NOTE

WHAT'S YOUR PRIVACY WORTH ON THE GLOBAL TECH MARKET?

WEIGHING THE COST OF PROTECTING CONSUMER DATA AGAINST THE RISK THAT NEW LEGISLATION MAY STIFLE COMPETITION AND INNOVATION DURING THIS GLOBAL, TECHNOLOGICAL REVOLUTION.

Sydney Wolofsky[*]

ABSTRACT

The world is currently in an artificial intelligence ("AI") arms race, whereby the first nation to develop AI will become the global super nation. That country will set the precedent for generations of future economic, technological, medical, and societal growth. While companies like Facebook, Google, and Amazon have propelled the United States to the front of this race for AI dominance, corporations have over-stepped ethical norms of data gathering and processing: methods necessary for technological development. Numerous data privacy breaches have left some consumers unlikely to ever share their data willingly without some assurances of protection. Noting these corporate scandals and data's potential for abuse, many countries have implemented data privacy laws to protect consumers. Statutes enacted for this purpose include the European Union's ratification of the General Data Protection Regulation ("GDPR"), the United States' various local statutes, and China's cybersecurity law ("CSL") and its Personal Information Security

* J.D. Candidate, 2022, Fordham University School of Law; B.S., 2019, Tulane University; Managing Editor, *Fordham International Law Journal*, Volume 45. I would like to thank Professor Olivier Sylvain for his guidance, as well as the board and staff members of the *Fordham International Law Journal* who edited this Note. I would especially like to thank Scott Mueller, Josh Diamond, Suzi Diamond, and my parents, Moira and Jon Fiore, for their continued support and guidance, and without whom this Note would not exist. The words "thank you" are not enough to express my gratitude.

Specification ("2018 Specification"). This Note argues that enacting wide-spread legislation as a means of protecting consumer data will cause more problems than it solves. Over-legislating technology will threaten innovation as tight-leashed constraints on development hinder growth. The consequences to a nation's global stance in this race to innovate are tantamount to individuals' privacy interests. The real battle will be treading the line between protecting citizens' privacy while facilitating technological growth. After examining the flaws with the GDPR, the CSL, and the 2018 Specification, this Note urges the United States to enact a federally binding data privacy statute, incorporating some principles found within various pieces of legislation, that strikes a balance between protecting consumer data privacy and enabling technological innovation.

I. INTRODUCTION TO DATA PRIVACY AND REGULATORY PROTECTIONS

Every day, over four billion people use the internet, spending over US$2.84 trillion in sales, and conducting over five billion Google searches.[1] Every click, like, view, post, share, and search internet users conduct generates data. Companies collect and process this data to help them better understand their clientele, provide their users a more tailored experience, and develop their technology.[2] Data collection benefits businesses who can, through gathering methods, grow and adapt their practices based on the data-driven insights they obtain.[3] From those insights, companies learn how best to market their products by analyzing consumer behavior and targeting product services toward specific groups.[4] While this is an undeniably helpful asset for corporations and

1. *See* Grace Park, Note, *The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act*, 10 U.C. IRVINE L. REV. 1455, 1459 (2020) (citing *Internet Stats & Facts (2021)*, WEBSITE SETUP, https://websitesetup.org/news/internet-facts-stats/ [https://perma.cc/N3YB-Q6M5] (last visited Feb. 15, 2021)).

2. *See Why Data is Important for Your Business*, GROW (Mar. 9, 2020), https://www.grow.com/blog/data-important-business [https://perma.cc/T7QQ-3BDT].

3. *See id.*

4. *See* DELOITTE, THE ANALYTICS ADVANTAGE WE'RE JUST GETTING STARTED 6 (2013).

consumers searching for certain products,[5] individuals fear data-gathering practices intrude upon their privacy rights.[6] Further, through analyzing customer behavior and utilizing targeted ads, data-gathering algorithms either purposely or inadvertently place consumers in echo chambers, fueling misinformation and dangerous self-serving beliefs.[7]

Though the echo chamber-producing results are less than ideal, technology—especially artificial intelligence ("AI")—is essential to societal advancement. As a result, countries throughout the world are currently in an artificial intelligence arms race, whereby the nation that develops AI superintelligence first will likely become *the* global super nation.[8] That country will be responsible for driving future economic, technological, medical, and societal growth.[9] The type of AI referred to here and through this Note is artificial general intelligence ("AGI"). Existing AI finds patterns and makes predictions based on those patterns.[10] AGI, in contrast, refers to human-like reasoning which includes the ability to make causal predictions.[11] While pattern and causal predictions may sound the same, causal predictions involve counter-factual reasoning about multiple hypothetical

5. *See* discussion *infra* Section II.A (discussing the Author's experience searching for a product for hours before an Instagram advertisement showed her exactly what she was searching for and where to find it).

6. *See* Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RES. CTR. (Feb. 19, 2016), https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ [https://perma.cc/AE6T-53AW] ("Our surveys show that people now are more anxious about the security of their personal data and are more aware that greater and greater volumes of data are being collected about them. The vast majority feel they have lost control of their personal data, and this has spawned considerable anxiety. They are not very confident that companies collecting their information will keep it secure.").

7. *See* discussion *infra* Section II.A (explaining what targeted advertising is, how it works, and how it places consumers in echo chambers).

8. *See* Indermit Gill, *Whoever Leads in Artificial Intelligence in 2030 Will Rule the world World Until 2100*, BROOKINGS (Jan. 17, 2020), https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/ [https://perma.cc/6BDS-645F].

9. *See id.*

10. Telephone Interview with Scott Mueller, PhD. Candidate, UCLA (Oct. 10, 2019); *see also* Hal Hodson, *DeepMind and Google: the Battle to Control Artificial Intelligence*, ECONOMIST (Mar. 1, 2019), https://www.economist.com/1843/2019/03/01/deepmind-and-google-the-battle-to-control-artificial-intelligence [https://perma.cc/H758-ZTUQ].

11. *See id.*

scenarios that meaningfully differ from observed patterns.[12] Consequently, whichever nation develops this type of AI first will likely become *the* global super nation.[13] That country will be responsible for driving future economic, technological, medical, and societal growth.[14] While this boost to notoriety may not happen overnight, even inching closer toward AI superintelligence can have a remarkable impact on a country's well-being.[15]

Still, some countries are currently struggling with the dissonance of wanting to promote innovation and advancing their nation in the technological arms race while protecting their citizens' data privacy from potentially data-abusing corporations. This "protection" will have consequences equally as threatening to a nation's global stance in this race to innovate as exposure does to individuals' privacy interests. The real battle will be treading the line between protecting citizens' privacy and facilitating technological growth.

In this race for AI dominance, many companies have over-stepped ethical norms of data gathering and processing, and their actions threaten consumer privacy and data security. These data breaches, including the Facebook Cambridge Analytica scandal,[16] have left some consumers unlikely to ever share their data willingly without some assurances of protection.[17] Noting these corporate scandals and their potential for user data privacy abuse, many countries have implemented data privacy laws to protect consumers. Statutes enacted for this purpose include the European Union's ratification of the General Data Protection Regulation ("GDPR")[18], the United States' various local statutes,[19]

12. *See id.*
13. *See* Gill, *supra* note 8.
14. *See id.*
15. *See id.*
16. *See* Facebook Cambridge Analytica scandal analysis, *infra* Section II.A.5.
17. Data privacy scandals are examined in more detail *infra* Section II.A.
18. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].
19. *See* discussion *infra* Section III.B (referencing examination of various pieces of US legislation, including analysis of the California Consumer Privacy Act, the Data Privacy Act, and the Consumer Online Privacy Rights Act).

and China's cybersecurity law ("CSL")[20] and its Personal Information Security Specification ("2018 Specification").[21] Racing to legislate privacy protections may seem logical in the wake of serious abuses of data privacy, but this Note argues that over-legislation threatens technological innovation as tight-leashed constraints on development hinder growth. Among countries without privacy protections, one nation stands out: China.

China is a notorious surveillance state, monitoring its citizens' every move as a means of providing governmental protection as well as gathering information.[22] Chinese laws have historically offered citizens significantly fewer privacy protections than those of other nations.[23] The country's new CSL and 2018 Specification, however, seem to offer stronger security against data threats than US policies. These laws center around consumer rights; providing customers with protections against harmful private business practices.[24] These laws, however, do not restrict the Chinese government's access to private data.[25] Further, these new laws seem to offer Chinese citizens the privacy rights desired by American consumers.[26] A more thorough examination of the

20. *See* Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, NEW AM. (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ [https://perma.cc/5ZC7-YUQG].

21. *See* Mingli Shi et al., *Translation: China's Personal Information Security Specification*, NEW AM. (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/ [https://perma.cc/XZ2C-CZ6F].

22. *See* Anna Mitchell & Larry Diamond, *China's Surveillance State Should Scare Everyone*, ATL. (Feb. 2, 2018), https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ [https://perma.cc/N7PX-GRQA].

23. *See* Xiaofeng Lin, Note, *A Dangerous Game: China's Big Data Advantage and How the U.S. Should Respond*, 2020 U. ILL. J. L. TECH. & POL'Y 253, 266 (2020) (referencing James D. Fry, *Privacy, Predictability, and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. PA. J. INT'L L. 419, 440 (2015)).

24. *See* discussion *infra* Section III.C.

25. *See* Bojan Pancevski, *U.S. Officials Say Huawei Can Covertly Access Telecom Networks*, WALL ST. J. (Feb. 12, 2020, 8:41 AM), https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256 [https://perma.cc/5F9Y-3MYW] (referring to China's laws requiring corporations to disclose private information to the government at its request).

26. *See* Deep Tech, *Podcast: Want Consumer Privacy Rights? Try China*, MIT TECH. REV. (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1007425/data-privacy-china-gdpr/ [https://perma.cc/5GCA-UBNW].

two statutes, however, reveals the acts focus more on national security concerns than on individual rights.[27] Still, the CSL and 2018 Specification are more comprehensive than anything the United States has enacted, though they are less stringent than the GDPR.

In this sliding scale approach to legislation, the European Union sits at one end aggressively protecting consumer privacy rights to the detriment of technology-driven businesses.[28] China sits on the other end with nation-wide privacy protections deterring private entities from gathering data without consent but allowing the government and military to do so freely. Where the United States lies on this privacy spectrum remains to be seen. With no federal data privacy statute in effect, the United States offers fewer national protections than the world's most surveilled country.[29] Considering its dominance in the technology field, the world will be watching to see how the United States handles increasing demands for data security while maintaining its position in the race for technological dominance.

This Note explores emerging legislation in various jurisdictions tackling the issue of unchecked data collection by private companies, and whether such legislation harms technological growth and innovation. Part II explains what data is and defines key terms necessary to understand the impact data usage has on society. It explains why data is so valuable while examining how sharing consumer data with several organizations has come under fire lately. Part III explains the various legislative approaches nations have taken to protect data privacy. First, it examines the European Union's adoption of the GDPR and analyzes what GDPR compliance entails. Then, it explains the various statutes in force in the United States, while noting that the country lacks a federally-binding data privacy statute. Next, it discusses how the Federal Trade Commission ("FTC") and several states are unevenly enforcing consumer data-protection in

27. *See* Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect [https://perma.cc/YQ84-4D5Z].

28. *See* discussion *infra* Section IV.A.

29. *See* Matthew Keegan, *The Most Surveilled Cities in the World*, U.S. NEWS (Aug. 14, 2020, 2:11 PM), https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world.

America. Finally, it ends with an evaluation of China's two most distinct regulations regarding data privacy: the CSL and the 2018 Specification.

Part IV explores what a US federally-binding data privacy statute should include drawing from the successful aspects of the GDPR, CCPA, CSL, and 2018 Specifications. In doing so, this Part examines the GDPR's shortcomings and how the law can be harmful to technological innovation. Overall, Part IV analyzes the impact of each response nations have undertaken in trying to combat data-privacy misuse. It argues that while the United States needs federal data protection, a GDPR-sized statute may stifle competition too much to maintain the United States' position in the tech arms race. Ideally, corporations would have more transparent privacy practices, encouraging consumers to feel more comfortable with sharing their data. One possible solution is introducing legislation that requires corporations to use only explainable AI practices.[30] These corporations would also have to obtain consent from consumers before using their data and to re-obtain consent upon any changes to the agreed-upon data usage. The Note concludes by arguing that the United States can reconcile the competing interests of consumers, corporations, and the government with a federal privacy statute that contains clear and concise compliance obligations.

II. WHAT DATA IS AND WHY COMPANIES GO TO SUCH GREAT LENGTHS TO OBTAIN YOURS

Data collection is a powerful tool capable of driving technological innovation far beyond what man could do without AI processors. Through data collection, companies have created self-driving cars that accumulate vast amounts of digitized images to improve vision recognition software.[31] International Business Machine's Watson also uses AI to analyze digital research records.[32] In only two months, Watson has found six new cancer suppressors: a feat that would have taken scientists years to

30. *See* discussion *infra* notes 357-360 and accompanying text defining "explainable AI."

31. *See* Lynn Wu, *How Data Analytics Can Drive Innovation*, KNOWLEDGE@WHARTON, (Sept. 17, 2019), https://knowledge.wharton.upenn.edu/article/data-analytics-innovation/ [https://perma.cc/8XYK-FX8Y].

32. *See id.*

achieve.[33] In addition to medicine, data has also aided advancements in ecology,[34] oceanography,[35] and scientific processes.[36] Of the many types of data,[37] personal data refers to identifiable information like an individual's name, address, phone number, employment location, credit card information, social security number, and more.[38] The term "data privacy" describes the pertinent use of an individual's information in a given situation, in light of the expectations of the law, the individual, and the right to control use and disbursement of that data.[39] Through using an entity's servers, users who accept its privacy policy allow the server to collect their data, thus willingly exchanging their data privacy for favorable services. For example, users' disclosure of personal data allows them to activate and use the internet and social media accounts.[40] By gaining control over consumers' personal data, companies can enter a user's behavior and demographic characteristics into an algorithm that then informs the company how best to adapt their services to meet and exceed client demands.[41] The more data a company has, the more it can tailor its services to a particular demographic and improve its products.[42] This, in turn, attracts more users which generates

33. *See id.*

34. *See* Lin, *supra* note 23, at 262 (referencing James R. Hunt et al., *Redefining Ecological Science Using Data*, *in* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 21, 21 (Tony Hey et al. eds., 2009)).

35. *See* Lin, *supra* note 23, at 262 (recognizing John R. Delaney & Roger S. Barga, *A 2020 Vision for Ocean Science*, *in* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 27, 27 (Tony Hey et al. eds., 2009)).

36. *See* Lin, *supra* note 23, at 263 (referencing Mark R. Abbott, *A New Path for Science?*, *in* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 111, 111 (Tony Hey et al. eds., 2009)).

37. This Note will only examine personal data.

38. *See generally* Park, *supra* note 1.

39. *See* Park, *supra* note 1, at 1458 (citing *What Does Privacy Mean?*, IAPP, https://iapp.org/about/what-is-privacy/ [https://perma.cc/KQ3M-GGQH] (last visited Feb. 15, 2021)); *see also Data Privacy vs. Data Protection: Understanding the Distinction in Defending Your Data*, FORBES (Dec. 19, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#58bfba1150c9 [https://perma.cc/LH8P-T6PH].

40. *See* Park, *supra* note 1, at 1459.

41. *See* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY (June 17, 2020), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/C3BZ-HF3H].

42. *See The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-

more data and continues the process.[43] Data collection is incredibly valuable to technology companies because data, as the primary input of AI technology, drives the rise and advancement of AI.[44] In 2016 alone, people produced as much data as had been produced in all of history through 2015, proving that there is ample data available for processing.[45] Accordingly, access to this abundant data will be crucial for companies hoping to compete in the AI arms race.[46]

While data can serve many useful functions, there are unwelcomed consequences of data collection. Because online data processing relies on such vast amounts of data from countless online actors, processors often use consumer data without first obtaining the owner's consent.[47] A server can obtain consent in one of two ways: (1) the user can willingly disclose their data to a company, often by agreeing to a server's terms of use or privacy policies, [48] or (2) through indirect means of disclosure such as mining data through use of cookies, web bugs, tracking software, or monitoring IP addresses.[49] Some find firms' profiling of users to be a privacy rights violation but insist that if individuals want to continue using a processor's services, the individual does not have

---

resource-is-no-longer-oil-but-data [https://perma.cc/UF97-FZ6V]. *See also* Park, *supra* note 1, at 1460 (citing Nancy S. Kim & D.A. Jeremy Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent*, 80 MO. L. REV. 723, 729 (2015)).

43. *See The World's Most Valuable Resource Is No Longer Oil, but Data*, *supra* note 42.

44. *See* Lin, *supra* note 23, at 262 (referencing Cade Metz, *As China Marches Forward on A.I., the White House Is Silent*, N.Y. TIMES (Feb. 12, 2018), https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html [https://perma.cc/EX3K-7YBS]).

45. *See id.* at 254 (citing Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 25, 2017), https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ [https://perma.cc/U9TX-XLKE]).

46. *See* Clay Chandler, *How China's Rise as AI Superpower Could Reshape the World*, FORTUNE (Sept. 26, 2018, 8:49 AM), http://fortune.com/2018/09/26/china-ai-superpower-book-review/ [https://perma.cc/U73U-7ZNJ].

47. *See* Lita van Wel & Lambèr Royakkers, *Ethical Issues in Web Data Mining*, 6 ETHICS & INFO. TECH. 129, 129 (2004), https://cdn.tc-library.org/Rhizr/Files/FkE9DdrKdtH7PAQaw/files/124601.pdf [https://perma.cc/3ZEN-BUSZ].

48. Park, *supra* note 1, at 1459 (citing CLARA RUYAN MARTIN & DAVID B. OSHINSKY, INTERNET LAW & PRACTICE IN CALIFORNIA § 9.3(1) (2019)).

49. *See* Park, *supra* note 1, at 1460 (citing MARTIN & OSHINSKY, *supra* note 48, § 9.4(2)).

much choice in allowing the firm to continue mining their data.[50] In theory, consenting to these practices is simple: if a user does not want their data mined, they should not use these platforms. In reality, opting-out of certain services becomes much more complicated. As social media advances society, lack of participation may leave individuals feeling left behind. Through these websites and applications, people are finding new means of connecting with one another that seemed impossible only a decade ago.[51] From connecting with friends that users have not seen in years, to finding long-lost relatives and even locating missing pets, the internet can be a force for good. Social media "groups," likes those Facebook allows user to create, have encouraged participants to form support groups and have even found organ donors for patients in need, not to mention the hours of enjoyment users gain from browsing these sites.[52]

With all the benefits that social media affords, some users, however, have become the unwitting targets of unsolicited advertising and data mining. Some companies' failure to implement sufficient privacy policies protecting personal data not only worries users but also enables companies to profit from the misuse of user data.[53] Lately, data collection has come under intense scrutiny from several governments as well as consumers due to corporate mishandling of classified information and unethical data practices.[54] The public, as a result, has begun pressuring the government into implementing legislation to protect consumer privacy rights.[55]

---

50. *See* Park, *supra* note 1, at 1473 (citing Joseph A. Tomain, *Online Privacy and the First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 3-4 (2014)).

51. *See infra* text accompanying note 54.

52. *See* THE SOCIAL DILEMMA (Exposure Labs 2020), https://www.thesocialdilemma.com [https://perma.cc/D5JY-XDQ4].

53. *See* Park, *supra* note 1, at 1457 (citing Justin McCarthy, *Worries About Personal Data Top Facebook Users' Concerns*, GALLUP (Apr. 12, 2018), https://news.gallup.com/poll/232343/worries-personal-data-top-facebook-usersconcerns.aspx [https://perma.cc/NE23-FKPU]); *see also* Brian Byer, *Internet Users Worry About Online Privacy but Feel Powerless to Do Much About It*, ENTREPRENEUR (June 20, 2018), https://www.entrepreneur.com/article/314524 [https://perma.cc/AME8-2V6U].

54. *See* discussion *infra* Section II.A.

55. Current US data policies are discussed in depth in Part II of this Note. *See* Park, *supra* note 1, at 1457 (referring to PUBLIC OPINION ON PRIVACY, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/survey/ [https://perma.cc/ZPS4-WS5L] (last visited Mar. 1, 2021)).

A. Notorious Corporate Data Breach Scandals

1. Google is Infested with Data-Mining Bugs

In October of 2018, Google announced plans to shut down Google+—Google's attempt at providing a social network service—after learning of a "bug" whereby external hackers exploited Google's software, exposing 500,000 users' data during a three-year period.[56] Months later, Google found another bug in a Google+ API[57] which exposed 52.5 million users' data that these data owners had not made publicly available, including private messages between users.[58] David Kennedy, the CEO of TrustedSec (an information security advisory service company), stated that the Google breach "didn't impact passwords or financial data, but it did give [Google] the ability to extract large amounts of information like email addresses and profile data."[59] While exposing user data is never good, Kennedy realized this exposure is one risk companies continuously take as they race to provide to consumers the newest, most advanced technologies on the market.[60] Further, Kennedy, along with other critics, felt Google's quick detection in the aftermath of the October incident was "heartening" as it signified Google's active monitoring measures even in a program it planned on shutting down in mere days.[61] In his statement, Kennedy referred to the six days it took Google to detect and consolidate the November security breach as opposed to the three years it took them to announce the previous breach.[62]

While Google's failure to report the initial security breach until three years after it began was not illegal, it did leave many

56. *See* Lily Hay Newman, *A New Google+ Blunder Exposed Data From 52.5 Million Users*, WIRED (Dec. 10, 2018, 2:19 PM), https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/ [https://perma.cc/U9JF-3SKU].

57. "APIs are sets of requirements that govern how one application can talk to another . . . APIs are what make it possible to move information between programs—for instance, by cutting and pasting a snippet of a LibreOffice document into an Excel spreadsheet." Brian Proffitt, *What APIs Are and Why They're Important*, READWRITE (Sept. 19, 2013), https://readwrite.com/2013/09/19/api-defined/ [https://perma.cc/XE7M-876P].

58. *See* Newman, *supra* note 56.

59. *Id.*

60. *See id.*

61. *See id.*

62. *See id.*

wondering why Google did not come forward sooner.[63] Critics felt the company's failure to disclose not only threatened the data privacy of millions of users, but also cast doubt on Google's allegiance to its consumers, alleging Google did not disclose the breach for fear of embarrassing the company.[64] Steven Andrés, a management information systems professor at San Diego State University, acknowledged the lack of a legal requirement to disclose the software vulnerabilities, but found it "troubling—though unsurprising" that the company was more concerned with appearances if it chose to report.[65] Because Google's failure to disclose the breach was not illegal, and because it reported finding no evidence that "any user profiles were touched,"[66] some find no fault with Google's silence. Arvind Narayanan, a Princeton University computer science professor, is often critical of tech companies' flawed privacy practices.[67] Regarding Google, however, Narayanan tweeted that companies often fix problems before they are exploited and that internally discovering and immediately fixing software issues happens "thousands of times every year."[68] For that reason, Narayanan feels new laws requiring disclosure of every threat would be "totally counterproductive."[69]

2. Capital One: What's in Your Data?

While the 2018 Google data privacy violation showed how external hackers can threaten data privacy, a 2019 Capital One server breach proved internal actors can be just as dangerous. In March 2019, Capital One servers suffered a data breach which exposed personally-identifying information of millions of the bank's customers.[70] The United States Department of Justice

63. *See id.*

64. *See id.*

65. Daisuke Wakabayashi, *Google Plus Will Be Shut Down After User Information Was Exposed*, N.Y. TIMES (Oct. 8, 2018), https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html [https://perma.cc/CGX9-5M4N].

66. *Id.*

67. *See id.*

68. *Id.*

69. *Id.*

70. *See* Rob McLean, *A Hacker Gained Access to 100 million Capital One Credit Card Applications and Accounts*, CNN BUS. (July 30, 2019, 5:17 PM), https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html [https://perma.cc/VE3N-3PPC].

reported that the breach gave hacker Paige Thompson access to 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers, and 80,000 bank account numbers.[71] Additionally, Thompson accessed an unknown number of customers' personal information such as names, addresses, credit scores, credit limits, balances, and more.[72] Capital One stored the personal data on external Amazon servers.[73] Thompson, a former Amazon tech software engineer familiar with the technology, was able to hack into Amazon's servers by exploiting a "misconfigured web application firewall."[74] In a statement, Thompson explained she used a command to extract files Capital One had stored on Amazon servers.[75] Capital One claims to have fixed the vulnerability and does not feel the information gained was used for fraud or shared with third parties.[76] While Capital One has taken steps to fix the server weaknesses and has worked with customers to restore their losses, many feel the hack demonstrates the dangers of companies relying on authorized third parties when securing sensitive data.[77]

3. TikTok's Data Flops

While internal hackers can pose an existential threat to corporations, sometimes company practices alone threaten users' safety and data. The targeting of children in corporate data collection and sharing practices compounds user fears of data security breaches.[78] On February 27, 2019, TikTok's[79] parent

71. *See id.*
72. *See id.*
73. *See id.*
74. *Id.*
75. *See id.*
76. *See id.*
77. *See* Hannah Murphy & Shannon Bond, *Capital One Data Breach Sparks Cloud Security Fears*, FIN. TIMES (July 30, 2019), https://www.ft.com/content/5b3046ca-b2d4-11e9-bec9-fdcab53d6959 [https://perma.cc/R4AH-89LP]; *but see* LILLIAN ABLOM, PAUL HEATON, DIANA CATHERINE LAVERY & SASHA ROMANOSKY, CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION (RAND Corp. 2016) (noting that the vast majority of data breaches are discovered by third parties, rather than the affected company).
78. *See* Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 17, 2014, 1:32 PM), https://www.politico.com/story/2014/05/data-mining-your-children-106676 [https://perma.cc/CTY8-FG4G].
79. TikTok is a social media app that allows users to upload short video clips, usually involving songs and popular dance trends. It rapidly grew in popularity, surpassing other

company, ByteDance, responded to allegations that TikTok illegally collected the data of minors and agreed to pay the FTC a US$5.7 million settlement.[80] The excessive fines imposed on the social media company were not solely a response to the data abuses, but to penalize the company for unlawfully targeting children.[81] Companies' collection of data or information from children under thirteen years old without parental permission violates the United States' Children's Online Privacy Protection Act of 1998 ("COPPA").[82] The issue with allowing children on TikTok, according to one reporter, is that children rarely understand the complexities or necessities of privacy.[83] FTC Chair Joe Simons admitted that the operators of TikTok knew children used their app, but continued to collect personal information from their accounts without seeking parental consent before doing so.[84] While TikTok has paid the US$5.7 million FTC fine, as of May 2020, children's advocacy groups continue to criticize TikTok for failing to take down child-created content as promised under the February 2019 FTC agreement.[85] These advocacy groups claim the company still unlawfully collects information from children's accounts and shares that data with third parties for advertising purposes.[86]

TikTok has also faced other serious allegations over data security breaches within the app. According to Israeli cybersecurity company CheckPoint, the app has "serious vulnerabilities" that can afford hackers access and control over user data, revealing personal information.[87] These weaknesses

popular social media sites such as Snapchat and Twitter in app store downloads by only its second birthday. *See* Chavie Lieber, *TikTok has Been Illegally Collecting Children's Data*, VOX (Feb. 28, 2019, 2:50 PM), https://www.vox.com/the-goods/2019/2/28/18244996/tiktok-children-privacy-data-ftc-settlement [https://perma.cc/M2YC-6YYW].

80. *See id.*

81. *See id.*

82. 15 U.S.C.S. § 6501 (Lexis Advance through Pub. L. No. 116-158).

83. *See* Lieber, *supra* note 79.

84. *See id.*

85. *See Advocacy Group Says TikTok Violated FTC Consent Decree and Children's Privacy Rules*, REUTERS (May 14, 2020), https://www.reuters.com/article/idUSL1N2CV2LV [https://perma.cc/K52B-CYDE].

86. *See id.*

87. Ronen Bergman, Sheera Frenkel & Raymond Zhong, *Major TikTok Security Flaws Found*, N.Y. TIMES (Jan. 08, 2020),

would have enabled hackers to reach TikTok users by sending messages with malicious links that, once opened, would grant the hackers control over the accounts and their content (including private videos).[88] CheckPoint tested these alleged vulnerabilities and found they were able to send themselves malware infested links that gave them complete access to others' accounts.[89]

In addition to private sector data privacy concerns, the Trump administration has also faced internal data privacy concerns.[90] Throughout much of 2020, President Trump alleged that TikTok posed a threat to national security because of its ties to the Chinese government.[91] The President feared the app gathers data for the Chinese Communist Party to enable them to spy on American users.[92] TikTok denies allegations of both censorship and user data sales, though its privacy policies explicitly mention the distribution of user data to third-party sites.[93] While the Trump Administration's fears of data-gathering as a means of Chinese governmental surveillance may seem far-fetched, even xenophobic to some,[94] Chinese surveillance of American tech usage is nothing new.

---

https://www.nytimes.com/2020/01/08/technology/tiktok-security-flaws.html [https://perma.cc/AA66-H5B4].

88. *See id.*

89. *See id.*

90. *See* Selina Wang, *TikTok's US Ban Is On Hold. What Comes Next?*, CNN BUS. (Oct. 5, 2020), https://www.cnn.com/2020/10/05/tech/tiktok-what-next-intl-hnk/index.html [https://perma.cc/8ATA-HXTM].

91. Shirin Ghaffary, *Do You Really Need to Worry About Your Security on TikTok? Here's What We Know.*, VOX (Aug. 11, 2020, 10:00 AM), https://www.vox.com/recode/2020/8/11/21363092/why-is-tiktok-national-security-threat-wechat-trump-ban [https://perma.cc/MJ4P-8M7F].

92. *See* Wang, *supra* note 90.

93. *See* Bergman, *supra* note 87 (stating "American lawmakers have expressed concern that TikTok censors material that the Chinese government does not like and allows Beijing to collect user data. TikTok has denied both accusations."); *see generally TikTok Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/privacy-policy?lang=en [https://perma.cc/2VJW-EZ98] (last visited Oct. 8, 2020).

94. *See, e.g.*, Alexander Urbelis, *Trump's TikTok Worries Are Grounded in Xenophobia and Fear*, PHILA. INQUIRER (Aug. 04, 2020), https://fusion.inquirer.com/opinion/commentary/trump-tiktok-ban-china-microsoft-20200804.html [https://perma.cc/5FNW-WSZ7].

4. Huawei's Tele-miscommunication

For years, countries like the United States and Germany have opposed the domestic sale and use of Chinese tech company Huawei's products.[95] Government leaders cite Huawei as a grave threat to national security.[96] Countries fear the Chinese government can spy on Huawei-device owners through "backdoors" installed in Huawei electronic devices.[97] When referring to accessing a computer system or software, "backdoors" are "undocumented portal[s] that allow[] an administrator to enter the system to troubleshoot or do upkeep."[98] It can, however, also refer to "a secret portal that hackers and intelligence agencies use to gain illicit access [to a users' system]."[99] Many countries require telecom-equipment manufacturers to build in backdoors to information stored on devices for legitimate and lawful interception purposes.[100] In almost every nation, strict laws govern when and how governments may use these backdoors.[101] United States officials warn that Huawei devices can preserve access to networks without the carriers' knowledge or consent.[102] While Huawei has insisted that it has never spied on behalf of any country and would refuse a request to do so, Huawei's backdoors make it possible for the Chinese government to access user data.[103] Based on the country's laws,[104] if the Beijing government wanted such access, Huawei would be compelled to provide it.[105]

95. *See* Pancevski, *supra* note 25.

96. *See id.* (citing a confidential memo written by the German Foreign Office and posted in the Wall Street Journal providing "smoking gun" evidence that Huawei equipment posed a spying risk (to foreign governments and citizens)).

97. *See id.*

98. Kim Zetter, *Hacker Lexicon: What is a Backdoor?*, WIRED (Dec. 11, 2014, 6:35 AM), https://www.wired.com/2014/12/hacker-lexicon-backdoor/ [https://perma.cc/D2VR-JNBG].

99. *Id.*

100. *See* Pancevski, *supra* note 25.

101. *See id.*; *see also* discussion *infra* Part III.

102. *See* Pancevski, *supra* note 25.

103. *See id.*

104. *See infra* Section III.C.

105. *See* Pancevski, *supra* note 25 (referring to China's laws requiring corporations disclose private information to the government at its request).

5. Facebook Gets Political

Another danger in unchecked collection and misuse of user data is that parties can use the gathered data to manipulate users' future behaviors. In a targeted advertising campaign, an algorithm reviews a consumer's search trends and demographics to feed consumers products or information the algorithm determines consumers will find satisfactory.[106] Targeted advertising of products can be beneficial to both consumers and marketers. Without targeted advertising, searching the internet for a specific item can take hours or days before finding something remotely close to the search target. In contrast, data gathering applications like Instagram can comb through a user's searches, find the most closely related products to the search terms, and recommend the exact item for which the consumer spent hours searching.[107] For example, a consumer who searches for a red, cowl neck, silk dress may encounter an ad on the user's Instagram account advertising the exact dress sold at Nordstrom. The user purchases the dress while the manufacturer, Nordstrom, makes a sale thanks to Instagram's targeted advertising to a particular consumer.

While this experience is helpful, even desirable, the ads do not stop at clothing. Companies employing this practice collect consumers' information and draw conclusions about the consumers' demographics, which can then be used against the consumer through pointed advertising, swaying the consumers' opinions.[108] In this way, targeted advertising practices often lead to confirmation bias and providers placing unsuspecting consumers into echo chambers wherein consumers are shown affirmatory articles at the top of their search results, rather than relevant and factual information, even if these results do not align

106. *See* JOE PLUMMER, STEVE RAPPAPORT & TADDY HALL, THE ONLINE ADVERTISING PLAYBOOK: PROVEN STRATEGIES AND TESTED TACTICS FROM THE ADVERTISING RESEARCH FOUNDATION (John Wiley & Sons, Inc. ed., 1st ed. 2007).

107. *See id.*

108. *See* Rebecca Walker Reczek et al., *Targeted Ads Don't Just Make You More Likely to Buy — They Can Change How You Think About Yourself*, HARV. BUS. REV. (Apr. 4, 2016), https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself [https://perma.cc/9UMY-G4ZF]; *see also* Leslie K. John et al., *Ads That Don't Overstep*, HARV. BUS. REV. (Jan. 2018), https://hbr.org/2018/01/ads-that-dont-overstep [https://perma.cc/BT9R-6NWX].

with the user's views.[109] This negative feedback loop, created via the same traditionally helpful technology, fuels misinformation and leads to amplification of consumers' preconceived beliefs.

In 2014, political consulting firm Cambridge Analytica secured a US$15 million investment after persuading wealthy Republican donor, Robert Mercer, and his political advisor, Stephen Bannon, of its ability to sway the 2016 US presidential election in their party's favor.[110] Cambridge Analytica boasted psychoanalytic tools capable of identifying personality traits of American voters that could influence their behavior.[111] Cambridge Analytica planned to use the information obtained with these tools to inform targeted political advertising on the social media platform Facebook.[112] The new algorithm Cambridge promised to develop would specifically track users who were "more prone to impulsive anger or conspiratorial thinking than average citizens."[113] To obtain the necessary data to build this tool, the firm "harvested" privileged information from more than 50 million Facebook users' accounts without their permission.[114] Of the 50 million, approximately 270,000 users had consented to sharing their data.[115] That means only half of one percent of all Facebook users gave permission to Facebook to share the data with Cambridge Analytica. After illicitly gaining the necessary data to develop this tool, Cambridge used "various methods, such as Facebook group posts, ads, sharing articles or even creating fake Facebook pages to provoke these [easily angered] users."[116] Confirming what many Americans feared

109. *See* Giovanni Luca Ciampaglia & Filippo Menczer, *Biases Make People Vulnerable to Misinformation Spread by Social Media*, SCI. AM. (June 21, 2018), https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/ [https://perma.cc/U9XG-ZTCS].

110. *See* Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/K6V2-DNZL].

111. *See id.*

112. *See* Rosalie Chan, *The Cambridge Analytica Whistleblower Explains How the Firm used Facebook Data to Sway Elections*, BUS. INSIDER (Oct. 5, 2019, 5:53 PM), https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10 [https://perma.cc/N75W-SJN9].

113. Rosenberg et al., *supra* note 110.

114. *See id.*

115. *See id.*

116. Chan, *supra* note 112.

from big tech companies, one of Cambridge Analytica's founding members, Christopher Wylie, admitted in an interview that "[r]ules don't matter for [Big Tech company leaders]."[117]

Further, reviews of the firm's emails and documents revealed that as of March 2018, years later, Cambridge still possessed most or all of the wrongfully gathered data.[118] The data collected included users' potentially identifying information including name, address, email address, phone number, place of work, etc. The collected data also included users' networks, meaning other users with whom the original user has connected, or "friended," and reactions to posts their friends have shared, known as "likes."[119] Facebook's Deputy General Counsel stated that Cambridge Analytica certified that all data it had collected has since been destroyed.[120] Confirming this statement, however, may be near impossible since copies of the data remain beyond Facebook's control.[121] Aside from Cambridge Analytica not obtaining consent from the data's owners, an especially insidious problem with its targeted advertising practice is that it feeds consumers products, news stories, and social media posts that reflect the consumer's views, even if those views are deluded, conspiratorial, or hateful. Targeted advertising effectively prevents providing users with alternative, more credible perspectives.

III. LEGISLATIVE APPROACHES TO DATA-PRIVACY AND SECURITY IN THE EUROPEAN UNION, UNITED STATES, AND CHINA

Regarding data and technology, the European Union, the United States, and China have set different standards in the way of legislative protection.[122] The European Union has recently enacted one of the most expansive regulations in the data-privacy

117. Rosenberg et al., *supra* note 110.

118. *See id.*

119. *See id.*

120. *See id.*

121. *See id.*

122. Other nations have also enacted laws in the data-privacy area, however, the scope of this Note will be limited to examining data-privacy rights and legislation affecting the European Union, the United States, and China only.

field: the General Data Protection Regulation ("GDPR").[123] While the United States has some state-adopted statutes, neither the United States nor China have federally-binding laws protecting general consumer data.[124] Though nations around the world are racing to be the first to develop AI, two countries forge far ahead of the rest: the United States and China. Whoever wins this race will "define generations of technology to come."[125] Given the necessity of access to data in developing AI, Chinese companies appear to be better positioned to take the lead.

China's over 800 million "netizens,"[126]—active internet community participants—use their cell phones more actively than Americans do, thus creating more data on Chinese devices.[127] As of December 2019, China's 854 million internet users more than double America's 313 million users.[128] Further, China's plans to develop their AI include investing US$7 billion in the industry by 2030.[129]

The European Union is also investing significantly in the field, pledging US$24 billion in a two-year period.[130] While the United States has not discussed its plans, it is currently the world leader in technological development.[131] Additionally, while China may have the highest number of data contributors, [132] Americans still contribute the greatest amount of online content to the internet.[133] Consumers may fear, however, that nations' push to innovate will encourage governments to allow developers almost unfettered use of private data to advance their respective nation's

123. GDPR, *supra* note 18.

124. *See* discussion *infra* Section III.B-C.

125. Dave Gershgorn, *Forget The Space Race, The AI Race Is Just Beginning*, WORLD ECON. F. (May 8, 2018), https://www.weforum.org/agenda/2018/05/ai-is-the-new-space-race [https://perma.cc/MP82-H7UT].

126. *Netizen*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/netizen [https://perma.cc/45YN-YJ5C] (last visited Oct. 23, 2020).

127. *See* Chandler, *supra* note 46.

128. *See* J. Clement, *Countries with the highest number of internet users as of December 2019*, STATISTA (June 25, 2020), https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/ [https://perma.cc/LEH2-5UFC].

129. *See* Gershgorn, *supra* note 125.

130. *See id.*

131. Metz, supra note 44.

132. *See* Clement, *supra* note 128.

133. Generating online content contributes highly to data creation and development.

global stance. On the other hand, technology experts and developers worry over-legislation, to protect consumer data privacy, will stifle competition and innovation.[134]

The United States currently has bills pending before Congress calling for greater enforcement of data-privacy protections,[135] but China's authoritarian regime will likely never codify generalized privacy rights. Some technology experts credit this lack of regulation for rapid advancements in technology, especially during the internet's naissance.[136] This Part will discuss nations' legislative approaches to combatting data-privacy abuses by analyzing various pieces of legislation that have been either introduced or enacted as a response to data privacy breaches.

A. The European Union Enacts One of the Most Comprehensive Data-Privacy Laws: The GDPR

According to Article 16(1) of the Treaty on the Functioning of the European Union ("TFEU"), the GDPR emerged out of necessity from its predecessor, the 1995 European Union Data Protection Directive ("1995 Directive"), [137] due to the "rapidly changing landscape in data storage, collection, and transfer." [138] In light of the TFEU's mission to establish that data privacy protection is a fundamental right,[139] the GDPR aims to "strengthen, unify, and make more coherent data protection laws and its framework across the twenty-seven European Union member states."[140]

---

134. *See* Zen Soo, *Alibaba's Jack Ma says he is 'worried' Europe will stifle innovation with too much tech regulation*, SOUTH CHINA MORNING POST (May 17, 2019), https://www.scmp.com/tech/big-tech/article/3010606/alibabas-jack-ma-says-he-worried-europe-will-stifle-innovation-too [https://perma.cc/JG5S-2QB9].

135. *See* discussion *infra* Section III.B (discussing the Consumer Online Privacy Rights Act ("COPRA") and the Digital Accountability and Transparency to Advance Privacy Act ("Data Privacy Act") as examples of some of the bills pending before Congress).

136. *See* Soo, *supra* note 134.

137. Directive 95/46/EC, 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, art. 25, 1995 O.J. (L 281) [hereinafter Directive 95/46/EC].

138. GDPR, *supra* note 18; *accord* Park, *supra* note 1, at 1466.

139. Park, *supra* note 1, at 1465 (citing Treaty on the Functioning of the European Union, art. 16, Dec. 13, 2007, 2012 O.J. (C 326), 1).

140. Park, *supra* note 1, at 1467 (citing GDPR, *supra* note 18, arts. 7, 9, 10).

The pre-GDPR European Union hoped to solve what is currently the United States' main issue: numerous state-level regulations establishing independent policies, rather than a unified, federally binding statute. This issue and subsequent ideal of a single unifying piece of legislation is precisely why the European Commission replaced the 1995 Directive with the GDPR.[141] In doing so, the European Commission had two goals in mind: (1) fixing the imbalance of competition created through varying legislation across the European Union, and (2) reinforcing its implementation to bolster compliance with the European Union's laws amongst various organizations and member states.[142]

The GDPR heavily emphasizes consumer protections, setting strict requirements for data processors, such as companies and data controllers, and use and storage of user data. The regulation requires explicit and informed consent from users before processors may use their data.[143] It also places strict penalties on noncompliant corporations to dissuade unfair practices and imposes a strict compliance deadline.[144] Most importantly, the GDPR greatly expands the rights of consumers regarding the use of their data.[145]

The GDPR requires data subjects[146]—identified or identifiable natural persons—to give clearly established, informed, and affirmative consent to data processors[147] responsible for the collection and usage of subjects' mined data.[148] Affirmative consent means that "[s]ilence, pre-ticked

141. *See* Nate Lord, *What is the Data Protection Directive? The Predecessor to the GDPR*, DIGIT. GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr [https://perma.cc/92YW-Z9M4].

142. *See* GDPR, *supra* note 18, at 9.

143. *See generally* GDPR, *supra* note 18.

144. *See id.*

145. *See id.*

146. GDPR, *supra* note 18, at 33 ("[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.").

147. "[A] natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.*

148. *Id.* at 32.

boxes or inactivity should not therefore constitute consent."[149] The GDPR's proscription of acceptance-through-silence nullifies providers' abilities to use an "Opt-Out approach" to obtain user consent to data usage.[150] The Opt-Out method refers to a processor's ability to automatically collect user data, unless the user affirmatively manifests an unwillingness to comply.[151] Moreover, the data controller must be able to demonstrate that the data subject has consented to the processing of personal data through a written agreement "clearly distinguishable from the other matters" and presented in an "intelligible and easily accessible form."[152] Consent, as required by the GDPR, must always be clearly distinguishable from other terms of service and cannot be hidden within other text.[153] As an example, upon visiting many websites for the first time, users are immediately presented with a pop-up notice preventing them from navigating further without first consenting to privacy policies. Further, the GDPR establishes that data subjects must be able to withdraw consent "at any time as easily as it was to give consent."[154] In enacting this provision, the GDPR requires that data collection be purpose-limited, meaning a user's consent expires upon fulfillment of the purpose for which it was collected.[155] Additionally, the GDPR provides for automatic termination of consent if the data is no longer necessary for the originally stated purpose.[156]

The European Court of Justice ("ECJ") also recognized the right to be forgotten—a right codified in Article 17 of the GDPR.[157] The right to be forgotten allows data subjects who no

149. *Id.*

150. *See* Park, *supra* note 1, at 1476. The GDPR has removed any possibility of opt-out consent in its other provisions.

151. *See* Brian Barrett, *Hey, Apple! 'Opt Out' Is Useless. Let People Opt In*, WIRED (Aug. 2, 2019, 4:32 PM), https://www.wired.com/story/hey-apple-opt-out-is-useless/ [https://perma.cc/E299-8SC9].

152. Park, *supra* note 1, at 1477 (citing GDPR, *supra* note 18, art. 7, at 1-2).

153. Detlev Gabel & Tim Hickman, *Chapter 8: Consent – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation [https://perma.cc/Z8KE-QHHE].

154. Park, *supra* note 1, at 1477 (citing GDPR, *supra* note 18, art. 7, at 3).

155. *See* Park, *supra* note 1, at 1477 (citing Tomain, *supra* note 50, at 35).

156. *See id.*

157. GDPR, *supra* note 18, art. 17.

longer want their data used or stored by data controllers to require the controller remove the data from its system, provided there is no legitimate reason for keeping it.[158] The right to be forgotten does, however, have exceptions. "[T]he right of freedom of expression and information, compliance with other obligations under the European Union or member state laws, for reasons of public interest and public concerns, for archiving purposes, and the exercise and establishment of law enforcement and legal claims" indemnifies controllers from complying with the right to be forgotten under Article 16.[159] In the case of *Google Spain SL v. AEPD and Costeja Gonzalez*, the ECJ specified that the privacy protection "rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information."[160] The language of this opinion illustrates the degree to which the GDPR prioritizes consumer rights over those of a company or even the public's right to access of information.

B. Americans and US Legislators Call for Enactment of a Federally Binding Data-Privacy Statute

While the European Union has been successful in legislating standards for privacy protection, in the United States, the private sector sets standards for consumer data processing and usage. Consequently, US legislation is more business-friendly while the GDPR focuses more on individuals' rights.[161] This business-focused legislation emphasizes the significance the United States places on the role of business in its society. The United States prioritizes competitiveness and the race to innovate over consumer autonomy and privacy rights. Even the California Consumer Privacy Act ("CCPA")—the most expansive data regulation in the United States—carves out an exception from its

158. Press Release, Speech of Viviane Reding, Eur. Comm'n, The European Union Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5 (Jan. 22, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF [https://perma.cc/D98P-FXJT]; *see also* GDPR, *supra* note 18.

159. GDPR, *supra* note 18, art. 16.

160. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, ¶ 99 (May 13, 2014).

161. *See* discussion *infra* Part III (weighing the pros and cons of such a business-focused legislation in the United States).

privacy interest requirement by providing that the interest be "balanced against competing interests, which may be justified if legitimate interests derived from legally authorized and socially beneficial activities of the government and private entities" exist.[162] Moreover, the balancing of legitimate privacy interests against activities of governmental and private entities favors private actors, such as large private data-mining corporations.[163]

In support of this view, the California Supreme Court noted that individuals have "greater choice in dealing with private actors than when dealing with the government."[164] The Court, however, seems to overlook the prevalence of monopolies or monopolistic-like corporations in America. These large corporations wield substantial influence over not only how American consumers live their daily lives, but also how the world views the United States as a competitor in the technological market.[165] As one of only two nations leading the tech race, [166] the United States must weigh appeasing its citizens calling for stronger data protections against maintaining their global technological primacy. Many tech and corporate leaders fear over-legislation's impact on technological innovation and competition.[167]

---

162. Park, *supra* note 1, at 1469 (citing Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655-56 (Cal. 1994)).

163. *See* Park, *supra* note 1, at 1470 (citing *Nat'l Collegiate Athletic Ass'n*, 865 P.2d at 656).

164. Park, *supra* note 1, at 1470 (citing *Nat'l Collegiate Athletic Ass'n*, 865 P.2d at 633, 656).

165. *See* Shaoul Sussman & Matt Stoller, *Why Amazon, Facebook, Google and Apple are Bad for America*, POLITICO (July 28, 2020, 4:30 AM), https://www.politico.com/news/agenda/2020/07/28/agenda-amazon-facebook-google-apple-hearing-383612 [https://perma.cc/VJ73-5SQY]; *see also* Tom Huddleston Jr., *Bill Gates: 'Government needs to get involved' to Regulate Big Tech Companies*, CNBC (Oct. 17, 2019, 1:16 PM), https://www.cnbc.com/2019/10/17/bill-gates-government-needs-to-regulate-big-tech-companies.html [https://perma.cc/G69B-P8VQ].

166. *See, e.g.*, Audrey Cher, '*Superpower Marathon': U.S. May Lead China in Tech Right Now — but Beijing has the Strength to Catch Up*, CNBC (May 17, 2020, 9:43 PM), https://www.cnbc.com/2020/05/18/us-china-tech-race-beijing-has-strength-to-catch-up-with-us-lead.html [https://perma.cc/HF8U-YPYD].

167. *See* Larry Downes, *How More Regulation for U.S. Tech Could Backfire*, HARV. BUS. REV. (Feb. 9, 2018), https://hbr.org/2018/02/how-more-regulation-for-u-s-tech-could-backfire [https://perma.cc/8KH2-PQB9].

Unlike the European Union, the United States does not consider data privacy a fundamental right.[168] Nevertheless, Fourteenth Amendment jurisprudence has found privacy an implied protection guaranteed by the US Constitution.[169] Noting that there does not currently exist a federally-binding statute on data-privacy protection, some states have chosen to codify protective acts themselves.[170]

In 2018, California passed the CCPA. It is the first regulation of its kind overseeing business data-collection practices in the United States and provides the most comprehensive coverage of data-protection.[171] Despite tech companies spending millions of dollars to oppose Assembly Bill 375 (the bill creating the CCPA), it was ultimately passed on June 28, 2018.[172] The regulation protects consumers' data privacy in several ways. The CCPA grants consumers (1) the right to request businesses delete any of the consumer's personal information; (2) the right to request businesses that sell personal information disclose categories of information sold and identify third parties to which it was sold; and (3) the right to opt out of the sale of their personal information.[173] As much protection as the CCPA affords California consumers, it still errs on the side of protecting businesses more than the general public. The bill requires that businesses be provided "thirty-day written notice to 'cure' any

168. *See* Park, *supra* note 1, at 1465 (citing LEE A. BYGRAVE, INTERNET GOVERNANCE BY CONTRACT 23, 118 (2015) (noting that a right of privacy is not directly expressed anywhere in the US Constitution, including in the Bill of Rights)).

169. *See* Park, *supra* note 1, at 1468 (citing Lawrence v. Texas, 539 U.S. 558, 564-65 (2003); Roe v. Wade, 410 U.S. 113, 152-53 (1973); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972); Griswold v. Connecticut, 381 U.S. 479, 485 (1965)).

170. *See generally* H.R. 1128, 71st Gen. Assemb., Reg. Sess. (Colo. 2018) (enacted) [hereinafter CCDPA]; A.B. 375, 2017-2018, Reg. Sess. (Cal. 2018) [hereinafter CCPA] (known as the Colorado Consumer Data Privacy Act and the California Consumer Privacy Act, respectively).

171. *See* Park, *supra* note 1, at 1456 (referencing Wakabayashi, *supra* note 65).

172. CCPA § 1798.1000; *see also* Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://perma.cc/E4P7-3G54].

173. Park, *supra* note 1, at 1472 (citing Lapowsky, *supra* note 172); Noah Ramirez, *Can CCPA Affect Your Small Business?*, OSANO (Oct. 30, 2019), https://www.osano.com/articles/ccpa-small-business [https://perma.cc/4KCC-6FT7].

alleged violations before an action is undertaken."[174] Further, except in cases of data breaches, citizens may not bring private actions against corporations for privacy-related abuses.[175] In support of this stance, critics of the CCPA argue that the CCPA would otherwise open technology companies up to too much liability, hindering their businesses and impinging on their ability to hire.[176]

In defending consumer rights, section 1798.120(a) of the CCPA provides consumers a right to "Opt-Out" of businesses selling their data to third parties.[177] The provision states businesses must inform consumers that their data may be distributed and that they have a right to request it not be.[178] To satisfy this requirement, websites must include a "clear and conspicuous link on the business Internet homepage, titled 'Do Not Sell My Personal Information'."[179] This link must provide consumers with an "opt out" option.[180] After a consumer has opted-out, businesses must comply with the request and are not allowed to contact the consumer asking permission to sell their data again for twelve months.[181]

Similar to the GDPR's right to be forgotten, section 1798.105 of the CCPA contains a "right to delete" clause.[182] The provision allows users to request that a business delete any personal information it has collected from the user.[183] Additionally, the business must also notify any third party to whom the business has distributed the data of the request.[184] Some feel the CCPA will

---

174. "A consumer may only bring a private lawsuit if they first provide the business with thirty-days written notice identifying specific provisions that have been violated." Park, *supra* note 1, at 1487 (citing CCPA § 1798.150(b)(1)).

175. "As the CCPA is currently written, only the AG can sue for most violations, with an exception for private right of action under section 1798.150." Park, *supra* note 1, at 1487 (citing CCPA § 1798.150(a)(1)).

176. *See* Park, *supra* note 1, at 1473 (citing Lapowsky, *supra* note 172); *see also* James Harvey & Gavin Reinke, *The CCPA Could Reset Data Breach Litigation Risks*, JDSUPRA (Aug. 20, 2019), https://www.jdsupra.com/legalnews/the-ccpa-could-reset-data-breach-14801/ [https://perma.cc/G89A-YUVU].

177. CCPA § 1798.120(a).

178. *See id.* § 1798.120(b).

179. *Id.* § 1798.135(a)(1).

180. *See id.*

181. *See id.* § 1798.135(a)(5).

182. *Id.* § 1798.105(a).

183. *See id.*

184. *See id.* § 1798.105(c).

serve as a precedent in state-level data privacy regulation and await other states to follow suit.[185]

Currently, there is no federal statute in the United States regarding data privacy protection,[186] and instead, federal agencies stepped in to fill the gap. The Federal Trade Commission has broadly relied upon Section 5 of the Federal Trade Commission Act ("FTC Act") to vindicate consumer protection violations, "including in the context of data privacy and security."[187] Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[188] Under the authority allegedly vested by Section 5 of the FTC Act, the FTC has been pursuing companies who violate data privacy and security practices on an individual basis and seeking either injunctive or monetary relief against them, citing Section 13(b) of the Act as a grant of authority.[189] The FTC has found that the monetary pressure of paying fines and litigation costs has kept companies compliant with Section 5.[190]

Currently, however, there are two cases pending before the Supreme Court that could potentially constrict the FTC's interpretation of Section 13(b).[191] Depending on the outcome,

185. "[D]ata privacy remains high on the agenda of California legislators and will likely sweep across the United States as more states jump on the bandwagon to ensure greater data protection for its residents." Park, *supra* note 1, at 1488.

186. *See* Emily Birnbaum & Harper Neidig, *State Rules Complicate Push for Federal Data Privacy Law*, HILL (Mar. 5, 2019 6:00 AM), https://thehill.com/policy/technology/432564-state-rules-complicate-push-for-federal-data-privacy-law [https://perma.cc/UV9Z-9SRU].

187. Céline M. Guillou, *How the FTC's Enforcement of Data Privacy and Security May be Impacted by the U.S. Supreme Court's Upcoming Review of the FTC's Use of Section 13(b)*, LEXOLOGY (Sept. 30, 2020), https://www.lexology.com/library/detail.aspx?g=37fdf828-4a9a-4aa2-8f20-f8f6bb0e1ce0 [https://perma.cc/UV9Z-9SRU].

188. Federal Trade Commission Act, 75 P.L. 447, 52 Stat. 111, 75 Cong. Ch. 49.

189. *See* Guillou, *supra* note 187.

190. *See id.*

191. *See id.* (referring to FTC v. Credit Bureau Ctr., LLC, 937 F.3d 764 (7th Cir. 2019)). In *FTC v. Credit Bureau Center, LLC*, the FTC sued Credit Bureau Center, LLC ("Brown") under §13(b) of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 53(b), alleging that its websites and referral system violated several consumer-protection statutes. Upholding the FTC's victory, the Seventh Circuit found §13(b) of the FTC Act provided for injunctive relief and temporary restraining orders, and that both §§45(I) and 57b(b) "expressly authorized additional equitable remedies," but that "section 13(b) lacked comparable language," *Credit Bureau Ctr., LLC*, 937 F.3d at 764. District courts also have authority to order equitable monetary relief under §13(b) of the FTC Act. FTC v. AMG Capital Mgmt., LLC, 910 F.3d 417 (9th Cir. 2018).

the FTC may be constrained from obtaining equitable relief against corporate deceptive or unfair practices.[192] Some fear the decisions could impact some corporations' willingness to provide transparent, fair, and non-deceptive disclosures to consumers.[193] Others feel the rulings may expand the FTC's enforcement authority by providing clearer guidelines on how the FTC handles data privacy and security.[194] They argue the many recent "egregious corporate data privacy and security fails" may bring legislators closer to a federal privacy law.[195] Currently, Congress is deliberating numerous proposed bills outlining how corporations should handle data privacy, security, and enforcement. The following Sections examine two of the most comprehensive bills pending before Congress: the Consumer Online Privacy Rights Act ("COPRA") and the Digital Accountability and Transparency to Advance Privacy Act ("Data Privacy Act").

COPRA is a bill introduced in the Senate that sets requirements for organizations that collect, process, or share a consumer's data.[196] If passed, the bill will require data-gathering entities to: (1) make their privacy policies publicly available and inform individuals about how their data is being used; (2) delete or amend an individual's data upon request; (3) export reports in a readable format, upon request; (4) establish data security practices to protect confidentiality and accessibility of consumer data; and (5) designate a privacy officer and a data security officer to implement and conduct privacy and data security programs and risk assessments.[197] The bill prohibits companies from, among other things, engaging in deceptive or harmful data practices, processing or transferring an individual's sensitive data without affirmative express consent, and providing a service or product conditioned upon an individual's waiver of privacy rights.[198] Additionally, the bill requires the FTC to establish a new bureau specifically tasked with enforcing its provisions.[199] In sum, COPRA holds accountable entities who process personally

192. *See id.*
193. *See id.*
194. *See id.*
195. *Id.*
196. S. 2968, 116th Cong. (1st Sess. 2019).
197. *Id.*
198. S. 2968, 116th Cong. (1st Sess. 2019).
199. *See id.*

identifiable information.[200] Aside from accountability, the bill gives individuals a right of access, deletion, data minimization, and data security.[201] Finally, though the bill would be a federal statute, it would provide minimum guidelines for state level data-privacy coverage.[202]

Like COPRA, the Data Privacy Act establishes requirements for businesses that "collect, process, store, or disclose information."[203] Unlike COPRA, however, the bill only places security requirements on data processors who collect from at least 3,000 people per any twelve-month period.[204] Further, the bill does not cover data pertaining to employment or restrict use of publicly available governmental records.[205] The Data Privacy Act requires businesses to: (1) "provide consumers with accessible notice of the business' privacy practices with respect to such information"; and (2) "if meeting a certain revenue threshold, appoint a privacy officer to oversee compliance with the information privacy standards of the bill."[206] Though the bill outlines when a company should appoint a privacy officer, the bill does not elaborate as to what that "threshold" is. The bill further calls on the FTC to enforce requirements of limiting the scope and reasoning, allowing consumers to amend, and examining the impact of user data on covered businesses.[207] Finally, the bill requires the National Science Foundation to include research and instructions on encrypting or removing personally

200. *See, e.g.*, Jesse Woo, Jan Whittington & Ronald Arkin, Note, *Urban Robotics: Achieving Autonomy in Design and Regulation of Robots and Cities*, 52 CONN. L. REV. 319, 374 (2020) (citing Consumer Online Privacy Rights Act, S. 2978, 116th Cong. § 2(9) (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text. [https://perma.cc/E4G9-7E8M]).

201. *See id.* (citing Consumer Online Privacy Rights Act, S. 2978, 116th Cong. §§ 101-10 (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text [https://perma.cc/2GYX-RFJ4]).

202. *See id.*

203. Digital Accountability and Transparency to Advance Privacy Act, S. 583, 116th Cong. (2019).

204. *See id.*

205. *See id.*

206. *See id.*

207. *See id.*

identifiable elements from collected consumer data within its information security grants program.[208]

In sum, the United States does not have federally-binding data privacy laws or standard methods of regulation. As such, some states[209] have taken it upon themselves to create legislation protecting consumer data.[210] As a response to the plethora of data breaches corporations have faced over the past several years,[211] legislators have drafted several proposed bills calling for federal data privacy laws, such as COPRA and the Data Privacy Act.

C. China's Surveillance State Affords its Citizens Data Protections

Historically, Chinese laws have offered citizens significantly fewer privacy protections than those of other nations.[212] Of the few privacy laws in place, China's cybersecurity law ("CSL")—the most comprehensive of any Chinese privacy protection yet enacted—[213] focuses more on national security than on securing individual privacy rights.[214] Even in its provisions that do not implicate national security, the laws center around consumer privacy protections rather than rights derived as citizens.[215] Still, the CSL, alongside China's Personal Information Security Specification (2018 Specification)—which sets standards for data collection, use, and sharing and concisely defines "consent"—[216] is more comprehensive than anything the United States has enacted, though it is less stringent than the GDPR. Regarding data collection and processing, data breaches, and oversight, the CSL resembles US laws.[217] Conversely, the 2018 Specification sets much stronger protections in the areas of transparency, limiting

208. *See* Cong. Rsch. Serv., *Summary S.583 – 116th Congress (2019-2020)*, U.S. CONG., https://www.congress.gov/bill/116th-congress/senate-bill/583 [https://perma.cc/2QKK-MUS2] (last visited Mar. 1, 2020).

209. The states referred to are specifically California and Colorado regarding the California Consumer Privacy Act and the Colorado Consumer Data Privacy Act, respectively. H.R. 1128, 71st Gen. Assemb., Reg. Sess. (Colo. 2018) (enacted).

210. *See generally* CCPA.

211. See *supra* Section II.A.

212. *See* Lin, *supra* note 23, at 266 (referencing Fry, *supra* note 23, at 440).

213. *See* Emmanuel Pernot-Leplay, *China's Approach On Data Privacy Law: A Third Way Between the U.S. and The European Union?*, 8 PENN. ST. J. L. & INT'L AFF. 49, 73 (2020).

214. *See* Sacks, *supra* note 27.

215. *See* Pernot-Leplay, *supra* note 213, at 54.

216. *See* Shi et al., *supra* note 21.

217. *See* discussion *infra* Section III.C.1.

additional processing, and increasing autonomy rights, echoing the same protections enumerated in the GDPR.[218]

1. Sections of the CSL Bear Resemblance to United States Laws

a. Data Collection and Processing Requirements: Consent and Data Quality

In the European Union, lawfulness of data processing depends on legal principles of: (1) consent from the data subject; (2) a contract to which the data subject is party; (3) the necessity of processing data to advance vital interests; (4) compliance with any legal obligations; (5) the carrying-out of a task in the public interest; or (6) the necessity of processing data for the "legitimate interests of the data controller unless the rights and freedoms of the data subject override them."[219] However, in the United States and China, the main determinant of the legality of data processing is this first principle: consent.[220] The United States, European Union, and China all require data subjects' consent to data controllers' use and processing of their data, though Article 6 of the GDPR defines giving consent much narrower than the United States and China do.[221] In the European Union, consent must be "freely given, informed and unambiguous, which excludes implicit consent."[222] The United States requires an individual to consent to data processing,[223] but infers such consent from a user using a website that has privacy policies rather than requiring explicit consent.[224] Similarly, China's CSL

218. *See* discussion *infra* Section III.C.2.

219. *See* Pernot-Leplay, *supra* note 213, at 83 (drawing from the Directive 95/46/EC, UK's DP Act of 1998 and Netherland's WBP (which are laws implementing the Directive), the OECD Guidelines, and the Fair Credit Reporting Act of 1970 in the United States).

220. *See* Pernot-Leplay, *supra* note 213; *see also infra* Section IV.A.1.

221. *See* GDPR, *supra* note 18, art. 6.

222. Pernot-Leplay, *supra* note 213, at 83 (summarizing the definition of consent as laid out in the GDPR art. 6).

223. *See* Paul M. Schwartz, *The European Union-U.S. Privacy Collision: a Turn To Institutions and Procedures*, 126 HARV. L. REV. 1966, 1976-77 (2013); *see also* Noah Ramirez, *Data Privacy Laws: What You Need to Know in 2020*, OSANO (Nov. 8, 2020), https://www.osano.com/articles/data-privacy-laws [https://perma.cc/G4ZA-VS6Z].

224. Default collection is permissible in the absence of a law explicitly forbidding it. *See* Schwartz *supra* note 223, at 1976 (distinguishing between the EU data regime and that of the United States, noting "the United States does not rely on a notion that personal information cannot be processed in the absence of a legal authorization.

requires only consent for data collection and processing and allows for consent to be implied.[225] Nonetheless, the CSL does not allow for default collection or processing.[226] It includes exemptions to obtaining consent which overlap with some of the GDPR's legal bases. Consent is unnecessary for purposes of protecting national security, preserving public health, conducting criminal investigations, protecting lives or "major lawful rights" of the data subject, or accessing previously lawfully and publicly disclosed information.[227]

Another distinction between the data protection regimes of the three states is their treatment of data quality. The data quality principle, as outlined in the GDPR, necessitates that personal data intended for collection be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."[228] The United States sets data quality standards in some federal laws, but unevenly applies its principles across state laws.[229] Again, following the United States' vague application of privacy practices, neither the CSL nor the 2018 Specification mention data quality.[230] Regarding consent and data quality, China seems to follow the United States' lead on systematic application of privacy principles.

b. Data Breach Repercussions and Oversight Committees

Protection of data security is essential to maintaining confidentiality and security of users' personal data. When data

---

Rather, it permits information collection and processing unless a law specifically forbids the activity.").

225. Drafters of the CSL and the 2018 Specification stated that explicit consent is only required where the phrase "explicit consent" is expressly written, not everywhere "consent" is used. *See* Samm Sacks, *China's Emerging Data Privacy System and GDPR*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 9, 2018), https://www.csis.org/analysis/chinas-emerging-data-privacy- system-and-gdpr [https://perma.cc/8WR5-NFWZ] [hereinafter Sacks II].

226. *See* Pernot-Leplay, *supra* note 213, at 84.

227. *See* Pernot-Leplay, *supra* note 213, at 85 (referencing 2018 Specification art. 5.4 (a)-(f)).

228. GDPR, *supra* note 18, art. 5.1(d).

229. *See, e.g.*, Privacy Act of 1974, 5 U.S.C § 552a(e)(5); *see also* discussion *supra* Section III.B.

230. *See* Pernot-Leplay, *supra* note 213, at 86.

breaches occur, most nations require data controllers to provide notification of such breaches.[231] The European Union has dedicated supervisory authorities in place to monitor data breaches.[232] On the other hand, the United States and China do not have designated oversight committees. Moreover, the consequences for a data controller's inaction after a breach has occurred also differs by nation.

The CSL contains a vague requirement of security for personal data.[233] The 2018 Specification is similarly vague, but explicitly mentions that "data controllers should 'possess the appropriate security capacity taking into account the security risks faced, and employ sufficient management and technical measures to protect the confidentiality, integrity, and availability of personal information.'"[234] In the event of a data breach, all three states require disclosure to authorities and specify steps to remediation. China's CSL requires data controllers to inform not only authorities, but also compromised individuals of such breaches.[235] The 2018 Specification specifies such requirements and compels companies to give full incident reports to enforcement agencies in the event of a breach and conduct cybersecurity drills annually.[236] The laws require data controllers to inform authorities and individuals of the breach "promptly," but does not specify a timeframe.[237] Similarly, most US statutes only require notifications to be made within a reasonable time.[238] In the European Union, however, data controllers must notify supervisory authorities within seventy-two hours of the controller

231. *See id.*

232. *See id.*

233. CSL articles 40 and 42 set out certain, vague requirements such as network operators maintaining user confidentiality over the information they collect, establishing protection systems, and adopting measures that ensure protection of the personal information they gather. *See* Creemers, *supra* note 20.

234. Pernot-Leplay, *supra* note 213, at 87 (quoting 2018 Specification art. 4 (f)).

235. *See* Creemers, *supra* note 20, art. 42.

236. Pernot-Leplay, *supra* note 213, at 88-89 (citing 2018 Specification arts. 9.1(a), (b)).

237. *Id.* at 89.

238. *See, e.g.*, California Data Security Breach Notification Law, § 1798.29 (a), 1798.82 (a) (California S.B. 1386) (stating "disclosures shall be made in the most expedient time possible and without unreasonable delay").

becoming aware of the breach.[239] They also must notify the data subject if there is a risk to their safety or autonomy.[240]

Regarding oversight committees, the European Union follows the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines") for data privacy.[241] The United States does not have a designated regulatory oversight authority but distributes oversight responsibilities among a broad array of government bodies including: the US Federal Trade Commission ("FTC"), state attorneys general, the Federal Communications Commission ("FCC"), the Securities and Exchange Commission ("SEC"), and more.[242] Of these, the FTC has assumed the responsibility of enforcing privacy protections in the United States.[243] China's CSL also delegates data protection to several regulators, rather than a single organized, EU-style task force.[244] Chinese authorities take a sectorial approach to regulation but fall short of effectively delegating responsibility among oversight groups.[245]

Another issue with these systems is the enforcement of violation penalties. Chinese companies responsible for data breaches may face fines for their actions, but those fines are limited to the greater of either "RMB 1,000,000 (USD 150,000) or ten times the amount of unlawful gains from the misuse of

239. GDPR, *supra* note 18, art. 33(1).

240. *See* GDPR, *supra* note 18, art. 34.

241. *See Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines), 1980*, OECD, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [https://perma.cc/HSR7-FR8C] (last visited Mar. 2, 2021). The OECD member countries are asked to "establish privacy enforcement authorities, free from instructions, bias or conflicts of interest, with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis." Pernot-Leplay, *supra* note 213, at 89 (quoting OECD Privacy Guidelines P 19(c)).

242. *See* ALAN C. RAUL, UNITED STATES, THE PRIV., DATA PROT. AND CYBERSECURITY. REV. 269 (Alan Charles Raul et al. eds., 4th ed. 2017); The list includes: the US Federal Trade Commission, state attorneys general, the Federal Communications Commission, the Securities and Exchange Commission, financial and banking regulators like the Consumer Financial Protection Bureau, the Department of Health and Human Services, the Department of Education, the judicial system, and the US plaintiffs' bar.

243. *See* discussion *supra* Section III.B.

244. *See* Pernot-Leplay, *supra* note 213, at 90 (referring to Article 8 of the CSL).

245. *See* Bo Zhao & G.P. (Jeanne) Mifsud Bonnici, *Protecting EU Citizens' Personal Data in China: a Reality or a Fantasy?*, 24 INT'L J. L. & INFO. TECH. 128, 135 (2016).

data."[246] This fine may seem insignificant to large corporations, however the CSL grants regulators the authority to "temporarily suspend business operations, shut down the website or even cancel business licenses and relevant operations permits . . . " upon a company's breach of data privacy.[247]

In comparison, China's sectoral regulation of data breach violations resembles the United States' approach whereby several different oversight committees are responsible for responding to data security breaches.[248] Enforcement of violations in both nations is based on a case-by-case analysis, with set maximums for monetary enforcement.[249] On the contrary, while the GDPR allows regulators to issue fines based on company turnover, those fines tend to be highly deterrent and are enforced by a designated data breach security team.[250]

2. China's Laws Echo the GDPR on Key Issues

Two principles central to the GDPR are the data minimization principle and the sensitivity principle. In the 2018 Specification, China has adopted standards mirroring the GDPR on these two topics. The United States, on the other hand, barely refers to them.

a. Transparent Data Usage Practices and Limitations on Additional Processing

The data minimization principle, as expressly outlined in the GDPR, allows data collection and processing of only the minimum amount of data necessary to fulfil the purpose for which it was collected.[251] Once the data controller no longer needs the data, the principle requires its erasure.[252] In the United States, the Privacy Act mandates governmental records contain "only such information about an individual as is relevant and necessary to accomplish a purpose,"[253] though the Act does not provide limitations on retention periods. Additionally, neither

246. Pernot-Leplay, *supra* note 213, at 91.
247. *Id.* (citing CSL art. 64).
248. *See* discussion *supra* Section III.C.1.b.
249. *See id.*
250. *See id.*
251. *See* GDPR, *supra* note 18, recital 39, art. 5.1(c).
252. *See* GDPR, *supra* note 18, art. 5.1(e).
253. Privacy Act of 1974, 5 U.S.C. § 552a(e)(1).

the FTC nor the CPPA explicitly mention the principle.[254] Suffice to say, application of the principle across the United States is inconsistent, at best.

China's CSL and 2018 Specification seem to reflect the GDPR in their approach to the data minimization principle. The CSL prohibits collection of personal data unrelated to a legitimate purpose and requires network operators acting as data controllers to follow the data minimization principle.[255] The 2018 Specification further requires data collectors to follow the data minimization principle and delete data when the original purpose for collection is fulfilled.[256]

The second principle facilitating transparent data practices is the sensitivity principle. This concept recognizes that certain content necessitates additional safety protections based on the sensitivity of the information contained therein.[257] Some information, such as credit card numbers and bank account information, should be protected more stringently than a user's fantasy football picks because of the consequences of stealing one's financial information, like identity theft, loss of finances, credit depreciation, and much more. Unlike the US public regime,[258] the GDPR adheres to this principle and considers information such as socioeconomic background, political opinions, religious beliefs, union membership, criminal convictions, and genetic or biometric data as some of the protected classes of personal data.[259] While both China and the European Union place increased protective measures on sensitive data, China adopts a risk-based approach to classifying data as

254. *See* Pernot-Leplay, *supra* note 213, at 94 (stating "The data minimization principle is absent from the FTC's list of fair information practice principles but exists in the list provided by the Department of Homeland Security. It is not an express requirement in the CCPA.") (citing DHS, *Fair Information Practice Principles (FIPPs)*, DEP'T HOMELAND SEC'Y (2015), https://www.dhs.gov/publication/fair-information-practice-principles-fipps-0 [https://perma.cc/24FN-3HYF]).

255. Creemers, *supra* note 20, art. 41, P 2.

256. Shi, *supra* note 21, arts. 4(d), 6.1.

257. *See* Anneliese Roos, *Core Principles of Data Protection Paw*, 39 COMP. & INT'L L.J. S. AFR. 121 (2006).

258. The United States does not have federal laws codifying the sensitivity principle, although some private companies may choose to offer higher levels of protection based on the sensitivity principle's ideals.

259. GDPR, *supra* note 18, arts. 9-10.

"sensitive."[260] According to the risk-based definition, sensitive data are "those that, if disclosed or altered, could endanger the safety of persons or property, harm personal reputation and physical or psychological health, lead to discriminatory treatment, etc."[261] Overall, the European Union is the leader in regulating and codifying privacy protections, followed by China which adopts similar protections with a governmental exception to user data access and usage. The United States, thus, falls behind both the European Union and China in privacy protection regulations.

3. Even with New Privacy Protections, China Remains a Surveillance State

While protections are increasing through the passing of the CSL and the 2018 Specification, the Chinese government still enforces laws allowing for the gathering and mining of citizens' data, citing national security protection in doing so.[262] The CSL, as groundbreaking as it is, allows many opportunities for lawful governmental and third-party encroachment upon citizens' privacy rights.[263] Both the public and private sectors use data-gathering methods, as required by law, to assist in government surveillance of Chinese citizens, including the "citizen score"[264] system.[265] The "citizen score" is a government owned, privately operated, system whereby citizens are monitored then ranked based on their behavior and trustworthiness in the government's eyes.[266] Many feel this public-private sector collaboration fuels a

260. *See* Shi, *supra* note 21, art. 3.2 (listing types of sensitive data and defining the risk-based approach).

261. Perot-Leplay, *supra* note 205, at 96.

262. *See* Arjun Kharpal, *Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice*, CNBC (Mar. 4, 2019, 8:13 PM), https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html [https://perma.cc/C69R-W2VF].

263. *See* Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 100 (2018).

264. *See infra* note 266.

265. *See* Mitchell & Diamond, *supra* note 22.

266. *See* Alexandra Ma, *China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you*, BUS. INSIDER (Oct. 29, 2018, 12:06 PM), https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4 [https://perma.cc/U265-TWUH].

Chinese effort to become the first nation to actualize an omnipresent "algorithmic surveillance" system.[267] The impacts of such a system will greatly alter how Chinese citizens and corporations operate within the nation.

Today's technological business model is largely dependent upon data-sharing.[268] Consequently, data-gathering and AI-powered surveillance technology have become deeply ingrained in China's economic infrastructure.[269] One of China's largest companies, Alibaba, operates the social media app Sesame Credit.[270] The app enables Alibaba to monitor financial consumer behavior of 100,000 Chinese citizens.[271] Alibaba has privatized China's "citizen score" system through its user data-gathering practices and character-rating system.[272] This system helps maintain Alibaba's stature as one of the most competitive e-commerce companies in the world.[273] As the most successful of the only eight companies chosen to develop a credit scoring system for the country, Alibaba is dominating the market, leaving little room for competitors.[274] While the government may appreciate Alibaba's product development, the company now holds a monopolistic-like control over the market.[275]

While this rating system greatly benefits China's economy, the lack of privacy laws within this scheme has mixed impacts on its citizens. Privacy intrusions such as cameras covering the majority of every block,[276] governmental phone-tapping, and

267. *See* Mitchell & Diamond, *supra* note 22.

268. *See* Perot-Leplay, *supra* note 205, at 111.

269. *See* Charlie Campbell, *'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World*, TIME (Nov. 21, 2019, 6:39 AM), https://time.com/5735411/china-surveillance-privacy-issues/ [https://perma.cc/5SS8-M7AA].

270. Mitchell & Diamond, *supra* note 22.

271. *See id.*

272. *See id.*

273. *See id.*

274. *See* Lea Nonninger, *Here's Why China is Concerned About Tencent and Alibaba's Credit Scoring Efforts*, BUS. INSIDER (Feb. 6, 2018 9:37 AM), https://www.businessinsider.com/china-tencent-and-alibabas-new-credit-scoring-solution-2018-2 [https://perma.cc/FF7B-VX8G].

275. *See id.*

276. *See* Campbell, *supra* note 269 (noting that "[e]ight of the top 10 most surveilled cities in the world are in China, according to [tech-research website] Comparitech.").

other known methods of surveillance are widespread.[277] Many regard the city of Chongqing as the most surveilled city in the world.[278] Chongqing boasts a "[r]atio of one CCTV camera for every 5.9 citizens."[279] This surveillance regime has led Chinese citizens, particularly those of Muslim minority groups such as the Uighurs,[280] to significantly alter their behavior to meet China's various requirements.[281] While Chinese citizens have reported ways in which this system has positively impacted their lives (e.g., facilitating the return of publicly lost items),[282] the ramifications of failing to comply with the communist regime have considerably negative impacts on citizens as well.[283] The United Nations has noted one particularly catastrophic impact of the regime, calling the mandatory "re-education centers" in China akin to concentration camps.[284] Chinese authorities have described these re-education centers as "vocational training and re-education programmes that aim to alleviate poverty and counter terrorism threats."[285] In reality, these centers are filled with Muslim citizens, targeted "for 'offences' as trivial as owning a Qur'an, or abstaining from eating pork."[286] In these so-called "vocational training programs," detained inmates endure forced labor, torture, medical neglect, and coercive birth control.[287] Outside of these camps, Uighur families continue to suffer egregious intrusions into their lives with forced quartering of Han Chinese officials residing inside Uighur homes as an extra measure of surveillance.[288] In sum, China's surveillance state can benefit and harm its citizens, while corporations such as Alibaba seem to

277. *See generally id.*

278. *See id.*

279. *Id.*

280. *See Xinjiang: China defends 'education' camps*, BBC (Sept. 17, 2020), https://www.bbc.com/news/world-asia-china-54195325 [https://perma.cc/YB9X-MJX6].

281. *See* Campbell, *supra* note 269.

282. *See id.*

283. *See id.*

284. *See id.*

285. *See* Emma Graham-Harrison, *China has built 380 internment camps in Xinjiang, study finds*, GUARDIAN (Sept. 23, 2020, 10:00 PM), https://www.theguardian.com/world/2020/sep/24/china-has-built-380-internment-camps-in-xinjiang-study-finds [https://perma.cc/XHQ6-JQQD].

286. *See id.*

287. *See id.*

288. *See id.*

thrive under the data-gathering-friendly regime. It is possible to use this surveillance power as a force for good, but the question remains on whether the Chinese government can be trusted to not abuse this power. So far, widespread abuse of this power proves China cannot.

Overall, nations vary greatly in their enforcement of citizen data-security provisions. While the European Union's implementation of the GDPR provides citizens with the greatest privacy protections, its impact on corporations poses such risks of stifling innovation that many feel no EU tech companies will be able to compete with the likes of US and Chinese corporations on the global market.[289] The United States may not have federal protections for citizens' privacy comparable to those the GDPR affords Europeans, however, with looser requirements, US companies are free to develop their technology at faster rates, thus pushing the nation toward the front of the tech race.[290] Citing recent data-privacy breaches, however, Americans are currently calling for reform.[291] Legislators have introduced numerous draft bills—currently awaiting deliberation in Congress—that can regulate corporate America's use of user data by encouraging stronger consumer protections and more transparent privacy practices.[292] US legislators hope their bills will achieve what China's new laws currently do: promote corporate accountability by protecting data subjects' private information.[293] Even with more regulation than the United States, China's lack of organized oversight committees leaves citizens nearly helpless in any attempt at recourse against data abuse practices.[294] Moreover,

289. *See* Nick Wallace & Daniel Castro, *The Impact of the EU's New Data Protection Regulation on AI*, CTR. FOR DATA INNOVATION (Mar. 27, 2018), https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf [https://perma.cc/6TVF-E5YX].

290. *See* Ed Stacey, *Data Privacy Laws Need Rethinking To Encourage Innovation*, FORBES (June 7, 2019, 11:08 AM), https://www.forbes.com/sites/edstacey/2019/06/07/data-privacy-laws-need-rethinking-to-encourage-innovation/?sh=37bfa668a91a [https://perma.cc/L7YH-SL2M].

291. *See* Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/SJ8Q-ZTT3].

292. *See* discussion *supra* Section III.B (discussing various bills pending before Congress).

293. *See* discussion *supra* Section III.C.

294. *See id.*

the privacy principles set out in the new laws exempt the government from their requirements when it acts in the name of national security.[295] While China's constant surveillance of its cities may make some feel safer, the country's monitoring system provides a clear path to the dissolution of anonymity.

IV. THE FINE LINE BETWEEN CONSUMER DATA PROTECTION AND OVER-LEGISLATION

The United States' current enforcement of data privacy protections is inconsistent and defective. Lacking a federally-binding statute, the current state-by-state legislative framework leads to uneven data protection practices across the nation.[296] Additionally, the United States lacks a properly established oversight committee dedicated to the enforcement of data security.[297] The FTC has assumed this role and has undertaken the task of enforcing data privacy standards set out in various pieces of legislation.[298] Without uniform standards, however, the FTC imposes fines and disciplinary actions on a case-by-case basis, increasing the likelihood of differing penalties for similar violations of hazy standards.[299]

The European Union, by adopting the GDPR, has avoided the American problem of inefficient, opaque data-privacy protections by setting clear guidelines for compliance and enforcement.[300] While adopting a GDPR-like federal statute may solve the United States' transparency problem, the consequences of such rigid data regulation could jeopardize its position in the global tech market.[301] While it is true that the United States needs to do more to establish clear data protection measures, a GDPR-sized regulation would be too stifling to competition and hurt the United States more than it protects American citizens.[302]

This Part begins by weighing the good that comes from the GDPR against the risk of stifling technological development in

295. *See* discussion *supra* Section III.C.2.a.
296. *See* discussion *infra* Section IV.B.
297. *See id.*
298. *See id.*
299. *See id.*
300. *See* discussion *infra* Section IV.A.
301. *See* discussion *infra* Section IV. B.
302. *See id.*

EU companies. It then analyzes how a GDPR-sized legislation would be harmful to the United States.[303] Finally, this Part ends with suggestions on how the United States should balance economic competitiveness and the sufficiency of its data protections.

A. GDPR Takes Big Steps Against Big Tech

The GDPR's enactment prompted a divided reaction amongst business owners, tech experts, and foreign nations.[304] On one side of the divide are numerous data abuse victims seeking stronger data privacy protections and proper enforcement. In the wake of numerous data abuse scandals,[305] some consumers began favoring the privacy protections offered by the GDPR.[306] The GDPR's strict enforcement of data protections can help victims of data misuse to feel vindicated through fining or prosecuting data privacy abusers. On the other side of the divide were small businesses, techies,[307] and large corporations dependent upon data to drive technology.[308]

The GDPR set out rules providing for legal certainty, opening the doors for increased consumer trust in data-driven technology. The GDPR assuaged tensions over mistrust in tech by assuring consumers that when a company oversteps, there will be repercussions.[309] This, in turn, allows data owners to feel safer in

303. While this Section discusses the harms of applying the GDPR to the United States, Section IV.C highlights advantageous aspects of the GDPR which should be applied to a federal US statute.

304. *See id.*

305. *See* discussion *supra* Section II.A.

306. *See* Andrew Martins, *Consumers Want a Federal Data Privacy Law*, BUS. NEWS DAILY (Jan. 23, 2020), https://www.businessnewsdaily.com/15467-consumers-want-federal-data-privacy-law.html [https://perma.cc/64Y7-DDEP]; *see also* Smith, *supra* note 291.

307. Techies are persons highly knowledgeable or enthusiastic about technology. *Techie*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/techie [https://perma.cc/8TAZ-G77N] (last visited Nov. 27, 2020).

308. *See* Ivana Kottasová, *These companies are getting killed by GDPR*, CNN BUS. (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html [https://perma.cc/EN54-HRWS]; *see also* Kate Fazzini, *Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators*, CNBC (May 5, 2019, 9:34 AM), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html [https://perma.cc/3XKU-2HB9].

309. *See* discussion *supra* Section III.A.

allowing companies access to their data, knowing the stakes for misuse are extremely high. Likewise, the cost to businesses for non-compliance equates to millions of dollars in fines.[310] These fines not only hold companies accountable for their actions but can also serve as a deterrent to other potential data-abusers.[311] Many companies, especially small business owners, fear for their financial futures with the GDPR's incommensurate fines.[312]

B. The United States Needs Stronger Data Protections, But Adopting Overbroad Regulation Would Be Overwhelming

The United States currently lacks proper data protection measures including regulation, oversight, and uniformity. Without stronger and clearer data protections, the government's case-by-case analysis of what constitutes data abuse[313] becomes blurred, leading to uneven application of various laws and arbitrarily set remedies. On the other hand, enacting a GDPR-sized regulation would stifle technological innovation and competition, and, as a result, threaten the United States' lead over China in the race to develop technology.

The United States' current data privacy enforcement measures lack uniformity. Absent a federally binding data protection statute, many companies are left to grapple with the myriad of state and vaguely applicable federal laws currently in place. Many companies become confused while trying to comply with these disorderly policies,[314] leading to some good faith businesses adhering to unnecessarily cautious practices at high costs.[315] Compliance complications may frustrate some companies, leading to their outright refusal to use data-insights. While this will certainly ensure the company does not run into data privacy non-compliance issues, it can also stifle future innovation and efficiency. For companies of any size, data insights

310. *See id.*

311. *See id.*

312. *See* discussion *infra* Section IV.B (assessing the GDPR's privacy violations and accompanying fines).

313. Data abuse and data misuse, while separate concepts, are used here interchangeably.

314. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/ZLT9-Z9RB].

315. *See* Sacks II, *supra* note 225.

can drive success. Using these insights does not exclusively entail marketing via targeted advertising. A company can use data to understand and improve performance in stores and online, understand consumers, and make more informed business decisions.[316] The government must provide more clarity regarding what compliance entails while preserving companies' ability to innovate.[317] Adopting the GDPR may solve America's enforcement-transparency problem but would be too costly for American businesses.

One of the biggest issues the GDPR faces is balancing protection for consumers against the cost to technological innovation by restricting developers' access to data. The CCPA, following many key GDPR principles, also faces this issue. The GDPR and the CCPA are rigid in what they require of businesses, and many fear this rigidity will hurt innovation and cost the United States its position on the global technology market.[318]

China is the only rival to the United States in the technological development sector. Currently, the United States is ahead of China in the AI industry which data fuels.[319] China, however, is quickly catching up, worrying some American technology experts and businesses.[320] The Huawei cyberespionage scandal highlighted some such American concerns.[321] The more exposed data is to Chinese corporations, the more autonomy users risk losing when handing control over to Huawei.[322] China leading the tech race would compromise more than just American innovation, but also threaten US national security as pervasive surveillance becomes the norm.[323]

---

316. *See Why Data is Important for Your Business*, *supra* note 2.

317. *See Will California's New Privacy Law Be Preempted? Federal Hearings and Public Comments Begin*, Dorsey & Whitney (Sept. 27, 2018), https://www.dorsey.com/newsresources/publications/client-alerts/2018/09/california-new-privacy-law [https://perma.cc/4ZVX-EXH8].

318. *See* Lin, *supra* note 23, at 278 (noting that the GDPR's rigid requirements will hurt innovation).

319. *See* Tom Simonite, *China is Catching up to the US in AI Research – Fast*, WIRED (Mar. 13, 2019), https://www.wired.com/story/china-catching-up-us-in-ai-research/ [https://perma.cc/JM2R-6V4H]; *see also Supra* Section II. *See also supra* note 31.

320. *See id.*

321. *See* discussion *supra* Section II.A.4 (discussing Huawei's cyberespionage scandal).

322. *See id.*

323. *See id. See also* discussion *supra* notes 264-71.

While testifying before Congress, Facebook founder and CEO Mark Zuckerberg urged legislators to recognize the careful balance between requiring entities to obtain consent for sensitive data collection and providing American companies room to innovate.[324] Over-regulation would place such stringent requirements on entities that, Zuckerberg argued, America would risk "fall[ing] behind Chinese competitors."[325] Zuckerberg is not wrong. Chinese companies, while complying with the CSL and 2018 Specification, are already hoarding mass amounts of user data.[326] For example, Chinese tech giant Tencent Holdings' social media apps QQ and WeChat collect user data through their messages, including those that users have deleted.[327] This data storage system is accessible to interested authorities, which includes the Chinese government.[328] WeChat rivals Apple's App Store in availability of instant in-app downloads.[329] With access to data from all of China's WeChat users, new regulation limiting much of American companies' access to American data will hold back the United States in the race for AI dominance.

The GDPR is so stifling to competition that even if the United States considers forming alliances to propel it to the front of the tech race, it is highly unlikely it will even consider collaborating with any of the twenty-seven EU member states

---

324. *See* Sacks II, *supra* note 225 (referencing Mark Zuckerberg's remark that "there's a balance that's extremely important to strike . . . where you obtain special consent for sensitive features like face recognition, but . . . we still need to make it so that American companies can innovate in those areas, or else we're going to fall behind Chinese competitors.").

325. Natasha Lomas, *Zuckerberg urges privacy carve outs to compete with China*, TECHCRUNCH (Apr. 10, 2018, 4:48 PM), https://techcrunch.com/2018/04/10/zuckerberg-urges-privacy-carve-outs-to-compete-with-china/ [https://perma.cc/BX5G-7777].

326. *See* Daniel Rechtschaffen, *How China's Tech Empire Is Being Used To Gather Data On Its Citizens*, FORBES (Jan. 9, 2018, 8:45 PM), https://www.forbes.com/sites/danielrechtschaffen/2018/01/09/how-beijing-built-a-tech-empire-and-then-turned-it-against-its-citizens/#7ebb468b4424 [https://perma.cc/PR22-443D].

327. *See* Lin, *supra* note 23 (citing Devin Coldewey, *Chinese Government Admits Collection of Deleted WeChat Messages*, TECHCRUNCH (Apr. 30, 2018, 2:17 PM), https://techcrunch.com/2018/04/30/chinese-government-admits-collection-of-deleted-wechat-messages/ [https://perma.cc/4KF2-3FFG]).

328. *See* Coldewey, *supra* note 327.

329. *See* Steven Millward, *China's Biggest Messaging App Is On A Collision Course With Apple*, TECHINASIA (Jan. 11, 2017), https://www.techinasia.com/wechat-instant-apps-versus-apple [https://perma.cc/E9WG-LYRT].

party to the GDPR and agree to abide by the GDPR's constrictions. Even if it does, the GDPR may not allow data information exchange within such collaborations. The data localization feature of the GDPR prohibits data sharing with non-EU member states lacking "adequate" levels of data protection.[330]

As a result of its enactment, companies scrambled to adapt their policies to the GDPR rules by the designated compliance deadline of May 25, 2018.[331] Instead of restructuring their entire practice in an incredibly short period of time, businesses instead began "pulling users out of reach of European Union privacy laws or blocking European Union citizens' access to online services" to avoid the GDPR's harsh repercussions for non-compliance.[332] Many tech magnates, including Chinese business mogul and Alibaba Group co-founder Jack Ma, feel the GDPR's rigidity is responsible for Europe's lack of technological innovation, keeping them out of the tech race by producing substantially fewer big tech firms as nations like the United States and China.[333] Ma, in response to the GDPR, urged legislators of all nations to focus less on tightening data-usage requirements and instead on enacting laws with innovative capacity in mind.[334] In support of his suggestion, Ma cited China as a prime example of how a lack of regulation was critical in allowing the early internet and mobile phones to "flourish" and enable "Alibaba to thrive."[335] He warned that Europe's tendency to regulate immediately upon hearing concerns over privacy issues will halt the union's technological development.[336] Ma gets to the heart of nations' apprehension to sign onto the GDPR: technology is the way of the future and

330. *See* Andrew Rossow, *The Birth Of GDPR: What It Is and What You Need To Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=a71f85e55e5b [https://perma.cc/C9TV-U3NJ].

331. *See* Park, *supra* note 1, at 1467-68.

332. *See id.* (citing Alex Hern, *Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law*, GUARDIAN (Apr. 19, 2018), https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law [https://perma.cc/E3Z5-H23F]). *See also* Bloomberg, *Blocking 500 Million Users Is Easier than Complying with GDPR*, FORTUNE (May 25, 2018), https://fortune.com/2018/05/25/gdpr-compliance-lawsuits/ [https://perma.cc/DJB4-HZJ3]).

333. *See* Soo, *supra* note 134.

334. *See id.*

335. *See id.*

336. *See id.*

under the GDPR's stifling regime, there will be no room for growth, knocking signatory nations aside as China and the United States continue to lead the world during this technological revolution.

Some feel Europe is right to regulate technology, citing concerns over citizens' rights and well-being rather than focusing on "money, power and technological innovation."[337] This belief, however, betrays a narrow conception of technology's role in our society and polarizes the issue. Ma is correct that legislation should consider technological progression needs in adopting consumer protection laws. Technology is at the forefront of society and ignoring the need for continued development not only disregards our general reliance on technology, but reduces the likelihood of future tech-assisted breakthroughs for individuals or companies.

In addition to over-regulating tech, the administrators of the GDPR wield the regulation's punitive power too aggressively. The fines GDPR regulation committees impose on data abusers may be too harsh in certain scenarios, especially when small-businesses are subjected to the GDPR's one-size-fits-all punitive system.[338] Under the GDPR, one violation can cost startups their business. To ensure compliance, a business may be spending an exorbitant amount on compliance officers, licenses, and reporting measures, before even beginning its venture. Additionally, the business must sacrifice time that would be better spent developing the startup to ensure survival of the venture itself.[339] Once in place, the fines continue, becoming even more expensive for a business' failure to maintain compliance standards.[340] According to the Financial Times, the more governmental oversight there is over a business's

337. *Why Europe is right to regulate tech: Jack Ma got it wrong*, SOUTH CHINA MORNING POST (May 22, 2019, 5:00 PM), https://www.scmp.com/comment/letters/article/3010989/why-europe-right-regulate-tech-jack-ma-got-it-wrong [https://perma.cc/ZSY5-5DP7].

338. *See infra* text accompanying note 339. *But see* Stephen P. Mulligan et al., Cong. Rsch. Serv., R45631, Data Protection Law: An Overview 46-47 (2019).

339. *See* GDPR, *supra* note 18, art. 83 (outlining finable infringements); *see also* Kottasová, *supra* note 308 (stating "[c]omplying with the new regulations isn't cheap, and experts say the world's biggest companies are spending tens of millions of dollars to prepare. Smaller companies that do not have the same resources are struggling.").

340. *See* GDPR, *supra* note 18, art. 83 (discussing infringements that carry harsher penalties for violations such as data processing and consent violations articulated in Article 5).

daily operations, the slower the growth of the business in a time where speed is one of the most important factors in technological development.[341] In contrast, the CCPA fixes a maximum fine on violations at US$ 7,500, an amount that is practically negligible to tech giants. [342] Further, the statute only punishes intentional violations which result in data breaches.[343]

Proponents of the GDPR cite consumer satisfaction at the enactment of the regulation. In the wake of numerous data-abuse scandals, the GDPR helps victims feel vindicated through its enforcement of protections and implementation of stronger penalties for transgressors. Advocates also emphasize the notion of a society more trusting of corporations as an effect of more transparent data-usage practices.[344] In theory, people may begin feeling more comfortable living alongside technology by understanding how companies use their data for good. This, in turn, may create technology and AI investors where once these individuals felt distanced from technology. Additionally, supporters of the GDPR feel the European Union's adoption of the regulation will encourage other jurisdictions to increase their regulation and legislation of data privacy protection, as China has.

C. What the United States Should Do

The United States should enact a federally binding privacy law. This law must protect citizens, provide clear compliance guidelines and standards for corporations, and allow room for innovation. To accomplish these goals, the new statute should preempt state laws for uniformity purposes. Allowing states to

341. *See* Guy Chazan, *SAP Raises Fears Over European Union Data Privacy Rules*, FIN. TIMES (Jan. 15, 2017), https://www.ft.com/content/22d5e078-d9a1-11e6-944b-e7eb37a6aa8e [https://perma.cc/U4PQ-FLCM] ("The penalties were too high, "especially for just a single violation.' . . . The more bureaucracy, the more complexity you have in your business segment, the harder it is to grow fast, and speed is what matters these days . . . .").

342. *See* CAL. CIV. CODE § 1798.155(b) (2018) (requiring the maximum fine placed on a data breach be $7,500).

343. *See id.*

344. *See* Kevin Cochrane, *To Regain Consumers' Trust, Marketers Need Transparent Data Practices*, HARV. BUS. REV. (June 13, 2018), https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices [https://perma.cc/4ASW-VZXZ].

continue creating their own specifications exacerbates the issue of corporations fronting the cost of complying with disparate regulations and risking accidental non-compliance. While allowing states to use the federal act as a default regulation may provide for greater safety measures within that region, the burden of state-by-state adaptations of the federally binding statute will overwhelm compliance officers, frustrating technological innovation efforts. Data transfers, whether from owner to processor or processor to third party, etc., implicate interstate commerce, triggering a host of additional compliance issues with local level regulation.

As it currently stands, legislators are submitting numerous local GDPR-sized bills, flooding their state legislatures at a rapid rate.[345] Ensuring continued compliance in an evolving legal landscape is a business in itself and would be a "logistic nightmare."[346] A single, federal privacy bill with clear terms would ameliorate the flooding problem the current pending legislation is about to create. In unifying compliance requirements, this single bill would take the pressure of accidental non-compliance off businesses and leave them free to do what they do best: innovate. The GDPR's uniformity is one of its redeeming qualities. As stifling as it is, the GDPR provides a uniform standard for compliance so companies and consumers know their rights and obligations. However, the GDPR and the CCPA, while successful in some capacities, might not be suitable for federal application, placing too much responsibility on tech operators unfamiliar with legal compliance operations.[347]

To accomplish the goal of providing clear compliance standards, new legislation should feature clear terms that frame

345. *Comparison Chart of Pending CCPA and GDPR-like State Privacy Legislation*, AKIN GUMP (May 29, 2019), https://www.acc.com/sites/default/files/2019-06/2019-05-30%20Akin%20Gump%20HANDOUT-State%20Privacy%20Legislation%20Comparison%20Chart.pdf [https://perma.cc/Y6UG-TJT9].

346. *See* Lin, *supra* note 23, at 277 (citing Julie Bernard, *Consumer Data Privacy: Why We Need a (Single) Federal Law*, FORBES (Mar. 29, 2019, 6:00 AM), https://www.forbes.com/sites/forbesagencycouncil/2019/03/29/consumer-data-privacy-why-we-need-a-single-federal-law/#6e7d8687623f [https://perma.cc/PU7R-9ZHR]).

347. *See* Lin, *supra* note 23, at 277 (citing Fahmida Y. Rashid, *Congress May Consider a U.S. Version of GDPR*, DECIPHER (Nov. 9, 2018), https://duo.com/decipher/congress-may-consider-a-us-version-of-gdpr [https://perma.cc/8AUS-CNQC]).

compliance in an easily understandable way. Some could argue broader laws allow for greater flexibility—a principle-based regulatory regime may be more accommodating to startups than a rules-based approach. On the other hand, vaguely defined key legal terms can lead to confusion regarding what constitutes compliance.[348] With clearer terms, companies will have a better sense of what compliance entails. This seemingly obvious solution will help entities continue to innovate while complying with the law and without placing an undue burden on them.

Many agree that data processors should first obtain consent before mining a user's data.[349] Consent, however, is not as clear a term as it may seem. One data privacy principle providing for more transparent practices includes requiring "Opt-In," rather than "Opt-Out" consent. Opt-In consent requires data processors to receive the data subjects' "express, affirmative and informed consent" before processing their data.[350] This can either mean: (1) a subject affirmatively agrees to allow a processor complete use and disclosure of his data or, (2) by agreeing to the processor's terms, the user allows the processor to use the data of any other on the same browser with the same IP address on which the original user accepted the processor's terms.[351] For example, in this second definition, in a household that shares one computer, one resident agreeing to a processor's terms automatically means the processor may use any data stored on the computer, regardless of which household member generated such data. These two constructions of the term "Opt-In requirement" represent only a couple of ways in which "consent" may be interpreted. To avoid the ambiguity in the situation set

348. *See* Lin, *supra* note 23, at 278 (citing *The CCPA - Making Things Worse*, ANA (Mar. 4, 2019), https://www.ana.net/blogs/show/id/rr-blog-2019-01-The-CCPA-Making-Things-Worse [https://perma.cc/5K4P-9RDW]); *see also* Sam Sabin, *Fresh Off GDPR, Companies Puzzle Over Complying With California's Privacy Law*, MORNING CONSULT (Dec. 18, 2018, 1:00 PM), https://morningconsult.com/2018/12/18/fresh-off-gdpr-companies-now-have-to-prepare-for-californias-privacy-law/ [https://perma.cc/4HWH-KKCC] ("[CCPA] creates 'unworkable obligations'").

349. *See* Thomas C. Redman & Robert M. Waitman, *Do You Care About Privacy as Much as Your Customers Do?*, HARVARD BUS. REV. (Jan. 28, 2020), https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do [https://perma.cc/QQ2B-8F4Q].

350. Tomain, *supra* note 50, at 4.

351. Nicklas Lundblad & Betsy Masiello, *Opt-In Dystopias*, 7 SCRIPTED 155, 158 (2010).

out above, this new privacy statute should clearly define consent while establishing stringent compliance standards.

A federal data privacy statute should require processors obtain consent to data gathering, processing, mining, and distributing from the user, with an option for users to decline all data-usage methods while retaining access to the processor's services. The processor may incentivize sharing data but may not coerce consent. The processor must first obtain consent from the data subject before sharing his data with a third party. The data processor must explicitly state to whom the user's data is distributed and for what purpose(s). Each time the processor wants to share user data with another party, the processor must re-obtain consent from the original user.

Even with clear terms, some processors fear obtaining consent will be detrimental to their ability to process data and thus limit their ability to innovate.[352] On the contrary, most tech users will not care to read terms and conditions and will often click "I agree" when prompted. For the minority who have concerns about their data's usage, however, they can opt out of data-share feature without having to forego using a company's product. So, some may question why service providers and regulators should care about the scant minority of users who do not want to share their data in exchange for using a company's services. Assuming only one percent of the US population cares to read terms and conditions and would have a problem with sharing their data, that equals about 3.3 million people.[353] The services these millions of Americans cannot use include those of giants like Google, Amazon, Walmart, and more. While one percent may seem insignificant, it is enough users to cause potential economic turmoil for even some of the largest

352. *See, e.g.*, Daniel Castro & Michael McLaughlin, *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence*, INFO. TECH. & INNOVATION FOUND. (Feb. 4, 2019), https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence [https://perma.cc/HZM4-GQT3] ("Policies that require firms to get prior consent before using commercial applications of AI, including facial recognition, can actually delay improvements in consumer experiences.").

353. *See Population Estimates, July 1, 2019 (V2019) – United States: Quick Facts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045219 [https://perma.cc/LLH8-ELUM] (last visited Mar. 2, 2021).

corporations. Google's annual revenue is US$ 160.74 billion.[354] In the US alone, Google has 246 million users.[355] This means a loss of one percent of Google's US users will cost Google over US$ 1.607 billion per year. This example shows the impact to massive corporations: the consequences of losing even one percent of customers overnight to average-sized businesses would be devastating.

While corporate data mishandling scandals continue to surface as quickly as levels of user mistrust grow, no amount of abuse is likely to push users completely offline and end society's dependence upon the internet. Despite rising data misconduct, few users have followed through on their threats of shutting down their social media accounts.[356] For this reason, consumer protection needs to be at the forefront of drafters' concerns, alongside the idea that reliance upon American-developed technology will only improve the United States' global market stance.

A new federal privacy bill should explicitly establish a regulatory enforcement committee. If the drafters of the new law choose to accept that regulatory oversight is the FTC's role, it should clearly delineate the FTC's powers. The best idea would be to establish a designated task force exclusively committed to data privacy security, whether that be a bureau under the FTC or a new federal agency altogether. This task force would replace the current redundancy of compliance officers, centralizing oversight in one task force. Compliance standards as well as repercussions should be clearly enumerated in the regulation along with

354. *See* J. Clement, *Google: annual revenue worldwide 2002-2019*, STATISTA (Feb. 5, 2020), https://www.statista.com/statistics/266206/googles-annual-global-revenue/ [https://perma.cc/J7R9-9CX8].

355. *See* Deyan Georgiev, *111+ Google Statistics and Facts That Reveal Everything About the Tech Giant*, REV. 42 (Nov. 21, 2020), https://review42.com/google-statistics-and-facts/ [https://perma.cc/Z2NY-S3CP].

356. *See* Michael Gold, *Senators Had a Lot to Say About Facebook. That Hasn't Stopped Them From Using It.*, N.Y. TIMES (Apr. 12, 2018), https://www.nytimes.com/2018/04/12/us/politics/facebook-senators-usage.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer [https://perma.cc/2L2S-DFRH]; *but see* Tiffany Hsu, *For Many Facebook Users, a 'Last Straw' That Led Them to Quit*, N.Y. TIMES (Mar. 21, 2018), https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html [https://perma.cc/TQX2-RTUT].

explicit data storage expiration dates, setting clear guidelines for this new task force's powers.

With this new committee, the United States should hold accountable corporations who have misused user data by enacting uniform, binding legislation that calls for more transparent data-usage practices. "More transparent practices" can include using "explainable AI"[357] and obtaining consent from consumers before sharing their data. Explainable AI refers to only using computer algorithms that humans can comprehensively understand, thus allowing coders to know what decisions the computer makes and why.[358] The more data consumers give to tech companies, the more these companies can develop and increase the United States' tech standing, but many question if they can trust the hands in which their data ends up.[359] Explainable AI practices may alleviate these fears by producing coders capable of explaining how computers use data and to what ends. The GDPR enumerates similar practices, some of which the Digital Accountability and Transparency to Advance Privacy Act ("Data Privacy Act") has already introduced in the Senate.[360]

Like the GDPR, the CCPA provides that data breaches are not the only form of non-compliance.[361] Where there are no breaches, the company in question will face no penalties, regardless of whether other company policies were compliant.[362] This system may, on its face, seem to promote companies acting

357. See Ron Schmelzer, *Understanding Explainable AI*, FORBES (July 23, 2019, 7:12 AM), https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/?sh=701802cb7c9e [https://perma.cc/HX3D-NA7R] ("The lack of explainability and trust hampers our ability to fully trust AI systems. We want computer systems to work as expected and produce transparent explanations and reasons for decisions they make. This is known as Explainable AI (XAI).").

358. *See id.*

359. *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/5X6Q-CHLU].

360. Digital Accountability and Transparency to Advance Privacy Act, S. 583, 116th Cong. (2019).

361. *See generally* Alice Marini et al., *Comparing privacy laws: GDPR v. CCPA*, DATAGUIDANCE & FUTURE PRIV. F., https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [https://perma.cc/8ELV-2YM2] (last visited Mar. 2, 2021).

362. *See* CAL. CIV. CODE § 1798.155 (2018).

to restrict the number of data breaches that occur. However, these laws merely incentivize companies to not get caught instead of promoting the consumer interest in corporations instituting sufficient data protection measures.[363]

To determine proper damages for non-compliance, a federal law should include a percentage-based formula. Some observers propose an algorithm that suggests fining a company for a "maximum of two percent of its global revenue for its first violation, and four percent for its second violation, etc."[364] This proportionality principle would ease startups' concerns over being fined gross sums for mistakes at a time when they are unlikely to have a developed compliance framework. At the same time, major corporations and tech giants cannot brush aside the fines which can amount to millions, dependent upon the company's revenue.

V. CONCLUSION

While the world continues to advance toward an AI-driven future, nations around the world have taken steps to protect consumer data privacy interests. The European Union enacted the GDPR to secure individual data interests against corporate misuse of privileged information. The expansive legislation, however, neglects the businesses from which it protects consumers, leaving many companies confused or unwilling to comply with such stringent requirements that threaten to halt technological advancement in favor of securing citizens' data. China, on the other hand, historically affords its citizens few privacy rights, yet even the surveillance state has enacted measures to prevent against unfettered data-collection. Lagging behind the two other bodies, the United States has several local acts aimed at residents of certain states but lacks a federally binding data privacy statute. With China and the United States paving the way through this technological revolution, the United States must step up to ensure its citizens' privacy interests are protected, while guaranteeing American companies' ability to innovate will not be stifled by over-regulation of data access.

363. *See* O'Connor, *supra* note 314.

364. Greater detail is discussed in Lin, *supra* note 23, at 279.

In an ideal world, companies would voluntarily implement privacy policies that guarantee consumers fair practices and promise not to overstep privacy bounds. Realistically, the likelihood of companies acting against their best interests in favor of their customers is impractical and foolish. Unreasonable as well is the idea that companies would willingly or even have the means to ensure their policies comply with countless local-level statutes. The United States would therefore benefit from a federally binding data protection statute whose requirements are clearly and concisely spelled out, unlike those of the GDPR. This new statute should incorporate successful aspects of the GDPR, the CSL, and the 2018 Specifications, but must weigh protection against barriers to innovation to maintain its stance in the global AI race. In addition to easing the concerns of US citizens, implementing this new statute may make the thought of living alongside technology more palatable to wary consumers. This new future may encourage freely sharing certain types of data with corporations who promise to use and develop it into a societally advantageous program.

Where once the thought of sharing data with companies or even the government seemed overwhelming, a clearly established and comprehensive data privacy statute may encourage participation on the global tech market and creative opportunities for individuals who had previously closed themselves off to such advancements. In enacting such a law, the United States could see tech investors emerge from industries not traditionally connected to technology, more individuals joining the tech workforce than before, and of course, fewer instances of corporate data misuse. All these aspects can contribute to the United States securing its place as the winner in the AI race.