the right of privacy to expand, rather than define, a right of data protection).

80. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7.

81. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-627, ¶ 237.

82. *See* FARINA, *supra* note 41, at 146–48; *see generally* Bignami, *supra* note 23 (providing an overview of the different data protection regimes among European States).

83. *See* FARINA, *supra* note 41, at 146–48.

84. To significant fanfare in the international community. *See, e.g.*, Sam Schechner, *GDPR Takes Effect on Friday–Here's What to Expect*, WALL ST. J. (May 24, 2018, 5:30 AM), https://www.wsj.com/articles/5-questions-about-what-to-expect-when-gdpr-takes-effect-1527154200 [https://perma.cc/Q2RP-T3ZS]; Alex Hern & Jim Waterson, *Sites Block Users, Shut Down Activities and Flood Inboxes as GDPR Rules Loom*, GUARDIAN (May 24, 2018, 12:59 PM), https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect [https://perma.cc/F3B6-XDZE].

85. GDPR, *supra* note 62, pmbl. ¶¶ 9, 10.

universal, baseline set of data protection laws starting in 2012.[86] Eventually, this resulted in the current GDPR, which has been in effect since May 25, 2018.[87] In broad reaching and never before seen levels of protection, the GDPR protects names, addresses, racial data, cultural data, IP addresses, health data, and a plethora of other personal information,[88] not just within EU Member States, but across the globe.[89] Although not vastly different from the 1995 Directive, the GDPR does seek to reconcile the varying Member States' interpretations of the 1995 Directive to allow for proper function and cooperation under the Treaty of Lisbon.[90]

With respect to the data stewardship element of the data protection framework, the GDPR balances the need for data subject consent with a focus on the actual uses to which personal data is being put. Although the GDPR lists consent as one possible means for permissible data processing,[91] other permissible purposes for processing include: other legal obligations, the public interest, and protection of a natural persons' vital interests.[92] In addition, certain categories of personal data[93] receive heightened forms of protection, requiring specific measures—explicit consent, substantial public interest, and protection of vital rights of a natural person who cannot legally give consent—to be met before such data can be processed.[94]

Additionally, the GDPR sets forth the conditions for valid consent to processing, stating that consent must be a "freely given, specific, informed and unambiguous indication of the data subject's agreement,"[95] unlike the 1995 Directive which allowed for implied consent through silence or inactivity.[96] Such measures are important for closing the "knowledge gap" inherent between a data subject and a data processor,[97] but ultimately, they do not do enough to shift reliance away from a data subject's consent to truly fulfill the spirit of the data stewardship element.[98]

However, it is important to remember that the GDPR is meant to set a baseline level of data protection, with individual Member States required to implement their

---

86. *See 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 1, 6, COM (2012) 11 final (Jan. 25, 2012).

87. GDPR, *supra* note 62 art. 94.

88. Sebastian, *supra* note 38, at 217.

89. *See* Peltz-Steele, *supra* note 12.

90. Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L L. REV. 1095, 1117 (2014).

91. *See* Peltz-Steele, *supra* note 12, at 374; GDPR, *supra* note 62, art. 6.

92. GDPR, *supra* note 62, art. 6.

93. *Id.* art. 9, ¶ 1.

94. *Id.* ¶ 2.

95. *Id.* pmbl. ¶ 32. This paragraph also expressly prohibits silence or inactivity as a valid form of consent. *Id.*

96. The 1995 Directive only defines consent as "any freely given specific and informed indication" of acceptance, allowing for silence or inactivity to be considered valid consent. The 1995 Directive, *supra* note 51, art. 2.

97. *See* Schwartz, *supra* note 16, at 1660.

98. For example, Article 6 of the GDPR allows for processing beyond the scope of a data subject's consent if "any link" can be established between the purpose for collection and the purpose of further processing. GDPR, *supra* note 62, art. 6.

own laws in accordance with the GDPR.[99] Looking at the laws passed by such Member States, it is clear that, while the GDPR itself may not shift focus on data stewardship, some Member States have expanded data protections to properly encompass a data stewardship element. For example, France, soon after the passing of the GDPR, enacted its new Law for a Digital Republic,[100] which expressly allows for data subjects to decide and control the ways their personal data is used.[101] However, such expansions are not universal. Germany, for example, has also instituted a new data protection law, the Federal Data Protection Act,[102] but it does not contain any specific provisions regarding a data subject's ability to control or decide upon uses of their personal data.

Although the GDPR does not, on its own, fulfill the data stewardship element of the data protection framework, it does create a system by which enterprises can balance the risks and the benefits of data processing. Rather than just referring broadly to vague risks that could be caused by data processing, it gives specific examples of harms, including identity theft, financial loss, reputational damage, or a violation of any other fundamental right.[103] Potential benefits of data processing are not enumerated in the same way, but implicit in many of its provisions are benefits that can justify data processing, particularly national security,[104] vital interests of another natural person,[105] and protection of other fundamental rights.[106]

The GDPR does not create a direct comparison between the benefits and harms of data processing. Instead, security measures required to be implemented by enterprises must be reflective of the risk of harm (and degree of those harms),[107] which thus allows enterprises to create security measures that balance both their own

---

99. *Id.* pmbl. ¶ 167.

100. Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic], JOURNAL OFFICIEL DE LA RËPUBLIC FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Oct. 8, 2016, p. 0235 [hereinafter Law for a Digital Republic]; *see also* Denise Lebeau-Marianna & Caroline Chancé, *France: New Data Protection Law Has Been Adopted*, DLA PIPER: PRIVACY MATTERS (May 16, 2018), https://blogs.dlapiper.com/privacymatters/france-new-data-protection-law-has-been-adopted/ [https://perma.cc/M35G-MZ2G].

101. Law for a Digital Republic art. 54; *see also* Olivier Proust & Gaëtan Goossens, *France Adopts Digital Republic Law*, FIELDFISHER (Oct. 4, 2016, 10:59), http://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law/ [https://perma.cc/3LBG-MC9Y].

102. Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 [DSAnpUG-EU] [Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680], June 30, 2017, BGBL I at 2097 (Ger.) [hereinafter German Data Protection Act].

103. GDPR, *supra* note 62, pmbl. ¶ 75.

104. *Id.* art. 23.

105. *Id.* art. 6.

106. *Id.* art. 23. This provision seems to suggest that the right to data protection is not as important as other rights. However, the first paragraph of article 23 specifies that these benefits are potential sources for legislation regarding data protection and that no such legislation should interfere, unduly, with any other fundamental right, including the right to data protection. *Id.*

107. *Id.* art. 24.

capability to create a data processing infrastructure (and the benefit they may receive from such processing) and the risk of harms resulting from such processing.[108] The GDPR also contains provisions that allow individual Member States and industry associations to set their own codes of conduct with regard to data processing,[109] further allowing for more specific refinement of this harm/benefit system as it applies to different countries or industries.

The final element of the data protection framework, requirements for transparency and redress, is where the GDPR truly excels. A key requirement throughout the provisions of the GDPR is the need for transparency in data processing.[110] Contained within this transparency requirement are three other requirements: first, a right of proper notice;[111] second, a right of access by the data subject;[112] and third, a right of rectification by the data subject.[113]

Unlike the 1995 Directive, which required only that a data processor provide information regarding the identity of the processing and the purposes of processing,[114] the GDPR requires "clear and plain language,"[115] which provides proper notice to the data subject regarding contact details of the processor, identity of the data protection officer, the purposes of processing, the interest which justifies the processing, recipients of the personal data, the categories of data to be processed, and information regarding the data subject's rights with respect to their personal data.[116] Such information relates back to the consent requirement discussed earlier, and helps to reduce the "knowledge gap" between data subject and data processor[117] and therefore allows for properly informed consent by the data subject.[118]

In addition to requiring notice be given to the data subject, proper transparency requires that a data subject be allowed to access personal data held by the processor.[119] This is important because there are methods by which a processor can obtain and process personal data without getting consent of the data subject,[120] meaning the data subject may not have been aware, at first, that the data was collected or processed. This right allows for interested data subjects to discover who (and how) their data is being processed.[121]

---

108. Alo, *supra* note 90, at 1134–37 (discussing the deterring effects of data protection laws (namely the 1995 Directive) that do not take into account the size and ability of the data processors).

109. GDPR, *supra* note 62, art. 41, ¶ 1.

110. *Id.* arts. 5, 12, 26, 40.

111. *Id.* art. 12.

112. *Id.* art. 15.

113. *Id.* art. 16.

114. The 1995 Directive, *supra* note 51, art. 10.

115. GDPR, *supra* note 62, art. 12.

116. *Id.* art. 13.

117. Schwartz, *supra* note 16, at 1683.

118. GDPR, *supra* note 62, art. 4.

119. *Id.* art. 15.

120. *Id.* art. 6.

121. Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 843–45 (2012).

The right of access, under the GDPR, is not automatic. It must be exercised by the data subjects themselves rather than automatically provided by a data processor to every data subject.[122] This helps to offset any deterrent effects against smaller enterprises that would be present by requiring data processors to actively inform all data subjects that their data is being processed[123] because enterprises are only required to provide information to data subjects who request that information.[124]

Closely linked to the previous two rights is the right of rectification: the ability to correct incorrect or inaccurate information regarding a data subject.[125] Within the transparency requirement, this requirement is vital since it allows a data subject to demand the correction of information that they find to be incorrect. Although other alternatives to a right of rectification have been proposed,[126] these solutions ultimately fail to offer the simplicity and effectiveness that a right to rectification provides.

Even with these rights in place, a data protection regime is not complete without offering a means of redress; regulations which are not enforced by appropriate agencies are essentially useless. In this respect, the GDPR offers several advantages over the previous 1995 Directive. First, the GDPR specifically allows for class action remedies,[127] which are vital for enforcing rights where "no single individual would find it worthwhile to pursue a lawsuit independently,"[128] making class actions a "powerful regulatory enforcement tool."[129] Without the ability for individuals to act collectively, it would be difficult for a single data subject to bring suit, either through the courts or through administrative proceedings, against a large data processor.

The GDPR also establishes two new, independent agencies responsible for maintaining and enforcing the GDPR and its corresponding rights. The first, Supervisory Authorities, are established by individual Member States, for the purposes of enforcing the GDPR.[130] Importantly, Supervisory Authorities are completely independent entities "competent for the performance of the tasks assigned" to them.[131] The powers of each Supervisory Authorities include the ability

---

122. GDPR, *supra* note 62, art. 15. This article states that data subjects have "the right to obtain," not that data processors need to automatically provide, various pieces of information. *Id.*

123. Alo, *supra* note 90, at 1135.

124. GDPR, *supra* note 62, art. 15; *see also* Alex Hickey, *6 Months to GDPR: What's Next?*, CIO DIVE (Nov. 28, 2017), https://www.ciodive.com/news/6-months-to-gdpr-whats-next/511761/ [https://perma.cc/PP2A-WWTJ].

125. GDPR, *supra* note 62, art. 16; *see also* Bignami, *supra* note 23, at 814 (discussing some of the harms that can result from incorrect personal data being used for data processing).

126. *See, e.g.*, LoCascio, *supra* note 59, at 326–27 (comparing a right to rectification with a right of the data subjects to merely add their own information, rather than removing "incorrect" information).

127. GDPR, *supra* note 62, art. 80 (allowing individuals to identify "a not-for-profit body, organisation or association . . . to lodge the complaint on his or her behalf").

128. Deborah R. Hensler, *Revisiting the Monster: New Myths and Realities of Class Action and Other Large Scale Litigation*, 11 DUKE J. COMP. & INT'L L. 179, 182 (2001).

129. *Id.* at 183.

130. GDPR, *supra* note 62, arts. 51, 58.

131. *Id.* art. 55.

to carry out appropriate investigations, impose injunctions as necessary, and levy fines on non-compliant enterprises.[132]

Beyond this, the GDPR provides for a new administrative agency capable of enforcing its provisions—a European Data Protection Board (EDPB).[133] The EDPB has a myriad of responsibilities, including monitoring application of the GDPR, advising the European Commission regarding data protection laws, and issuing guidelines for data processors to follow.[134] In fact, the EDPB has already begun the arduous process of analyzing implementation of the GDPR and providing guidelines in order to help entities comply with its provisions.[135] The EDPB will also be an independent entity, composed entirely of members from the individual Supervisory Authorities of each Member State.[136] Independence of these authorities is important since, in addition to monitoring the behavior of private enterprises, the GDPR also applies to processing done by state actors.

Overall, the GDPR does fit well with the three-element framework developed earlier in this Note. Although it does continue to focus on the consent of the individual data subject as justification for various data processing,[137] the GDPR provides a good baseline of data protection for Member States of the European Union.[138] It enumerates possible harms and benefits, gives Member States the ability to balance them as they see fit, and gives some guidance to enterprises on how to balance the two.[139] Finally, by ensuring both the data processing is a transparent process and that there are appropriate measures for redress present for data subjects to pursue if needed, the GDPR imposes very strong protections for the fundamental rights of citizens of the European Union.[140]

---

132. *Id.* art. 58.

133. *Id.* art. 68. The EDPB actually replaced the Data Protection Working Party established under Article 29 of the 1995 Directive, but under the GDPR the EDPB has much more authority than the Data Protection Working Party possessed. Cynthia O'Donoghue & Alexander Mackay, *European Data Protection Board Replaces Article 29 Working Party*, REEDSMITH: TECH. LAW DISPATCH (July 2, 2018), https://www.technologylawdispatch.com/2018/07/privacy-data-protection/european-data-protection-board-replaces-article-29-working-party/ [https://perma.cc/J5G7-QE9M].

134. GDPR, *supra* note 62, art. 70.

135. *General Guidance*, EDPB https://edpb.europa.eu/our-work-tools/general-guidance_en; *see also European Data Protection Board Backs Ban on 'Cookie Walls'*, OUT-LAW (May 31, 2018), https://www.out-law.com/en/articles/2018/may/european-data-protection-board-cookie-walls-ban/ [https://perma.cc/BG26-5BX3].

136. *See* GDPR, *supra* note 62, art. 69.

137. *See supra* text accompanying notes 92–98. In fact, the GDPR as a whole focuses on individual rights more so than duties of businesses. *See* INFO. COMM'R'S OFFICE, PREPARING FOR THE GENERAL DATA PROTECTION REGULATION (GDPR): 12 STEPS TO TAKE NOW 4 (2017) (listing a number of individual rights guaranteed by the GDPR, including rights to (1) be informed, (2) access, (3) rectification, (4) erasure, (5) restrict processing, (6) data portability, (7) object, and (8) not to be subject to automated decision-making).

138. A baseline which has enabled and required individual Member States to implement their own data protection laws. *See supra* text accompanying notes 99–106.

139. *See supra* text accompanying notes 107–109.

140. *See supra* text accompanying notes 126–132.

In addition, since it came into effect, the European Union has shown a renewed commitment to enforcing the GDPR and data protection more generally—a heavy criticism that plagued the 1995 Directive.[141] Max Schrems[142] has already brought a number of cases against prominent companies, like Facebook and Google, over alleged violations of the GDPR.[143] In addition, the European Parliament has demonstrated that it may no longer be willing to concede to the United States' lax data protection laws when it decided that it may revoke the Privacy Shield framework at some point in the future[144] if the United States does not become fully compliant by September 1, 2018.[145] The actions suggest that, with the passage of the GDPR, the European Union will be much more proactive and effective in protecting the personal data of its citizens than it has been in the past.[146] In fact, with its development of the ePrivacy Regulation, the European Union is already looking towards the future of data protection in the digital world.[147] While this regulation, if

---

141. *See* THORBEN BURGHARDT, KLEMENS BÖHM, ERIK BUCHMANN, JÜRGEN KÜHLING & ANASTASIOS SIVRIDIS, A STUDY ON THE LACK OF ENFORCEMENT OF DATA PROTECTION ACTS (2009).

142. Famous for his cases that invalidated the former "Safe Harbor" data regime between the United States and the European Union. *See, e.g.*, Case C-362/14, Schrems v. Data Prot. Comm'r (2015).

143. NOYB, GDPR: *NOYB.EU* FILED FOUR COMPLAINTS OVER "FORCED CONSENT " AGAINST GOOGLE, INSTAGRAM, WHATSAPP AND FACEBOOK (2018); 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/EX3F-U95B].

144. This framework, which replaced the former EU-U.S. Safe Harbor Regime, allows for the transfer of information and personal data (for commercial purposes) between the European Union and United States. *See generally* U.S. DEP'T OF COMMERCE, FACT SHEET: OVERVIEW OF THE EU-U.S. PRIVACY SHIELD FRAMEWORK.

145. Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, EUR. PARL. DOC. B8-0305 (2018); *see also* Matthew J. Majkut, Paul Hastings LLP, *European Parliament Votes to Suspend EU-U.S. Privacy Shield*, LEXOLOGY (July 5, 2018), https://www.lexology.com/library/detail.aspx?g=60cb18f1-c657-44e0-a030-f83eec6d5211 [https://perma.cc/6TPK-HMKQ]. Despite this threat, though, the deadline passed without significant correction by the United States. Thus far, the European Union has not followed through on their threat and the Privacy Shield appears to still be in place. *See, e.g.*, Ariel Silverstone, John Wunderlich, Sholem Prasow & Stephan Grynwajc, *European Parliament Voted to Suspend Privacy Shield: Now What?*, IAPP (Sept. 25, 2018), https://iapp.org/news/a/european-parliament-voted-to-suspend-privacy-shield-now-what/ .

146. *See* Natasha Lomas, *Europe's Top Court Takes a Broad View of Privacy Responsibilities Around Platforms*, TECHCRUNCH (June 5, 2018), https://techcrunch.com/2018/06/05/europes-top-court-takes-a-broad-view-on-privacy-responsibilities-around-platforms/ [https://perma.cc/56XR-AMPV].

147. 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), COM (2017) 10 final (Oct. 1, 2017).

it ever passes,[148] will come with its own challenges,[149] it certainly indicates that the European Union does not intend the GDPR to be a "one and done" solution to the problem of data protection.

B. China—The Network Security Law

Although the Chinese government has monitored internet usage for many years,[150] it has not taken a particularly active role in the development of a national data protection regime until relatively recent times.[151] It has not been until recently that China has begun to truly analyze its own role in cyberspace, seeing both the advantages a proper data protection regime as well as recognizing its potential risks not only to individuals but to the stability and longevity of the government itself.[152]

A cybersecurity framework has been in place since 1994 in order to protect "critical national infrastructures,"[153] but this framework provides "[l]ittle detail" apart from stipulating multiple levels of security needs and allowing for further development by "relevant departments."[154] In 2003, the government revisited its cybersecurity regime, promulgating Document 27, in an attempt to unify regional cybersecurity regimes.[155] Ultimately, though, Document 27 (even the new 2012 version) has been seen as having the opposite effect, resulting in various interagency disputes that prevent uniformity throughout the nation, caused by the opinion's "grab

---

148. *See* Andrew Ross, *European ePrivacy Regulation: Work in Progress*, INFO. AGE (June 7, 2018), https://www.information-age.com/european-eprivacy-regulation-123472251/ [https://perma.cc/W9CQ-S5ND].

149. *See, e.g.*, Natasha Singer, *The Next Privacy Battle in Europe Is over This New Law*, N.Y. TIMES (May 27, 2018), https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html [https://perma.cc/Q3RB-TUGH].

150. CHINA INTERNET NETWORK INFO. CTR., STATISTICAL REPORT ON INTERNET DEVELOPMENT IN CHINA (2017) (the latest of thirty-nine reports which document the development of China's internet usage since 1997).

151. Guowuyuan Guanyu Dali Tuijun Xinxi Hua Fazhan He Qieshi Baozhang Xinxi Anquan De Ruogan Yijian (国务院关于大力推进信息化发展和切实保障信息安全的若干意见) [Certain Opinions of the State Council on Promoting Informatization Development and Practically Safeguarding Information Security] (promulgated by the St. Council, June 28, 2012, effective June 28, 2012) Guo Fa [2012] No. 23 (WestlawChina) [hereinafter Informatization Opinions].

152. *See* AMY CHANG, CTR. FOR A NEW AM. SEC., WARRING STATE: CHINA'S CYBERSECURITY STRATEGY 10 (2014); *see also*, Edward Wong, *For China, Cybersecurity Is Part of Strategy for Protecting the Communist Party*, N.Y. TIMES (Dec. 3, 2014, 10:00 AM), https://sinosphere.blogs.nytimes.com/2014/12/03/for-china-cybersecurity-is-part-of-strategy-for-protecting-the-communist-party/ [https://perma.cc/ZE5C-DWLJ].

153. Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 158 (2014).

154. *Id.*

155. Guojia Xinxihua Lingdao Xiaozu Guanyu Jiaqiang Xinxi Anquan Baozchang Gongzuo De Jijian (国家信息化领导小组关于加强信息安全保障工作的意见) [Document 27: Opinions for Strengthening Information Security Assurance Work] (promulgated by the St. Council, Sept. 9, 2003, effective Sept. 9, 2003) [hereinafter Document 27].

bag of vague policy proposals" and its failure to be "internally consistent."[156] In fact, most scholarship regarding China's cyberspace regimes has been focused on its cybersecurity regimes, and how such regimes pose a threat (either militarily or economically) to other regions, and not on how China has developed its own domestic data protection regimes.[157]

Unlike data protection in the European Union, which at its base recognizes the right to data protection as a fundamental right, data protection in China is arguably in place primarily to protect the governing power of the Chinese Communist Party (CCP).[158] Beginning with the proposition that order and stability (in the form of a stable government) override the interests of an individual,[159] Chinese cybersecurity policy has evolved over time to encompass both the CCP's desire for economic growth (on the international stage) as well as its desire to maintain domestic stability (on the national stage).[160] For years, it has been the Chinese government's position that personal information security is important for "[p]roperly guiding internet opinion,"[161] and the government has used this interest in social stability—which it considers paramount during this "crucial stage of reform and development"—as a pretense for monitoring, controlling, and even protecting personal data.[162]

The true buildup to China's current Network Security Law[163] began in 2012, shortly before Xi Jinping ascended to power in the Communist Party.[164] In July, the

---

156. Adam Segal, *China Moves Forward on Cybersecurity Policy*, COUNCIL ON FOREIGN RELS. (July 24, 2012), https://www.cfr.org/blog/china-moves-forward-cybersecurity-policy [https://perma.cc/9AF3-LYW5]; *see also* Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 32–33 (2016).

157. *See generally China's Technological Rise: Challenges to U.S. Innovation and Security: Hearing Before Subcomm. on Asia and the Pacific of the H. Comm. on Foreign Affairs*, 115th Cong. 3–4 (2017) (statement of Rep. Ted Yoho, Chairman, Subcomm. on Asia and the Pacific); JASON R. FRITZ, CHINA'S CYBER WARFARE: THE EVOLUTION OF STRATEGIC DOCTRINE (2017); SCOTT WARREN HAROLD, MARTIN C. LIBICKI & ASTRID STUTH CEVALLOS, GETTING TO YES WITH CHINA IN CYBERSPACE (2016).

158. CHANG, *supra* note 152; *see also*, Wong, *supra* note 152.

159. *See* HAROLD ET AL., *supra* note 157, at 22.

160. CHANG, *supra* note 152, at 7.

161. Chris Buckley & Lucy Hornby, *China Defends Censorship After Google Threat*, REUTERS (Jan. 14, 2010, 12:24 AM), https://www.reuters.com/article/us-china-usa-google/china-defends-censorship-after-google-threat-idUSTRE60C1TR20100114 [https://perma.cc/XRK5-QNGW].

162. *Id.*; *see generally* INTERNET CENSORSHIP (Margaret Haerens & Lynn M. Zott eds., 2014).

163. Wangluo anquan fa (网络安全法) [Network Security Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm [https://perma.cc/XR8H-STPP]. Some sources refer to this law, alternatively, as the Cybersecurity Law due to the practical purposes of the law, but the more literal translation is Network Security Law. In order to be as true as possible to the source material, this Note will use the latter, more literal translation, although other cited sources may refer to it by its alternative name.

164. *See China New Leaders: Xi Jinping Heads Line-Up for Politburo*, BBC (Nov. 15, 2012), https://www.bbc.com/news/world-asia-china-20322288 [https://perma.cc/H2GM-AYXY]; *The Power of Xi Jinping*, ECONOMIST (Sept. 18, 2014), https://www.economist.com

State Council promulgated an opinion calling for all regions and agencies to begin implementing strategies designed to increase internet access across the country and for those same entities to institute effective information security systems.[165] Additionally in 2012, the Standardization Administration of the People's Republic of China set forth nonmandatory guidelines related to the protection of personal information.[166] These guidelines included fundamental principles that should be followed,[167] as well as a broad overview of the different steps involved in the processing of personal data.[168]

In 2014, President Xi established the Central Network Security and Information Leading Small Group ("Network LSG"), identifying "Internet security and informatization [as] a major strategic issue," while at the same time reaffirming that Chinese data protection strategies envision an internet intended to "nurture socialism's core values."[169] Overall, the trend in China has been a domestic focus on improving and preserving native internet use[170] rather than following other globalized trends.[171] This trend towards domestic control and ownership of data

---

/news/china/21618882-cult-personality-growing-around-chinas-president-what-will-he-do-his-political [https://perma.cc/V5ZY-NQ26].

165. Informatization Opinions, *supra* note 151.

166. Xinxi Anquan Jishu Gonggong Ji Shangyong Fuwu Xinxi Xitong Geren Xinxi Baohu Zhinan (信息安全技术 公共及商用服务信息系统个人信息保护指南) [Information Security Technology: Guidelines on Personal Information Protection of Public and Commercial Service Information Systems] (promulgated by the General Administration of Quality Supervision, Inspection, and Quarantine & the Standardization Administration of the People's Republic of China, Nov. 5, 2012, effective Feb. 1, 2013) GB/Z 28828-2012 (WestlawChina).

167. *Id.* art. 4.2. These principles include the principles of clear purposes, personal consent, security guarantee, and clear responsibility. *Id.*

168. *Id.* art. 5. These stages are the collection stage, *id.* art. 5.2, the processing stage, *id.* art. 5.3, the transfer stage, *id.* art. 5.4, and the deletion stage, *id.* art. 5.5.

169. Shannon Tiezzi, *Xi Jinping Leads China's New Internet Security Group*, DIPLOMAT (Feb. 28, 2014), https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/ [https://perma.cc/KT85-L8FX]; *see also Xijinping: ba woguo cong wangluo daguo jianshechengwei wangluo qiangguo* (习近平:把我国从网络大国建设成为网络强国) [*Xi Jinping: Building China into a Powerful Network Power from a Large Network Power*], XINHUANET (Feb. 27, 2014), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm [https://perma.cc/ZC8N-XDJH].

170. *See* Shackelford & Craig, *supra* note 153, at 162–63 (arguing that the large breadth of regulations is a result of China's "push for 'indigenous innovation'"); *see also* DIETER ERNST, INDIGENOUS INNOVATION AND GLOBALIZATION: THE CHALLENGE FOR CHINA'S STANDARDIZATION STRATEGY 36 (2011) (describing requirements for Chinese critical information infrastructures to be based on the Chinese mainland rather than outsourced to globalized industry leaders).

171. *See* Scott Kennedy, *The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars*, 2 ASIA POL'Y 41, 57–59 (2006) (detailing industry initiatives within China that sought to develop their own home networking standards, as opposed to joining standards set by the international community); Jun Mai, *Xi Jinping Renews 'Cyber Sovereignty' Call at China's Top Meeting of Internet Minds*, S. CHINA MORNING POST (Dec. 3, 2017, 11:20 PM), http://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top [https://perma

processing infrastructure has continued into the modern day, with the passing, in 2016, of the Network Security Law, which came into effect on June 1, 2017.[172]

1. The Network Security Law

While the Network Security Law does represent a very positive step for data protection in China, it is still far from perfect. Like other laws within China, the Network Security Law suffers from a problem with vagueness.[173] At times, it fails to elaborate specific remedies and instead merely references "administrative regulations" that should come in the future, but which were not present at the time the law came into effect.[174] Although prior to implementation, there were several administrative measures that the Network Security Law could potentially refer to,[175] unfortunately the Network Security Law does not explicitly reference these laws.

Like the GDPR, this Note will first consider the data stewardship element with regard to the Network Security Law. While consent is required under the Network Security Law, it is far from the primary focus of the law. In fact, the word consent (同意) only appears three times in the entire Network Security Law[176] and is not

---

.cc/ZBC2-D6VA] (reaffirming President Xi's support for cyber sovereignty). *But see* Cate Cadell, *China's Xi Says Country Will Not Close Door to Global Internet*, REUTERS (Dec. 2, 2017, 9:54 PM), https://www.reuters.com/article/us-china-cyber/chinas-xi-says-country-will-not-close-door-to-global-internet-idUSKBN1DX01S [https://perma.cc/YN98-2VB7] (quoting note by Xi claiming that China's doors will only become "more and more open").

172. Network Security Law, *supra* note 163, art. 79; *see also China's New Cybersecurity Law Takes Effect Today, and Many Are Confused*, CNBC (June 1, 2017, 3:15 AM), https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html [https://perma.cc/96VR-25PF].

173. *See, e.g.*, Nicole Chaput, *An Introduction to Insurance Law and Coverage in the People's Republic of China*, 30 TORT & INS. L.J. 871, 891 (1995) (discussing the shortcomings involved with China's vague contract laws); Lawrence J. Trautman, *American Entrepreneur in China: Potholes and Roadblocks on the Silk Road to Prosperity*, 12 WAKE FOREST J. BUS. & INTELL. PROP. L. 425, 436 (2012) (highlighting the shortcomings of vague investment laws in China).

174. Kareena Teh & Philip Kwok, Dechert LLP, *The Cyberspace Administration of China Clarifies the Cybersecurity Law*, LEXOLOGY (June 2, 2017), https://www.lexology.com/library/detail.aspx?g=2c6842f5-7c4a-49de-8498-da93e1a90a81 [https://perma.cc/D6AA-SQWJ].

175. *See, e.g.*, Tongxin Wangluo Anquan Fanghu Guanli Banfa (通信网络安全防护管理办法) [Administrative Measures for the Security Protection of Communication Networks] (promulgated by the Ministry of Indus. & Info. Tech., Jan. 21, 2010, effective Mar. 3, 2010) (WestlawChina); Xinxi Anquan Dengji Baohu Guanli Banfa (信息安全等级保护管理办法) [Administrative Measures for Hierarchical Protection of Information Security] (promulgated by the Ministry of Pub. Sec., June 26, 2007, effective June 26, 2007) Gong Tong Zi No. 43 (WestlawChina). *But see* Wangluo Chanpin He Fuwu Anquan Shencha Banfa (Shixing) (网络产品和服务安全审查办法 (试行)) [Measures for Security Review of Network Products and Services (For Trial Implementation)] (promulgated by the St. Internet Info. Office, May 2, 2017, effective June 1, 2017) [hereinafter Security Review Measures] (a short law that sets out guidelines for security review of networks, that was passed along with the Network Security Law).

176. Network Security Law, *supra* note 163, arts. 22, 41, 42.

actually defined within the text of the law itself. Rather, the law focuses far more on requiring proper use of personal data than acquiring consent of the data subject.[177]

Before listing permissible ways in which to use personal data, the Network Security Law, in article 27, first proscribes certain behaviors with respect to network security and personal data. These behaviors include the theft of network data, enabling others to endanger network services, and disturbing the use of network data by others.[178] When the Network Security Law describes permissible use of personal data, though, it again runs into problems of vagueness. While the law does require "dueness and necessity," it does not define possible justifications for processing of personal data or what qualifies as a valid necessity.[179]

Despite these weaknesses with regard to consent and proper data uses, the Network Security Law does maintain a strict focus on ensuring that data processors properly care for the personal data in their possession. Beyond simply creating a requirement for data processors themselves to monitor and protect personal data,[180] the Network Security Law lists specific measures that can be put into place to ensure proper protection of personal data, including encryption, security training, and proper documentation of security measures in place.[181] The law also creates a mandate for appropriate government agencies to review security measures in place for protection of personal data in order to ensure that they provide adequate protection.[182]

Although the Network Security Law does an excellent job providing for proper data stewardship, it fails to establish any system by which a data processor can balance the harms and benefits of data processing. Other than vague references to "social ethics" or potential "harm" resulting from improper data processing,[183] there are no specific references to harms that could result from improper data processing.[184] Similarly, beyond the vague references to "dueness and necessity" mentioned earlier, there are no specific benefits to data processing that are recognized in the law itself.

Without such a system in place, data processors are given almost no notice as to what will or will not constitute valid data processing.[185] There are several possible

---

177. *Id.* at 41 (describing circumstances in which collection and use of personal data is permissible without explicitly stating consent as a justification).

178. *Id.* art. 27.

179. *Id.* art. 41.

180. *Id.* arts. 10, 36, 40.

181. *Id.* arts. 21, 34; *see also* LING HUANG, DANIEL ILAN, ZHENG (JONATHAN) ZHOU & KATHERINE MOONEY CARROLL, UNDERSTANDING THE IMPACT OF CHINA'S FAR-REACHING NEW CYBERSECURITY LAW (2018).

182. Network Security Law, *supra* note 163, art. 51; *see also* Security Review Measures, *supra* note 175.

183. *See, e.g.*, Network Security Law, *supra* note 163, arts. 9, 12, 54. 64.

184. In a rather circular bit of reasoning, it seems that the only way to cause harm would be by violating the law, while at the same time, the law is only violated when harm is caused. *See id.* art. 64.

185. Additionally, since China is a civil law system, courts are free to look at each case independently, meaning that enterprises cannot rely on prior case law to (always) shape their behavior, though trends in prior cases may help provide some guidance where the law is silent. *See* Zhang Jing, *Five-Year Review of China's Case Guidance System*, 2016 Zeitschrift für Chinesisches Recht [ZChinR] 20 (2016).

explanations for such silence. First, it could simply be that the National People's Congress contemplated later regulations and guidelines to supplement the Network Security Law[186] and so left the law itself relatively vague (and broad).[187] An alternative reason for the silence could be that creating a very broad law helps to further the government's goal of controlling internet content[188]—a goal that seems increasingly likely given the Chinese government's actions recently.[189] Regardless of the reasoning behind the language of this law, one thing is still very clear—little guidance is given to data processors regarding what harms they must avoid and what benefits they should seek.[190]

The Network Security Law also takes a very different approach to transparency and redress than the GDPR. As discussed earlier,[191] three general rights make up sufficient transparency with regard to data processing: a right of notice, a right of access, and a right of rectification. With regard to the right of notice, the Network Security Law does require that data processors publicize the rules for collection and use of personal data.[192] However, the details of these rules are not clearly enumerated, as they are in the GDPR,[193] again leaving processors with uncertainty regarding their desires.[194]

Absent entirely from the Network Security Law is the right of access. There is no express right for an individual to request information or data from a data processor. Although the Network Security Law does contain a right of rectification,[195] allowing for individuals to force data processors to correct or delete erroneous data, such a

---

186. Most such guidance only exists in draft form, though, and has thus not been enacted by the Chinese government. *See* Ulrike Glueck & Sammie Hu, *New Developments in the PRC Cyber Security Law*, LEXOLOGY (Dec., 21, 2017), https://www.lexology.com/library/detail.aspx?g=c56075af-1e68-4e4e-96da-b1982c6cf948 [https://perma.cc/C47V-VMRW].

187. *See* HUANG ET AL., *supra* note 181, at 15. *But see supra* note 175 and accompanying text.

188. *See* Buckley & Hornby, *supra* note 161; *see also* Shackelford & Craig, *supra* note153, at 31.

189. *See* Rhys Dipshan, *China's Cybersecurity Law Isn't Just About Cybersecurity*, LAW.COM: LEGALTECH NEWS (Jan. 29, 2018, 1:13 PM), https://www.law.com/legaltechnews/sites/legaltechnews/2018/01/29/chinas-cybersecurity-law-isnt-just-about-cybersecurity/ [https://perma.cc/4CZQ-CES8].

190. *UN Rights Chief Concerned By 'Broad Scope' of China's New Security Law*, UN NEWS (July 7, 2015), http://www.un.org/apps/news/story.asp?NewsID=51355#.WkkP8BM-eu6 [https://perma.cc/3XYB-G33D] [hereinafter *UN Rights Chief Concerns*].

191. *See supra* notes 111–126 and accompanying text.

192. Network Security Law, *supra* note 163, art. 41.

193. *See* GDPR, *supra* note 62, art. 13.

194. Such uncertainty in legislative goals seems to be a theme throughout much of the Chinese government's behavior regarding cybersecurity (of which data protection is just one facet). *See* HAROLD ET AL., *supra* note 157, at 60–61; *see generally* FRITZ, *supra* note 157. Again, there could be a number of possible reasons for this. One of the primary reasons seems to be the presence of differing goals between various governmental agencies, each with seemingly equal authority, but at the same time, very divergent ideas of how to implement those ideas. *See* CHANG, *supra* note 152, at 15–20.

195. Network Security Law, *supra* note 163, art. 43 (allowing for data subject to request rectification if they discover something inaccurate).

right is weakened significantly by the lack of a corresponding right to discover that information.[196]

Rather than focusing on transparency, which would better allow for individuals to enforce the provisions of the law, the Network Security Law attempts to shift the burden of enforcing its provisions almost entirely onto its built-in (and state controlled) measures for redress.[197] Unlike many of its other provisions, the articles providing for fines, injunctions, and other remedies contain significant detail, spelling out both the offense as well as corresponding punishment.[198] In addition, the Network Security Law gives authority to monitor and enforce these provisions to "the National Grid and Information Department."[199] This department is the Cyberspace Administration of China (CAC), which reports to the Network LSG, which in turn is led by President Xi Jinping.[200] Unlike the Supervisory Authorities under the GDPR, the CAC is a subservient government agency and does not exercise its own independent judgment, again showing the Chinese government's desire to maintain control over internet content.[201]

Overall, the biggest criticism with China's Network Security Law is the vagueness of many of its provisions.[202] Without adequately clear guidelines, data processors are left without any clear way of knowing whether or not their behavior complies with the law. As a result, large enterprises may be tempted to reduce (or even abandon altogether) their operations within mainland China.[203] In time, further

---

196. *See generally* Samson Yoseph Esayas, *Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 317 (2014); Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097 (2007); Aidan Forde, *Implications of the Right to Be Forgotten*, 18 TUL. J. TECH. & INTELL. PROP. 83 (2015); Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 SAINT JOHN'S L. REV. 1569 (2010); Wehbé, *supra* note 56, at 90–93.

197. Network Security Law, *supra* note 163, arts. 59–75.

198. *Id.*

199. *Id.* art. 51.

200. *See supra* note 169 and accompanying text.

201. *See* Shackelford & Craig, *supra* note153, at 30–32; *see also* Ariel E. Wade, Note, *A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty*, 42 GEO. WASH. INT'L L. REV. 659, 666–67 (2010). Fears that this the Network Security Law could be used to stifle dissent and support began shortly after implementations, when the government began investigating large social media platforms throughout the country. *See* Josh Chin, *China Targets Social-Media Giants WeChat, Weibo in Cybersecurity Probe*, WALL ST. J. (Aug. 11, 2017, 2:14 AM), https://www.wsj.com/articles/wechat-weibo-among-targets-in-china-cybersecurity-probe-1502432081?mod=article_inline [https://perma.cc/9RZC-USXH].

202. Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, DIPLOMAT (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ [https://perma.cc/WL7H-PKNA]; *see also* Carly Ramsey & Ben Wootliff, *China's Cyber Security Law: The Impossibility of Compliance?*, FORBES: RISKMAP (May 29, 2017, 3:29 AM), https://www.forbes.com/sites/riskmap/2017/05/29/chinas-cyber-security-law-the-impossibility-of-compliance/#73f85ae8471c [https://perma.cc/PP4G-HHWD].

203. *See* LYNSKEY, *supra* note 6, at 76–81; Nicolas Groffman, *Foreign Firms Watch Out, Beijing May Require You to Leave China Data in China*, S. CHINA MORNING POST (Oct. 29, 2017), https://www.scmp.com/week-asia/opinion/article/2117346/foreign-firms-watch-out-beijing-may-require-you-leave-china-data [https://perma.cc/7NEN-874L]. He Huifeng,

guidance may come in the form of administrative regulations and other guidelines,[204] but in the meantime, the government expects full compliance with the law, which forces some firms to conform to the best of their ability and hope for few negative consequences.[205]

C. The United States—NIST

Unlike China and the European Union, the United States has not yet implemented an omnibus data protection regime,[206] in which the laws guarantee a minimum level of protection.[207] Instead, the United States has implemented sector specific data

---

Cybersecurity Law Causing 'Mass Concerns' Among Foreign Firms in China, S. CHINA MORNING POST (Mar. 2, 2018, 6:29 AM), https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china [perma.cc/UY6D-K3JD].

204. The PRC continues to develop its Network Security Law through various regulations, but the effectiveness and clarity of even these regulations is up for debate. *See* COVINGTON, CHINA SEEKS PUBLIC COMMENTS FOR DRAFT REGULATIONS ON CYBERSECURITY MULTI-LEVEL PROTECTION SCHEME TO IMPLEMENT THE CYBERSECURITY LAW (2018), https://www.cov.com/-/media/files/corporate/publications/2018/07/china-seeks-public-comments-for-draft-regulations-on-cybersecurity-multilevel-protection-scheme-to-implement-the-cybersecurity-law.pdf [https://perma.cc/WWM2-4S6X]. Certain aspects of the Network Security Law already have draft measures circulating, but when (and if) these measures will be implemented is still uncertain. *See* Clarice Yue, Michelle Chan, Sven-Michael Werner & John Shi, *China Cybersecurity Law Update: Draft Guidelines on Security Assessment for Data Export Revised!*, BIRD & BIRD (Sept. 26, 2017), https://www.twobirds.com/en/news/articles/2017/china/draft-guidelines-on-security-assessment-for-data-export-revised [https://perma.cc/GQ2M-TJXF] (observing one revised draft of the Guidelines on Security Assessment for Data Export).

205. *See* Wagner, *supra* note 202; *see also* Nick Beckett, *A Guide for Businesses to China's First Cyber Security Law*, COMPUTERWEEKLY (Nov. 2017), http://www.computerweekly.com/opinion/Chinas-first-cyber-security-law-what-it-means-for-companies [https://perma.cc/EZ4R-MPGQ]; Ron Cheng, *China Enforces First Action Under Developing Cyber Security Law*, FORBES (Aug. 8, 2017, 4:58 PM), https://www.forbes.com/sites/roncheng/2017/08/08/china-enforces-first-action-under-developing-cyber-security-law/#7d07d0e522bc [https://perma.cc/4ANR-ST7X] (showing that the Chinese government is fully intent on punishing even minor infractions of the Network Security Law).

206. Much scholarship discussing data protection laws in the United States refers to these laws as "data privacy" laws. For the purposes of this Note, the two terms, data protection and data privacy, will be considered interchangeable. However, especially with respect to the United States, the terms data protection and data privacy are not, necessarily, interchangeable. *See* STEPHEN COBB, DATA PRIVACY AND DATA PROTECTION: US LAW & LEGISLATION 1 (2016); PETER P. SWIRE & KENESA AHMAD, INT'L ASS'N PRIVACY PROF'LS, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION (Terry McQuay ed., 2012); DAVID FLAHERTY, DATA PROTECTION AND PRIVACY: COMPARATIVE POLICIES 2 (1985) (distinguishing between data protection and privacy protection in the legal context).

207. This is not to say that specific states have not implemented their own data protection laws. *See, e.g.*, An Act to Add Title 1.81.5 (Commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, Relating to Privacy, Assembly Bill No. 375 (2018) (to be codified at CAL. CIV. CODE § 1798.100 *et seq.*); Andy Green, *SHIELD Act Will Update New York State's*

protection regimes, which apply only to specific industries.[208] In addition, individual states are free to set their own data protection regimes, and some have done so.[209]

The first federal legislation in the United States specifically aimed towards data protection was passed in 1970,[210] the Fair Credit Reporting Act of 1970.[211] The FCRA established three important principles that would go on to be present in future data protection laws.[212] First, it established the principle of individual consent, requiring citizens to consent to specific types of personal data recording.[213] Second, it established various administrative procedures (overseen by appropriate agencies) available to individuals who feel their information is incorrect or their rights have been violated.[214] Third, the FCRA enumerated various conditions under which the collection and use of personal data can be justified.[215]

This trend of sector-specific legislation continued through the 1970s into the early twenty-first century[216] and includes: the Family Education Rights and Privacy Act of 1974,[217] the Right to Financial Privacy Act of 1978,[218] the Health Insurance Portability and Accountability Act of 1996,[219] and the Gramm-Leach-Bliley Act of 1999.[220] One key aspect of all of these laws is the idea that data protection stems from an individual's right to privacy. Unlike in the European Union, where data protection is recognized as a fundamental right,[221] no right to data protection is present in the U.S. Constitution. Instead, a constitutional right to privacy has developed through U.S. case law.[222] This right of privacy has been applied and

---

Breach Notification Law, VARONIS (Apr. 14, 2018), https://blog.varonis.com/shield-act-will-update-new-york-states-breach-notification-law/ [https://perma.cc/P7KP-4B9E].

208. *See, e.g.*, 5 U.S.C. § 552a (2012 & Supp. II 2015); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); Children's Internet Protection Act, Pub. L. No. 106-554, 114 Stat. 2763 (2000); *see also* GETTING THE DEAL THROUGH, DATA PROTECTION & PRIVACY 191–98 (Rosemary P. Jay ed., 2014) (describing U.S. data privacy laws as a "patchwork quilt").

209. *See, e.g.*, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2017).

210. COBB, *supra* note 206, at 2.

211. 15 U.S.C. § 1681 (2012) [hereinafter FCRA].

212. COBB, *supra* note 206, at 2.

213. *Id.*

214. *Id.*

215. *Id.* Such conditions include (but are not limited to): employment purposes, investment purposes, and other legitimate business needs. FCRA § 1681b.

216. *See* COBB, *supra* note 206, at 5–6.

217. 20 U.S.C. § 1232g (2012).

218. 12 U.S.C. §§ 3401–3422 (2012 & Supp. III 2016).

219. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

220. Gramm-Leach-Bliley Act , Pub. L. No. 106-102, 113 Stat. 1338 (1999).

221. *See supra* Section I.A.

222. Namely, in *Griswold v. Connecticut*, the U.S. Supreme Court recognized a right to privacy as inherent in the First Amendment. 381 U.S. 479, 483 (1965) (recognizing a "penumbra" where privacy is protected from government intervention); *see also* Katz v. United States, 389 U.S. 347 (1967) (recognizing a reasonable expectation of privacy for individuals within the context of searches and seizures).

discussed in several specific instances[223] but does not provide the same comprehensive protection that it does in the European Union.

In addition to this "right of privacy," other explanations for data protection laws in the United States have ranged from "the promotion of commerce and wealth, to 'a healthy distrust for governmental solutions.'"[224] But despite these reasons, the United States has still not passed comprehensive national data protection legislation. In place of such legislation, though, the U.S. government has turned to two alternative methods of enforcement: self-regulation within the private sector[225] and reliance on the Federal Trade Commission (and its broad authority) as the de facto cybersecurity agency.[226]

With regard to industry self-regulation, the primary mechanism by which enterprises tailor their behavior is by abiding by the National Institute of Standards and Technology's Cybersecurity Framework.[227] Although not mandatory itself,[228] the NIST Framework is likely to be considered the new "standard for due diligence" in the event that an enterprise's practices were ever questioned in litigation or investigation.[229] As such, it would be in most U.S. enterprises' best interests to conform with, or at least familiarize themselves with, this framework.

Beyond the NIST Framework, the FTC, with its responsibility to "monitor all domestic United States commerce,"[230] has undertaken to enforce privacy policies by classifying violations as "unfair or deceptive acts or practices in or affecting commerce."[231] Unlike the NIST Framework, though, the FTC's policies are seen as

---

223. *See, e.g.*, Sorrell v. IMS Health Inc., 564 U.S. 552 (2016); Fisher v. United States, 425 U.S. 391 (1976).

224. Robert R. Schriver, Note, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2779 (2002) (quoting James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSEPECTUS 145, 150 (2001)).

225. Balaban, *supra* note 23, at 9–11.

226. *See* Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 235–44 (2017).

227. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018) [hereinafter NIST Framework]. A new version, Version 1.1, was released in April 2018, meaning that many businesses have not had a chance to fully implement appropriate data protection regulations, but looking at industry compliance with the previous version, released in 2014, helps to determine the likelihood of compliance with the current version. *See The Stakeholders Have Spoken: NIST to Refine Cybersecurity Framework*, NIST (June 9, 2016), https://www.nist.gov/news-events/news/2016/06/stakeholders-have-spoken-nist-refine-cybersecurity-framework [https://perma.cc/44V6-LDZP].

228. Except to government entities.

229. Scott J. Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 222 (2016); *see also* John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOTPOINT SEC. (Feb. 25, 2014), https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework/ [https://perma.cc/2MBC-CDJS].

230. Balaban, *supra* note 23, at 14.

231. Federal Trade Commission Act, 15 U.S.C. § 45 (2012) [hereinafter FTCA].

reactive, rather than proactive, since the FTC cannot act until an enterprise has wronged the public.[232]

1. NIST Framework and the FTC

In response to an executive order by President Obama acknowledging a need for "improved cybersecurity,"[233] NIST developed its framework[234] as a way to "protect individual privacy and civil liberties."[235] Because the NIST Framework is a "voluntary Framework"[236] there are no (direct) consequences of enterprises not following its provisions. Additionally, the focus of the NIST Framework is behavior of data processors, rather than a focus on data subjects and their rights, which means that it severely lacks any forms of redress or transparency (as will be discussed later). To fill in the gaps of the NIST Framework, though, the FTC has stepped into the role of a national data protection authority within the United States.[237]

Even without the presence of an omnibus data protection law, the current data protection regime has a heavy focus on the data stewardship element of our data protection framework. The NIST Framework only mentions consent in passing, as one possible factor for enterprises to consider when implementing their data protection policies,[238] and instead focuses on ensuring the data processors develop appropriate systems for the use and protection of personal data.[239] The NIST Framework goes into significant detail regarding specific ways to protect personal data (even though it doesn't specify how exactly to use that personal data).[240]

Because of its focus on the behavior of data processors generally, rather than the rights of data subjects, the NIST Framework best fits with the data stewardship element of our data protection framework. The burden, under the NIST Framework, is entirely on the data processors to "[d]evelop and implement the appropriate safeguards" for data processing activities,[241] allowing for data subjects to remain confident that their personal data will neither be leaked to unknown third-parties nor used for purposes of which they do not approve.[242]

Although the NIST Framework describes itself as providing a method of "risk-based" implementation,[243] without actually enumerating potential risks, it is justified in doing so. Since the NIST Framework is intended to help data processors create their own data protection regimes (rather than simply using the NIST Framework

---

232. Balaban, *supra* note 23, at 14.
233. Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).
234. *See generally* Shackelford et al., *supra* note 229, at 221–24.
235. NIST Framework, *supra* note 227, at 2. The recognition of such rights is very reminiscent of the European Union's approach to data protection, which recognizes it as a fundamental right of all people. *See* GDPR, *supra* note 62, pmbl. ¶ 1.
236. NIST Framework, *supra* note 227, at vi.
237. *See* Pardau & Edwards, *supra* note 226, at 229.
238. NIST Framework, *supra* note 227, at 19.
239. *Id.* at 7–8.
240. *Id.* at 23–44.
241. *Id.* at 46.
242. *See* Cate, *supra* note 8, at 12.
243. NIST Framework, *supra* note 227, at 4.

themselves)[244] it cannot enumerate specific harms because such a list would apply (or not apply) to different industries in different ways.[245] Instead, the NIST Framework requires data processors to develop their own risk management system, which includes the identification of potential harm of processing, the chance of those harms occurring, and the goals and benefits of that processing.[246]

A problem with this approach, though, is that it allows individual data processors to create their own framework without necessarily needing to adopt industry standard practices.[247] Without an overarching organization that can reconcile competing safety standards within an industry, the NIST Framework leaves open the door to competing standards[248] and causes significant uncertainty for both data subjects, who may be uncertain which standard is being applied, and other data processors, who are unsure whether or not their own standard is adequate when compared with others. Although the NIST Framework does require consideration of "industry best practices,"[249] it does not explain how those best practices should be determined or applied.[250]

Finally, since the goal of the NIST Framework is to guide data processor behavior, there is very little information pertaining to data subject rights. With exactly one appearance of the word "transparency,"[251] the NIST only mentions the rights of data subjects as one consideration in a larger data protection regime,[252] with no guarantees of data subjects being given notice, access, or rectification. Of course, this also means there are no means of redress considered within the text of the NIST Framework.

Instead, the rights of data subjects are enforced and protected by the FTC.[253] In order to truly see the interaction between the right of privacy and data protection in the United States, one need only examine the behavior of the FTC in recent years. Under the Federal Trade Commission Act,[254] the FTC is empowered to prevent "unfair methods of competition . . . and unfair or deceptive acts or practices,"[255]

---

244. This is similar to the GDPR's provisions allowing for Member States and industries to set their own codes of conduct, GDPR, *supra* note 62, art. 41, ¶ 1, except under the NIST Framework there is no underlying minimum of data protection guarantees.

245. *See* Tara Swaminatha, *The Rise of the NIST Cybersecurity Framework*, CSO (May 11, 2018, 10:20 AM), https://www.csoonline.com/article/3271139/data-protection/the-rise-of-the-nist-cybersecurity-framework.html [https://perma.cc/E9XS-FTX9].

246. NIST Framework, *supra* note 227, at 7–8.

247. *Id.* at 3.

248. *See generally* INTERNET SEC. ALL., THE CYBERSECURITY SOCIAL CONTRACT: IMPLEMENTING A MARKET-BASED MODEL FOR CYBERSECURITY (Larry Clinton & David Perera eds., 2016).

249. NIST Framework, *supra* note 227, at 11.

250. In fact, the NIST Framework actually declares that one of its goals is to determine industry best practices, leaving one to wonder which comes first: the NIST Framework or industry best practices. There is also some concern about whether or not NIST is even the appropriate agency to oversee data protection and cybersecurity regulations. *See* H.R. REP. NO. 115-376, at 25–26 (2017).

251. NIST Framework, *supra* note 227, at 19.

252. *Id.*

253. Balaban, *supra* note 23, at 13–16.

254. FTCA, *supra* note 231.

255. *Id.* § 45(a)(2).

which the FTC has used to enforce the privacy policy.[256] Considering the lack of guidance given by the NIST Framework with regard to informing data subjects, the FTC's authority and willingness to act in this area has been of paramount importance. Using their broad powers, the FTC has issued a number of consent decrees designed to define "acceptable data security practices"[257] In addition, they have brought more than sixty cases against companies whose practices have "put consumers' personal data at unreasonable risk."[258]

Taken together, both the NIST Framework and the powers of the FTC are able to provide at least some basic data protection for citizens of the United States. The NIST Framework itself truly focuses on proper data stewardship, rather than just data subject consent, an issue that the GDPR struggled to resolve. However, where the NIST Framework begins to fail is in defining harms and benefits for data processors. Using very vague language, it generally leaves data processors to determine their own systems of risk management and gives them very little guidance. Finally, while the FTC has undertaken to protect data subjects' privacy rights through their broad authority, ultimately, the United States needs a dedicated agency, like both the European Union and China, in order to ensure that personal data is being properly protected and data subjects' rights enforced.

CONCLUSION

Across the globe, governments have begun to realize that data protection is of vital importance as the internet grows. Different regions have attempted to regulate the behavior of data processors in different ways. In the European Union, data protection is seen as a fundamental right,[259] and so the GDPR focuses on protecting individual data subjects. In contrast, data protection in China is seen as one of many tools by which the government can protect social stability.[260] Finally, while the right to privacy has been recognized in the United States, the primary means for data protection has been self-regulation by data processors guided by the recommendations of the NIST.[261]

Each has its own advantages and disadvantages and can learn from the others. However, there are a few important lessons that the United States should try to learn from the other two jurisdictions with regard to its data protection regime and especially with regard to transparency and redress. First, the United States needs a dedicated data protection agency analogous to the Supervisory Authorities of the European Union[262] and the National Grid and Information Department.[263] Although the complete independence of such a body would ensure that the government doesn't exert undue influence over internet content, the United States tends to provide

256. Balaban, *supra* note 23, at 14.

257. Pardau & Edwards, *supra* note 226, at 256*; see also* FED. TRADE COMM'N, PRIVACY & DATA SECURITY: UPDATE: 2016 at 2 (2016) [hereinafter FTC Report 2016].

258. FTC Report 2016, *supra* note 257, at 4–5.

259. TFEU, *supra* note 65, art. 16.

260. *See* Buckley & Hornby, *supra* note 161.

261. NIST Framework, *supra* note 227.

262. GDPR, *supra* note 62, arts. 51, 58.

263. Network Security Law, *supra* note 163, art. 51.

government oversight for its various agencies. But as it stands, there is doubt as to whether NIST can determine adequate guidelines and whether the FTC is the appropriate agency to enforce data protection rights.[264]

In addition, the United States can also learn from China and Europe with regard to enumerating harms and benefits from data processing. Currently, the NIST Framework leaves it up to data processors themselves to develop a system of managing harms and benefits but gives almost no guidance regarding how to do so, which leaves data processors unsure what will or will not be acceptable.[265] As previously mentioned, data processors must be made aware of potential harms and benefits that can be achieved by data processors so that they can properly tailor their behavior to suit the risks.[266]

But the United States need not change its regime entirely. In fact, both Europe and China can learn from the United States' approach to data stewardship. Although having oversight and regulations for proper collection of information is important,[267] the real burden should be on data processors to properly protect and use personal data.[268] In this way, the NIST Framework excels, placing a great burden on data processors to "[d]evelop and implement the appropriate safeguards."[269] Both Europe, where the law has a strong focus on consent of the data subject,[270] and China, where the law is vague regarding proper processing,[271] could benefit from implementing some NIST-style principles.[272]

Overall, while no single data protection regime adequately fulfills the three-element framework set out by this article, each tackle the issue in a different way and can learn from each other. In the future, it is likely that the United States will attempt to implement a national data protection law,[273] following the global trend. When it

---

264. *See* H.R. REP. NO. 115-376, AT 25–26 (2017); *cf.* U.S. Telecom. Ass'n v. FCC, 855 F.3d 381, 417 (D.C. Cir. 2017) (Kavanaugh, J., dissenting) (suggesting that, if confirmed to the Supreme Court, Judge Brett Kavanaugh would not be in favor of the broad expansive powers and authority that the FTC has undertaken and would likely attempt to limit the FTC's power in the field of cybersecurity, since Congress has not expressly granted it such power).

265. A similar vagueness problem that plagues China's Network Security Law, although that law does at least enumerate some harms and benefits. *See supra* note 174 and accompanying text.

266. *See* CTR. FOR INFO. POLICY LEADERSHIP, *supra* note 45.

267. *See* Cate, *supra* note 8, at 15; *see also* FED. TRADE COMM'N, *supra* note 28, at 21; WHITE HOUSE BIG DATA REPORT, *supra* note 21, at 66–67; Balaban, *supra* note 23, at 8–11; Bignami, *supra* note 23 at 820–22; Schwartz, *supra* 16, at 1679–80.

268. *See supra* Section I.A.

269. NIST Framework, *supra* note 227, at 7.

270. *See* text accompanying notes 91–94.

271. *See* Ramsey & Wootliff, *supra* note 202; *UN Rights Chief Concern*, *supra* note 190.

272. Particularly the focus on proper data stewardship and uses in which the NIST Framework excels. *See supra* text accompanying notes 239–43.

273. In fact, the United States Senate has recently considered more national laws, but one did not progress very far before falling flat and the other has yet to progress in Congress. Tim Peterson, *WTF Is the CONSENT Act*, DIGIDAY (Apr. 17, 2018), https://digiday.com/media/what-is-the-consent-act/ [https://perma.cc/DH8X-3D9N]; *see also* Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES (Feb. 27, 2015), https://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data

does so, it should look not only at its own laws but at those of both the European Union and China so that it can learn from their mistakes and help bring about a more secure and globalized internet.[274]

-privacy-bill.html?_r=0 [https://perma.cc/BBJ5-X35L].

274. *See* Moshell, *supra* note 47, at 388–421.