A DANGEROUS GAME: CHINA'S BIG DATA ADVANTAGE AND HOW THE U.S. SHOULD RESPOND

Xiaofeng Lin[*]

TABLE OF CONTENTS

* J.D. University of Illinois College of Law, 2020. I would like to thank Professor Faye E. Jones for her valuable feedback on this note. Additionally, I would like to thank Professor Verity Winship for her input. I also thank the entire JLTP staff for their hard work. Lastly, I want to say thank you to my dog, Bentley, for not being judgmental when I stayed up all night drafting this Note.

I. INTRODUCTION

The fourth industrial revolution is no longer just getting started[1]—it is in full swing.[2] Big Data is a major part of this historical event. Humankind produced as much data in 2016 as it did in all of history through 2015.[3] Just like many other new technologies, Big Data is a double-edged sword.[4] But the stakes are unprecedently high here, partly because the "Internet of Things," which is just around the corner, could make gathering data much easier and almost ubiquitous.[5] Currently, concerns over privacy and Big Data are already a heated topic. But the anxieties we now have may seem minor in the near future when the Internet of Things is fully integrated into our daily lives.[6] According to a report by Cisco, it is expected that by 2030, 500 billion devices equipped with sensors will be connected to the Internet.[7] Imagine that one day you are not only monitored by the people around you but also by every streetlight and by the smart speaker in your bedroom.

Big Data is a Pandora's box, but the promise of technological advances,[8] a more stable nation,[9] and a more efficient economy[10] are too inviting for some countries to ignore. For example, China has used Big Data for many purposes.[11] From detecting students' mood in the class room[12] to identifying criminals at

1. Bernard Marr, *The 4th Industrial Revolution is Here - Are You Ready?*, FORBES (Aug. 13, 2018), https://www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/.

2. Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence*?, SCIENTIFIC AMERICAN (Feb. 25, 2017), https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

3. *Id*.

4. Daniel Riedel, *The Duality of Big Data: The Angel and the Demon*, WIRED, https://www.wired.com/insights/2014/10/duality-big-data/ (last visited Mar. 25, 2019).

5. *See infra* Section II.B (showing that the Internet of Things will include hundreds of millions of sensors).

6. *Id*.

7. CISCO, INTERNET OF THINGS (2016), https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.

8. JAMES MANYIKA ET AL., BIG DATA, THE NEXT FRONTIER FOR INNOVATION, COMPETITION AND PRODUCTIVITY 1–2 (2011).

9. Willy Wo-Lap Lam, *Beijing Harnesses Big Data & AI to Perfect the Police State*, JAMESTOWN (July 21, 2017), https://jamestown.org/program/beijing-harnesses-big-data-ai-to-perfect-the-police-state/.

10. Natalija Koseleva & Guoda Ropaite, *Big Data in Building Energy Efficiency: Understanding of Big Data and Main Challenges*, 172 PROCEDIA ENGINEERING 544, 544 (2017), https://www.sciencedirect.com/science/article/pii/S1877705817305702#bibl0005.

11. *See infra* Section II.A (demonstrating that China has an ambitious plan to make use of its abundant data).

12. Tara Francis Chan, *A School in China is Monitoring Students with Facial-Recognition Technology That Scans the Classroom Every 30 Seconds*, BUSINESS INSIDER (May 20, 2018), https://www.businessinsider.com/china-school-facial-recognition-technology-2018-5.

large among concert goers,[13] banning deadbeat debtors from buying luxury goods,[14] and identifying jaywalkers by how they walk,[15] China seems to embrace data gathering and its applications without hesitation. China is playing a dangerous game, and the United States cannot afford to stand by and do nothing. Big Data and its applications have the potential to fundamentally transform societies and economies, especially high-tech industries.[16]

Every industrial revolution witnesses the rise and fall of civilizations.[17] The First Industrial Revolution transformed Britain into "the empire on which the sun never sets."[18] With the help of the Second Industrial Revolution and the digital revolution, the U.S., a former British colony, turned into the most powerful country in the world.[19] Meanwhile, the Qing dynasty of China isolated itself from the outside world in the belief that its unparalleled population and wealth would shelter its "Mandate of Heaven."[20] The Qing dynasty was wrong.[21] It missed out on the First and Second Industrial Revolutions, which brought China into the Century of Humiliation.[22] China's advantages, accumulated throughout its thousands of years of history, were shattered by newer advantages acquired by other countries in a just few decades.[23] Today, the U.S. is not in a good position to embrace the Fourth Industrial Revolution.[24] Its citizens see data gathering as abominable.[25] It does not have a federal law

13. Yujing Liu, *Facial Recognition Tech Catches Fugitive in Huge Crowd at Jacky Cheung Cantopop Concert in China*, SCMP (Apr. 12, 2018), https://www.scmp.com/news/china/society/article/2141387/facial-recognition-tech-catches-fugitive-among-huge-crowd-pop.

14. Tim Cushing, *Chinese Court Creates App To Alert Citizens Of Deadbeat Debtors In Their Area*, TECHDIRT (Jan. 29, 2019), https://www.techdirt.com/articles/20190128/10321941475/chinese-court-creates-app-to-alert-citizens-deadbeat-debtors-their-area.shtml.

15. Kristin Houser, *China Can Now Identify a Citizen Based on Their Walk*, FUTURISM (Nov. 6, 2018), https://futurism.com/the-byte/gait-recognition-china-surveillance.

16. *See infra* Section III.A.2 (arguing that Big Data is the lifeblood of AI).

17. Moses Abramovitz, *Catching Up, Forging Ahead, and Falling Behind*, 46 J. ECON. HIST. 385, 385–406 (1986).

18. *See* Hakan Kırtay, *The Empire on Which the Sun Never Sets: The British Empire*, ACADEMIA, https://www.academia.edu/25637246/The_Empire_on_Which_the_Sun_Never_Sets_The_British_Empire (last visited Mar. 25, 2019) (discussing impact of the First Industrial Revolution on Great Britain).

19. *See* Rebecca Beatrice Brooks, *The Industrial Revolution in America*, HISTORY OF MASSACHUSETTS BLOG (Apr. 11, 2018), https://historyofmassachusetts.org/industrial-revolution-america/ (discussing the impact of the Industrial Revolution on the United States growth).

20. Xu Mingde (徐明德), *Lun Shisi Zhi Shijiu Shiji Zhongguo De Biguansuoguo Zhengce* (论十四至十九世纪中国的闭关锁国政策) [*On China's Policy of Seclusion from 14th to 19th Century*], HAI JIAO SHI YANJIU (海交史研究) [MARITIME HISTORY STUDIES], no. 1, 1995, at 19 (available at http://www.cqvip.com/qk/83514x/199501/4001247655.html). *See* Fercility, *The Qing Dynasty—China's Last Dynasty*, CHINA HIGHLIGHTS (Jan. 10, 2019), https://www.chinahighlights.com/travelguide/china-history/the-qing-dynasty.htm (giving brief history of the Qing Dynasty).

21. Although some historians argue the Qing Dynasty's isolationist policy was in response to the British Empire's economic aggression, the ill-considered policy further weakened China's ability to innovate and catch up with Western powers. *See* Xu Yinqi (徐映奇), *Qingdai Biguansuoguo Zhengce Xinlun* (清代闭关锁国政策新论) [*A New Theory on the Qing Dynasty's Isolationist Policy*], GUANZHOU SHEHUIZHUYI XUEYUAN XUEBAO (广州社会主义学院学报) [JOURNAL OF GUANGZHOU SOCIALIST COLLEGE], no. 1, 2004, at 69 (available at http://www.cqvip.com/QK/88312X/200401/1001242311.html).

22. Fercility, *supra* note 20.

23. *Id.*

24. *See infra* Section III.B (discussing the impact of public perception of privacy in the U.S.).

25. *See infra* Section III.B.3 (showing that Americans are generally wary of data gathering).

regulating data and privacy.[26] Its government would go to great expense to build a border wall but did not implement a national artificial intelligence strategy until February 2019, almost two years after China released its version.[27]

This article will argue that China has an advantage over the U.S. when it comes to Big Data and AI, and therefore, the U.S. needs to draft a federal privacy law as soon as possible in order to secure its citizens' data and prepare itself for the global battle over Big Data and its use in AI. This article will also argue that in order to prevent the global economy from being further balkanized, the U.S. should resist the global data localization trend that China participates in. Part II of this Note provides relevant background knowledge, including how China utilized its low human rights dividend, China's plans to upgrade its industries in the wake of its disappearing demographic dividend,[28] the impact of the Internet of Things on data gathering, and how data localization is the latest trend in the balkanization of the Internet. Part III has three sections. Section A explains why data gathering might be necessary although it violates citizens' right to privacy. Section B provides an analysis of how different laws and social attitudes in the U.S. and China might impact the Big Data industries in each country. Section C explains that the data localization trend will likely perpetuate any gap in data gathering between the two countries. Part IV proposes a single federal privacy law and advocates for the U.S. to resist the trend of data localization through the World Trade Organization (WTO) and bilateral agreements.

II. BACKGROUND

A. China's Plans: From Cheap Labor to Cheap Data

Since China joined the WTO, it has become the "world's factory."[29] An important part of the reason behind China's rapid economic growth lies in its cheap and abundant labor force, which is termed its "demographic dividend."[30] In the past two decades, China's demographic dividend was exploited through prohibition of union organization and poor enforcement of labor laws.[31] Some experts thus coined the term "low human rights advantage"[32] to explain China's rapid growth compared to the U.S. Due to this advantage, China was able to manufacture simple products at prices that were significantly lower than those

26. *See infra* Section III.B.2 (demonstrating that the U.S. only has a patchwork of laws governing privacy).

27. Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019) (available at https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/).

28. *China's Demographic Dividend Disappearing*, XINHUA (Jan. 28, 2013), http://www.chinadaily.com.cn/china/2013-01/28/content_16182243.htm.

29. Prableen Bajpai, *Why China Is "The World's Factory,"* INVESTOPEDIA (Oct. 22, 2014), https://www.investopedia.com/articles/investing/102214/why-china-worlds-factory.asp.

30. DAVID E. BLOOM, DAVID CANNING & JAYPEE SEVILLA, THE DEMOGRAPHIC DIVIDEND 45 (2003) (exploring possible relationships between demographic change and economic performance).

31. Dana C. Nicholas, Note, *China's Labor Enforcement Crisis: International Intervention and Corporate Social Responsibility*, 11 SCHOLAR 155, 168 (2009).

32. Hui Qin, *China's Low Human Rights Advantage*, CHINA RIGHTS FORUM, no. 1, 2009, at 85.

produced by its Western competitors.[33] In the beginning of the twenty-first century, offshoring from Western countries to China could cut costs by eighty-five to ninety percent.[34] More and more Western companies thus joined the trend of offshoring, and some even had to disclose their plans of outsourcing to avoid falling stock prices.[35]

Although China's labor is no longer as cheap, and its population is aging, the term "low human rights advantage" might remain relevant in the age of big data due to inefficient data protection in China.[36] *Made-in-China* has long been seen as a synonym for low quality,[37] which is a phenomenon the Chinese government is determined to change.[38] In May 2015, China's Prime Minster Li Keqiang announced the *Made in China 2025* Plan, aiming to upgrade China's manufacturing industries, especially high-tech industries.[39] Localization of data is one of the plan's central components.[40] Later, in 2017, China's State Council published its "Next Generation Artificial Intelligence Development Plan" (AI Plan),[41] and big data is the lifeblood of AI.[42] The Chinese government's determination to upgrade its industries, as reflected by *Made in China 2025* and the AI Plan, manifests its support for local big data industries.[43] Although China enacted its Cybersecurity Law in 2016 it is not surprising that the law has been heavily criticized for vagueness and signs of trade protectionism.[44] However, the most important reason for the inefficient data protection in China may not be legal.[45] Chinese citizens in general are much less enthusiastic about their right to privacy, compared to Americans.[46] All these factors allow Chinese tech companies to tap into the country's abundant data.[47]

---

33. S. James Boumil III, *China's Indigenous Innovation Policies Under the TRIPS and GPA Agreements and Alternatives for Promoting Economic Growth*, 12 CHI. J. INT'L L. 755, 758 (2012).

34. Colleen Walsh Schultz, *To Offshore Or Not To Offshore: Which Nations Will Win A Disproportionate Share Of The Economic Value Generated From The Globalization Of White-Collar Jobs?*, 29 HOUS. J. INT'L L. 231, 241 (2006).

35. Mark B. Baker, *"Awakening The Sleeping Giant:" India And Foreign Direct Investment In The 21st Century*, 15 IND. INT'L & COMP. L. REV. 389, 396 (2005).

36. Sophia Yan, *Made in China' Isn't So Cheap Anymore, And That Could Spell Headache for Beijing*, CNBC (Feb. 27, 2017, 12:37 AM), https://www.cnbc.com/2017/02/27/chinese-wages-rise-made-in-china-isnt-so-cheap-anymore.html.

37. Paul Midler, *Why 'Made in China' is a Mark of Shame*, TEL. (Jan. 10, 2010, 6:46 PM), https://www.telegraph.co.uk/finance/comment/6962703/Why-Made-in-China-is-a-mark-of-shame.html.

38. Dan Markus & Nick Marro, *'Made in China' Now 'Made by China': Update*, US-CHINA BUS. COUNCIL (May 27, 2015), https://www.uschina.org/'made-china'-now-'made-china'-update.

39. INST. FOR SEC. & DEV. POL'Y., MADE IN CHINA 2025 1, 1 (2018).

40. *Id.* at 9.

41. Pablo Robles, C*hina Plans to Be a World Leader in Artificial Intelligence by 2030*, SCMP (Oct. 1, 2018), https://multimedia.scmp.com/news/china/article/2166148/china-2025-artificial-intelligence/index.html.

42. Carlos Melendez, *Data Is The Lifeblood Of AI, But How Do You Collect It?*, INFOWORLD (Aug. 8, 2018), https://www.infoworld.com/article/3296044/data-is-the-lifeblood-of-ai-but-how-do-you-collect-it.html.

43. *See* Ji Dengqiang, *Big Data In China: From Myth To Political Economy*, DOC RES. INST. (July 9, 2018), https://doc-research.org/2018/07/big-data-china-myth-political-economy/ (explaining that big data carries multiple political and economic implications).

44. Sue-Lin Wong, Michael Martina, *China Adopts Cyber Security Law in Face of Overseas Opposition*, REUTERS (Nov. 6, 2016), https://www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049.

45. *See infra* Section III.B.3 (noting that Chinese citizens generally supports data gathering).

46. *Id.*

47. Mosha Morak, *Chinese Apps are Collecting Way Too Much Data*, ABACUS (Jan. 2, 2019, 5:55 AM), https://www.abacusnews.com/digital-life/chinese-apps-are-collecting-way-too-much-data/article/3000377.

China's cheap labor once incentivized the massive outsourcing of manufacturing industries from the U.S. to China.[48] One might wonder whether China will make use of the so-called low human rights advantage again to execute its ambitious plans by utilizing its cheap and abundant data.

B. The World That Is More Connected Than Ever

The Internet of Things is poised to make the world much more connected.[49] The Internet of Things has been defined in many ways. On the physical level, simply put, it is a giant network of objects able to collect and exchange data.[50] But the Internet of Things does not just connect every electronic device to the Internet;[51] it also features smart devices that communicate with each other, forming an ecosystem.[52] A broad range of existing objects can be turned into smart devices within the ecosystem, including watches, cars, fridges, and even railway track.[53]

Every second this ecosystem generates a huge flow of data, and this is where big data comes into play.[54] The concept of big data existed long before the Internet of Things,[55] but it is safe to say that the Internet of Things will bring a revolution to the way big data is handled.[56] Big data analytics tools are necessary to process the information influx generated by the Internet of Things, and in turn the Internet of Things will provide unlimited fuel to big data applications.[57] It is estimated that the number of smart devices will explode from 2 billion in 2016 to 200 billion by 2020,[58] and the Internet of Things will generate 4.4 trillion GB of data by 2020.[59] More data generated will in turn substantially transform the high-tech industries, as discussed in Section III.A of this Note.

However, the Internet of Things is making big data more controversial in terms of right to privacy. The number of smart devices that will be laden with sensors means that technology companies will be able to exploit consumers' rich

48. *See supra* notes 37–38 and accompanying text (identifying China's cheap labor cut cost for Western companies).

49. Sanjay Sarma, *The Internet of Things: Roadmap to a Connected World*, MIT TECH. REV. (Mar. 11, 2016), https://www.technologyreview.com/s/601013/the-internet-of-things-roadmap-to-a-connected-world/.

50. *Id.*

51. Jacob Morgan, *A Simple Explanation of "The Internet of Things,"* FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#572b4c086828.

52. Craig Swanson & Ron Sokolov, *Internet of Things: Move Past the Rhetoric and Focus on Success*, BOOZ ALLEN HAMILTON (Dec. 2014), https://www.slideshare.net/CiscoPublicSector/internet-of-things-move-past-the-rhetoric-and-focus-on-success.

53. Savaram Ravindra, *Understanding The Relationship Between IoT And Big Data*, JAXENTER (Oct. 18, 2017), https://jaxenter.com/relationship-between-iot-big-data-138220.html.

54. *Id.*

55. *Id.*

56. Ashish Goyal, *How Will the Internet of Things (IoT) Impact Big Data?*, DATAVERSITY (Oct. 3, 2018), https://www.dataversity.net/will-internet-things-iot-impact-big-data/.

57. Ronald Van Loon, *4 Ways Businesses Use The IoT to Fuel a Data-Driven Economy*, SIMPLILEARN (Oct. 6, 2018), https://www.simplilearn.com/ways-businesses-use-iot-article.

58. ORACLE, ENERGIZE YOUR BUSINESS WITH IOT ENABLED APPLICATIONS (2015).

59. *Id.*

data in almost real-time, and even our homes will no longer be safe.[60] The amount of data itself also brings risk.[61] It is reported that businesses are already struggling to manage the data generated daily, mostly due to a lack of adequate measures in place to secure the large amount of data gathered.[62] This is probably an important reason why the years 2017 and 2018 saw a seventy-five percent increase in data breaches.[63] When the Internet of Things finally comes, the burden on businesses to secure data will only be heavier.[64] We are waiting for a tsunami of data privacy violations, but, as discussed previously, the U.S. still does not have a comprehensive federal law to regulate data and privacy.[65]

C. The World That Is Heading Toward Digital Balkanization

Facebook was blocked in China due to national security concerns.[66] Similarly, Huawei is locked out of the U.S. market due to national security concerns.[67] Uber, Google, and Amazon are successful around the globe, except in China, the world's largest digital market.[68] Chinese phone makers are popular around the world, even including Europe,[69] but it is hard to find their presence in the U.S.[70] Whether these phenomena exist because of technical issues[71] or politics,[72] they reflect a more fundamental issue, that the U.S. and China now have two distinct digital ecosystems.[73] The term "balkanization of the Internet"[74] describes this state of affairs well.

60. Nicholas Fearn, *What the Internet of Things (IoT) Means for Data Security*, IT PRO (Mar. 28, 2018), https://www.itpro.co.uk/internet-of-things-iot/30844/what-the-internet-of-things-iot-means-for-data-security.

61. *Id.*

62. *Id.*

63. Aaron Hurst, *Data Breach Reports See 75% Increase in Last Two Years*, INFORMATIONAGE (Sept. 3, 2018), https://www.information-age.com/data-breach-reports-increase-last-two-years-123474521/.

64. *See* ORACLE, *supra* note 58 (highlighting that much more data are created).

65. *See infra* Section III.B.2 (the U.S. only has a patchwork of laws governing privacy).

66. Kristina Zucchi, *Why Facebook is Banned in China*, INVESTOPEDIA (Oct. 22, 2019), https://www.investopedia.com/articles/investing/042915/why-facebook-banned-china.asp.

67. Roger Cheng, *Why Some Of The Flashiest Android Phones Aren't In The US*, CNET (Mar. 27, 2018, 3:00 PM), https://www.cnet.com/news/why-some-of-the-flashiest-huawei-android-p20-p20-pro-mate-10-pro-phones-arent-in-the-us/.

68. Feng Li *Why Western Digital Firms Have Failed in China*, HARV. BUS. REV. (Aug. 14, 2018), https://hbr.org/2018/08/why-western-digital-firms-have-failed-in-china.

69. Raymond Zhong, *In Price and Value, Chinese Phone Makers Outpace Apple in Much of the World*, N.Y. TIMES (Jan. 4, 2019), https://www.nytimes.com/2019/01/04/technology/china-smartphones-iphone.html.

70. Alexandra Arici, *Why Don't More Chinese Smartphones Work On US Networks?*, ANDROIDGUYS (May 1, 2018), https://www.androidguys.com/featured/opinion/chinese-phones-on-us-networks/.

71. *See id.* (noting that many Chinese phones are incompatible with American networks).

72. *See* Li, *supra* note 68 ("The widely touted reasons for [western tech companies'] failures include censorship by the Chinese government and cultural differences between China and the West.").

73. *See generally* Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and The Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343 (2009) (introducing the balkanization of the Internet).

74. A. Michael Spence, *Preventing the Balkanization of the Internet*, COUNCIL ON FOREIGN RELATIONS (Mar. 28, 2018), https://www.cfr.org/blog/preventing-balkanization-internet.

This trend of balkanization is worsened by the trade war and other frictions between the U.S. and China.[75] Apple's market value dropped by 10 percent[76] after it announced that the trade war had dwindled demand for iPhones in China.[77] Investors began to worry that "the once-inexorable march of globalization could be reversed."[78] The trend goes beyond the U.S. and China. The U.S. has been diligently pushing allies to drop Huawei's 5G equipment,[79] some countries followed suit, and more countries are still caught in between.[80] Meanwhile, Huawei has built about seventy percent of Africa's 4G networks.[81] From a higher perspective, one might find that a main purpose of the Belt and Road Initiative is to rejuvenate Eurasia, which will potentially marginalize the U.S.[82] Interestingly, article 32.10 of the North American Free Trade Agreement (NAFTA), called by some as "the China Clause," prohibits any signatory to sign a free trade deal with a non-market economy.[83]

Data localization is another heavy blow to the world's digital economy that is already partially balkanized.[84] Data localization is a policy that a country's government forces internet content hosts to have data collected in that country or data about citizens of the country stored in the country.[85] The data stored in the country could be the sole copy of the data or a local copy of data generated in another country.[86] As discussed in Section IV.B of this Note, data localization is further damaging the world economy.[87]

---

75. Joshua Brustein *Trump's Trade War Threatens to Divide the World's Smartphone Makers*, BLOOMBERG (Jan. 10, 2019, 3:00 AM), https://www.bloomberg.com/news/features/2019-01-10/trump-s-trade-war-threatens-to-divide-the-world-s-smartphone-makers.

76. David Goldman & Matt Egan, *Markets Shudder After Apple Warns About China Sales*, CNN: BUSINESS (Jan. 3, 2019, 4:08 AM), https://www.cnn.com/2019/01/02/investing/dow-futures-stock-market-apple/index.html.

77. Brustein, *supra* note 75.

78. *Id.*

79. Chris Isidore, *US Reportedly Urges Allies To Block Use Of Huawei Equipment*, CNN: BUSINESS (Nov. 23, 2018, 5:56 AM), https://www.cnn.com/2018/11/23/tech/huawei-us-government/index.html.

80. Joe Panettieri, *Huawei: Banned and Permitted in Which Countries? List and FAQ*, CHANNELE2E (Feb. 13, 2020), https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/.

81. Amy Mackinnon, *For Africa, Chinese-Built Internet Is Better Than No Internet at All*, FOREIGN POL'Y. (Mar. 19, 2019, 3:53 PM), https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/.

82. *See* Jacob Shapiro, *Italy Signs Up For The Belt And Road Initiative*, REALCLEARWORLD (Mar. 18, 2019), https://www.realclearworld.com/articles/2019/03/18/italy_signs_up_for_the_belt_and_road_initiative_112988.html ("Being able to seamlessly connect markets from Shanghai to Lisbon would hamper the United States' ability to prevent the rise of a Eurasian hegemon or a Eurasia less dependent on Washington's support and approval.").

83. North American Free Trade Agreement, Can.-Mex.-U.S., art. 32.10, Mar. 1, 1993, 32 I.L.M. 289 [hereinafter *NAFTA*]; Josh Wingrove, *Nafta's China Clause Is Latest Blow to Trudeau's Asia Ambitions*, BLOOMBERG (Oct. 4, 2018), https://www.bloomberg.com/news/articles/2018-10-04/nafta-s-china-clause-is-latest-blow-to-trudeau-s-asia-ambitions.

84. Bret Cohen, Britanie Hall, & Charlie Wood, *Data Localization Laws and Their Impact On Privacy, Data Security and The Global Economy*, 32 ANTITRUST ABA 107, 107.

85. John Selby, *Data Localization Laws: Trade Barriers Or Legitimate Responses To Cybersecurity Risks, Or Both?*, 25 INT. J. LAW INFO. TECH. 213.

86. *Id.*

87. *See infra* Section IV.B ("Data localization acts as barrier to trade and investment.").

III. ANALYSIS

A. Big Data: It Is Here to Stay Although Not Welcomed by Everyone

1. Big Data's Invasion of Privacy

The most serious criticism of big data is its invasion of privacy.[88] In 2017, when a Tinder user asked Tinder for her personal data, she received 800 pages of information, including not only all of her tinder messages, but also her "Facebook 'likes,' links to where [her] Instagram photos would have been had [she] not previously deleted the associated account, [her] education, the age-rank of men [she] was interested in, how many Facebook friends [she] had and when and where every online conversation with every single one of [her] matches happened . . . ."[89]

More recent is Facebook's Cambridge Analytica scandal.[90] Cambridge Analytica was hired by President Trump's election campaign, and it acquired data collected from Facebook, including users' identities, friend network and "likes."[91] It mapped users' "personality traits" based on the data, and then used the "personality traits" to target audiences with digital political ads.[92] These intrusions might seem to be an inevitable consequence of the age of big data.[93] It is not coincidental that Facebook's founder Mark Zuckerberg once declared that "the age of privacy is over."[94] Similarly, Vint Cerf, Google's "Chief Internet Evangelist," suggested that the concept of privacy might be a "historical anomaly."[95] But the backlash of the Cambridge Analytica scandal in the U.S., along with the debate in response to Edward Snowden's revelations of the surveillance program PRISM, shows that Americans' expectation of privacy in the age of big data is still alive and well.[96]

2. Big Data's Charm

Of course, big data is not without any merit. For example, big data is promising to solve and prevent crime.[97] Internet and cellphone habits of the

88. Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy Is Over*, READWRITE (Jan. 9, 2010), http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~oo2UUoqssyO3eq.

89. Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages Of My Deepest, Darkest Secrets*, THE GUARDIAN (Sept. 26, 2017, 2:10 PM), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

90. Kevin Granville, *Facebook And Cambridge Analytica: What You Need To Know As Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

91. *Id.*

92. *Id.*

93. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 397–98 (2014).

94. Kirkpatrick, *supra* note 88.

95. Richards & King, *supra* note 93; Gregory Ferenstein, *Google's Cerf Says "Privacy May Be An Anomaly,"* TECHCRUNCH (Nov. 20, 2013, 4:06 PM), http://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right/.

96. Richards & King, *supra* note 93.

97. *Id.* at 407–08.

perpetrators in hate crimes can be useful in stopping tragedies before the perpetrators have the chance to carry out their plan.[98] Incidents like the Nice truck attack, the Orlando gay nightclub shooting and the Tree of Life Synagogue Shooting did not have to happen.[99] Big data could also help provide underserved populations easier access to financial services.[100] According to the World Bank, seventy-five percent of the world's poor do not have a bank account due to reasons like poverty, costs and travel distances.[101] Big data conglomerates and social networks' desire to obtain more data, along with the growing use of mobile phones, may facilitate and transform access to financial services for the underserved.[102] Big data is also able to reduce high school dropout rates,[103] detect infections,[104] and increase energy efficiency.[105]

Interestingly, big data is driving the development of technologies themselves.[106] In science research based on data-intensive computing, human kind is now "at a stage of development that is analogous to when the printing press was invented."[107] For instance, big data promotes the advance of ecological science,[108] ocean science,[109] medical science,[110] and scientific infrastructure.[111] More importantly, big data is also the life blood of AI.[112]

Vast amounts of data are needed in the field of deep learning, the main technology driving the rise of artificial intelligence (AI).[113] The AI race is deemed to be "a space-race redux, where world superpowers battle to define

98. Frederic Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 347 (2017)

99. *Id.*

100. *See* Nizan Geslevich Packin & Yafit Lev-Aretz, *Big Data and Social Netbanks: Are You Ready to Replace Your Bank?*, 53 HOUS. L. REV. 1211, 1242–46 (2016) (explaining that expansion of big data goliaths and social networks into the financial services market provides millennials a better option versus the traditional banking system, and provides the underserved population easy access to financial service).

101. Asli Demirguc-Kunt & Leora Klapper, *Measuring Financial Inclusion: The Global Findex Database* 11–19 (The World Bank Dev. Research Grp., Working Paper No. 6025, 2012).

102. Packin & Lev-Aretz, *supra* note 100.

103. Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance, CTR. FOR INFO. POL'Y LEADERSHIP (Feb. 2013) 6–7 (discussing efforts to reduce the high school drop-out rate using student record analysis in Mobile County, Alabama).

104. Brian Proffitt, *Big Data Analytics May Detect Infections Before Clinicians*, ITWORLD (Apr. 12, 2012), http://www.itworld.com/big-datahadoop/267396/big-data-analytics-may-detect-infection-clinicians.

105. *See generally* Omer Tene & Jules Polonetsky, *Big Data For All: Privacy And User Control In The Age Of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 241 (2013) (stating big data helps conserve our natural resources by making our use of electricity more efficient).

106. THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY xi–xv (2009).

107. *Id.* at xi.

108. James R. Hunt, Dennis D. Baldocchi & Catharine van Ingen, *Redefining Ecological Science Using Data*, *In* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 21, 21 (2009).

109. John R. Delaney & Roger S. Barga, *A 2020 Vision for Ocean Science*, *in* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 27, 27 (2009).

110. Iain Buchan, John Winn & Chris Bishop, *A Unified Modeling Approach to Data-Intensive Healthcare*, *in* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 91 (2009).

111. Mark R. Abbott, *A New Path for Science?*, *in* MICROSOFT, THE FOURTH PARADIGM: DATA-INTENSIVE SCIENTIFIC DISCOVERY 111, 111 (2009).

112. Steven Hansen, *How Big Data Is Empowering AI and Machine Learning*? HACKER NOON (Nov. 24, 2017), https://hackernoon.com/how-big-data-is-empowering-ai-and-machine-learning-4e93a1004c8f.

113. 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.

generations of technology to come."[114] China is investing at least 7 billion dollars in AI through 2030,[115] and has an ambitious plan to treat AI like a Chinese version of the Apollo 11 lunar mission, which could "stoke national pride and spark agenda-setting technology breakthroughs."[116] The European Commission also intends to invest 24 billion dollars between 2018 and 2020.[117] The U.S. did not have a central AI policy until February 2019,[118] but is currently still the leader in this field.[119] The inaction prior to 2019 seems to be an unintentional mistake rather than a strategic decision.[120]

AI will also manifest its power in global economic growth.[121] PricewaterhouseCoopers (PwC) projects that AI could contribute up to 15.7 trillion dollars to the world economy in 2030, more than the current annual GDP of China and India combined.[122] It is predicted that China will then take home 7 trillion dollars of the 15.7 trillion dollars.[123]

AI may change the dynamics of the high technology industries in a fundamental way.[124] The high technology industry has been in an "Age of Discovery," where a country's advantage depends on brilliant engineers and breakthrough insights, but due to AI, the industry is now entering an "Age of Implementation," where engineers do not have to be geniuses.[125] What matters most will instead be the access to abundant data.[126] In this respect, the current situation is in favor of Chinese companies, for a host of reasons, including China's 800 million internet users and the fact that Chinese netizens "channel more of their daily activities through mobile phones than their American counterparts."[127] There are also several other reasons: the lack of meaningful

114. Dave Gershgorn, *Forget The Space Race, The AI Race Is Just Beginning*, WORLD ECONOMIC FORUM (May 8, 2018), https://www.weforum.org/agenda/2018/05/ai-is-the-new-space-race.

115. *Id*.

116. Metz, *supra* note 113.

117. Gershgorn, *supra* note 114.

118. Baker, *supra* note 35.

119. Metz, *supra* note 113.

120. *See* Shirin Ghaffary, *Trump's Executive Order on AI, Explained*, VOX (Feb. 13, 2019, 9:40 AM), https://www.vox.com/2019/2/13/18222433/trump-executive-order-ai-explained (suggesting that the "American AI Initiative" is just "hollow words", which is far-reaching and provides no additional funds); Frederick Kempe, *The US is Falling Behind China in Crucial Race for AI Dominance*, CNBC (Jan. 26, 2019, 7:00 AM), https://www.cnbc.com/2019/01/25/chinas-upper-hand-in-ai-race-could-be-a-devastating-blow-to-the-west.html (the Trump administration was absent from the discussion of international data governance norms at the annual meeting of the World Economic Forum due to the government shutdown); Ali Breland, *Experts fear US losing ground to China on AI*, THE HILL (Feb. 14, 2018, 6:00 AM), https://thehill.com/policy/technology/373733-experts-fear-us-losing-ground-to-china-on-ai (although the White House claimed that it had an unpublished AI plan, many in the AI industry and academia were still puzzled by "federal disinterest in AI").

121. Peter H. Diamandis, *China Is Quickly Becoming an AI Superpower*, SINGULARITYHUB (Aug. 29, 2018), https://singularityhub.com/2018/08/29/china-ai-superpower/.

122. SIZING THE PRIZE: WHAT'S THE REAL VALUE OF AI FOR YOUR BUSINESS AND HOW CAN YOU CAPITALISE?, PRICEWATERHOUSE COOPERS 4 (2007).

123. *Id*. at 7.

124. Clay Chandler, *How China's Rise as AI Superpower Could Reshape the World*, FORTUNE (Sept. 26, 2018, 7:49 AM), http://fortune.com/2018/09/26/china-ai-superpower-book-review/.

125. *Id*.

126. *Id*.

127. *Id*.

legal protection of privacy in China; data localization due to Chinese laws;[128] and Chinese citizens' indifference to their right to privacy.[129]

More importantly, the possible AI-driven advantages in technology and economy may "compound with interest."[130] The more data one has in the first place, the better AI applications you can build, which will enable you to collect more data.[131] "AI will become concentrated, because of the inputs required to pull it off," says Tim Hwang, who leads the Harvard-MIT Ethics and Governance of AI Initiative.[132]

It is true that citizens' privacy is violated at times due to data gathering, but it is unwise for governments to adopt a laissez-faire approach to big data because of its potential impact on technologies,[133] the world economy[134] and geopolitics.[135] Therefore, the rest of this Note will discuss how big data is treated differently in the U.S. and China, and what the U.S. should do to secure its interests.

B. Data and Privacy in the United States and China

1. Legal Protection for Privacy in China

One cannot talk about privacy in China without mentioning China's cybersecurity law (CSL).[136] The CSL demonstrates Beijing's mentality when it comes to privacy protection, which is more about national security than individual rights.[137]

The CSL can be seen as part of a larger legal framework governing cyberspace.[138] How the law might operate is better understood if it is read along with other "mutually reinforcing parts of China's evolving cyber governance system."[139] Samm Sacks, a senior fellow at the Center for Strategic and International Studies, notes that key highlights of the framework include the CSL, Encryption Law, National Security Law, Counterterrorism Law,

128. Chris Mirasola, *U.S. Criticism of China's Cybersecurity Law and the Nexus of Data Privacy and Trade Law*, LAWFARE (Oct. 10, 2017, 12:00 PM), https://www.lawfareblog.com/us-criticism-chinas-cybersecurity-law-and-nexus-data-privacy-and-trade-law.

129. Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT. ECON. L. 245 (2018).

130. Nicholas Thompson & Ian Bremmer, *The AI Cold War That Threatens Us All*, WIRED (Oct. 23, 2018, 6:00 AM), https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/.

131. *Id.*

132. *Id.*

133. Hunt et al., *supra* note 108.

134. Diamandis, *supra* note 121.

135. Chandler, *supra* note 124.

136. *See* Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm [hereinafter CSL].

137. Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*., LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

138. *See id.* ("The CSL is better understood as the 'keystone in an arch' of the Xi government's larger buildout of a legal framework for security controls in cyberspace.").

139. *Id.*

International Cybersecurity Strategy, and *Made in China 2025*.[140] Therefore, the framework shows that national security is the real focus.

This observation can also be confirmed by Xi Jinping's dictum "without cybersecurity there is no national security."[141] Protection of personal data is hardly a priority of the Chinese government, especially when compared to national security.[142] Therefore, it is not difficult to understand why the CSL leaves many opportunities for the Chinese government or third parties to intrude upon Chinese citizens' privacy, although it apparently offers Chinese citizens unprecedented protection of their data privacy.[143] For instance, under the CSL, network operators are required to protect individuals' privacy, but individuals will not be able to claim any remedies for the infringements of their privacy by the Chinese government.[144]

Another problem with the CSL's efforts to protect personal data is its vague language.[145] On the one hand, the vagueness gives much flexibility to policymakers on how to implement the CSL.[146] On the other hand, as some have complained, the law is so vague and ambiguous that it is subject to broad interpretation.[147] It has also been suggested that the government created the ambiguities on purpose to have leeway to target internet companies when necessary.[148]

Besides the CSL, there are many other venues for data protection in China, some of which are shown by the key highlights provided by Samm Sacks.[149] In addition, China's Tort Liability Law and Criminal Law also provide general protection for personal information.[150] However, counterintuitively, more legal venues make data protection in China more difficult, because the responsibility would lie in the hands of a plurality of Chinese authorities, who regulate and govern in their own sectors.[151] While ideally this overlap of jurisdictions should increase the likelihood that a violation of right to privacy will be detected and the violators punished,[152] it is common in China that relevant administrative agencies have no incentive to make sure that their responsibilities are fulfilled

140. *Id.*
141. Mirasola, *supra* note 128.
142. Aaronson & Leblond, *supra* note 129.
143. Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 100 (2018).
144. *Id.* at 100–01.
145. Liudmyla Balke, *China's New Cybersecurity Law and U.S.-China Cybersecurity Issues*, 58 SANTA CLARA L. REV. 137, 159 (2018).
146. *Id.*
147. Lee, *supra* note 143, at 62.
148. *Id.*
149. Sacks, *supra* note 137.
150. Zhonghua Renmin Gongheguo Qinquan Zeren Fa (中华人民共和国侵权责任法) [China's Tort Liability Law and Criminal Law] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010), http://www.gov.cn/flfg/2009-12/26/content_1497435.htm; *see* Bo Zhao & G.P. (Jeanne) Mifsud Bonnici, *Protecting EU Citizens' Personal Data In China: A Reality Or A Fantasy?*, 24 INT. J. LAW INFO. TECH. 128 (2016) (discussing personal data protection in China from the lens of the EU citizen).
151. Zhao & Bonnici, *supra* note 150, at 128.
152. Xingxing Li, *An Economic Analysis of Regulatory Overlap and Regulatory Competition: The Experience of Interagency Regulatory Competition in China's Regulation of Inbound Foreign Investment*, 67 ADMIN. L. REV. 685, 710 (2015).

when they are simply "one of the many gatekeepers," as observed by some scholars.[153]

Also, historically the term "privacy" did not exist in Chinese laws and regulations until the Tort Liability Law was enacted at the end of 2009.[154] This indifferent attitude can be corroborated by the fact that China is not a party to the International Covenant on Civil and Political Rights or other human rights treaties involving privacy protections.[155] It is thus not surprising that privacy protections offered by Chinese laws have been significantly less robust than those in other countries.[156]

2. Legal Protection for Privacy in the United States

Unlike in China, the legal concept of "privacy" in the U.S. came into being as early as 1891.[157] However, although the American public has little faith in governmental and private organizations to protect their data,[158] the U.S. is similar to China in that there are only, "piecemeal legislative responses at the federal level."[159] The federal government only regulates certain kinds of sensitive information (e.g., health and financial) while creating, "overlapping and contradictory protections."[160] The Health Insurance Portability and Accountability Act (HIPAA) for example, the United States' main health privacy and security law, "only applies to 'covered entities' holding 'protected health information."[161] Similarly, the Family Educational Rights and Privacy Act (FERPA) only protects data of children under thirteen.[162]

U.S. common law does include tort liability for invasions of privacy. [163] The Restatement (Second) of Torts provides that the right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another; (b) appropriation of the other's name or likeness; (c) unreasonable publicity given to the other's

153. *Id.* at 710–11. *See* Wang Di (王地), *Zhengfu Bumeng "Tipiqiu", Gai Xiu Yi* (*政府部门"踢皮球"，该休矣*) [*It's Time for Governmental Agencies to Stop Passing the Buck*], JIANCHA RIBAO (检察日报)[PROCURATORATE DAILY], Oct. 23, 2014, at 5, *available at* http://newspaper.jcrb.com/html/2014-10/23/content_170597.htm (noting that governmental agencies passing the buck might threaten the legitimacy of the Chinese government).

154. Aaronson & Leblond, *supra* note 129, at 235.

155. Frederic Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 358 (2017); *see* Status of Treaties: International Covenant on Civil and Political Rights (Jan. 15, 2020), https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (China has signed the Covenant, but has not ratified it).

156. 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).

157. *See* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1335 (1992) ("[I]n the winter of 1890-91, that Samuel Warren and Louis Brandeis published their now famous article in the *Harvard Law Review*, entitled simply: *The Right to Privacy*.").

158. Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CENTER (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

159. NUALA O'CONNOR, COUNCIL ON FOREIGN RELATIONS, REFORMING THE U.S. APPROACH TO DATA PROTECTION AND PRIVACY (2018), *available at* https://www.cfr.org/report/reforming-us-approach-data-protection.

160. *Id.*

161. Pub. L. No. 104–191, 110 Stat. 1936, 1991; O'CONNOR, *supra* note 159.

162. 20 U.S.C. § 1232g (2018).

163. Frederic Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 379 (2017).

private life; and by (d) publicity that unreasonably places the other in a false light before the public.[164] But the tort remedies are inadequate, because they fail in particular situations.[165] For example, there is no cause of action for a violation of privacy if data about citizens are collected when they are, "on the public streets."[166]

State laws do not help either. On the one hand, state laws governing privacy and data lack uniformity.[167] As of September 2018, all fifty states and the District of Columbia have enacted laws requiring individuals to be notified if their information is compromised.[168] But the laws have different and even incompatible provisions regarding what kinds of personal information are protected, who are covered, and what constitutes a breach.[169] On the other hand, some of the state laws might violate the Constitution.[170] Several experts have argued that, for example, the California Consumer Privacy Act could regulate business that does not have significant ties to the state, and therefore likely unconstitutional.[171]

Some might hope that the statutory "unfair acts and practices" authority of the Federal Trade Commission (FTC) will come to the rescue of data security,[172] but it does not solve the problem. The FTC is "the chief federal agency" to carry out privacy policy and enforcement,[173] and its role enables it to develop its actions "into a rich jurisprudence that is effectively the law" of personal

164. RESTATEMENT (SECOND) OF TORTS §§ 652A-E (AM. LAW INST. 1977).

165. LEGISLATIVE ASSEMBLY OF NEW BRUNSWICK, PRIVACY IN GENERAL, *available at* https://www.gnb.ca/legis/business/committees/previous/reports-e/privacy2/P2e4-e.asp.

166. LARRY W THOMAS, LIABILITY OF TRANSPORTATION ENTITY FOR THE UNINTENTIONAL RELEASE OF SECURE DATA OR THE INTENTIONAL RELEASE OF MONITORING DATA ON MOVEMENTS OR ACTIVITIES OF THE PUBLIC 43 (2016).

167. O'CONNOR *supra* note 159.

168. NAT'L CONG. OF STATE LEGISLATURES, SECURITY BREACH NOTIFICATION LAWS (2018), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

169. O'CONNOR *supra* note 159.

170. Wendy Davis, *California Privacy Law May Violate Constitution, Some Privacy Experts Contend*, MEDIAPOST (Jan. 18, 2019), https://www.mediapost.com/publications/article/330758/california-privacy-law-may-violate-constitution-s.html.

171. Letter from Eric Goldman, Santa Clara University, to California Legislature re California Consumer Privacy Act (Jan. 17, 2019) (on file with Santa Clara University School of Law) ("The CCPA's purported application to activity outside of California raises substantial Constitutional concerns and potentially exposes the state to expensive and distracting litigation. More importantly, it causes tremendous uncertainty and possibly wasted expenditures for businesses without real ties to California"). *See* Pike v. Bruce Church, 397 U.S. 137, 142 (1970) (ruling that, "Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."); Nicholas F. Palmieri III, *Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws*, 11 HASTINGS SCI. & TECH. L.J. 37, 40 (2020) ("the CCPA will likely have significant difficulties overcoming the [Dormant Commerce Clause and First Amendment] challenges presented here, particularly because it provides little benefit in return for imposing significant burden on out-of-state actors."). *But see* Mallory Ursul, *The States' Role in Data Privacy: California Consumer Privacy Act Versus Dormant Commerce Clause*, 52 SUFFOLK U. L. REV. 577, 594 (2019) (arguing that CCPA is constitutional).

172. Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 963 (2016).

173. *Protecting Consumer Privacy and Security*, F.T.C. (last visited Feb. 23, 2020), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security.

information.[174] Generally, when deciding whether it should bring an action, the FTC focuses on two scenarios: (1) when a company misrepresents data security or misappropriates private data (i.e. the "deception" prong); or (2) when a company fails to protect the data from risks of breaches (i.e. the "unfairness" prong).[175] Nonetheless, because of its obscurity the FTC's "handbook" is not a perfect substitute of a comprehensive federal law on privacy.[176] It also does not help that nearly all FTC actions end in settlements.[177] Furthermore, companies are pushing back the FTC citing its lack of legal authority to police data-security practices.[178] It is also argued that the FTC has limited jurisdiction over entities like banks, insurance companies, and nonprofit organizations.[179]

Neither China nor the U.S. has an overarching data protection regime such as the EU General Data Protection Regulation (GDPR).[180] This exposes the personal data of both countries' citizens to risks. But the patchwork of protections in the U.S. might have an unintended consequence not found in China: the unnecessary deterrence of data gathering.[181] This century's economy will be fueled by data, but the lack of clear rules greatly discourages companies in the U.S. to secure data whether the company is acting in good faith or not.[182]

3. Different Social Attitudes

a. U.S. Citizens Are Generally Wary of Data Gathering

According to a survey conducted by Pew Research, Americans have strong views about their personal data and freedom from surveillance in daily life.[183] Ninety percent of adults feel that "controlling what information is collected about them is important."[184] This attitude is not surprising in light of the

174. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 589 (2014).

175. *Id.* at 585. *But see* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018) (highlighting that the FTC's authority under the unfairness prong was seriously challenged, but the Eleventh Circuit eventually declined to evaluate the authority); Julia Whall, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of Labmd*, 60 B.C.L. REV. E-SUPPLEMENT II.-149, II.–154 (2019) ("The FTC's broad exercise of authority under the unfairness prong has proved controversial among scholars.").

176. *See id. at* 589 ("[A] large domain of the U.S. privacy regulatory framework", that is the FTC's jurisprudence, "primarily consists of a relatively obscure body of doctrines that scholars have not analyzed in depth.").

177. *Id*. at 588.

178. *See* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1227 (11th Cir. 2018) (LabMed argued that FTC didn't have the general authority to regulate data security in the health care space); FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 250 (3d Cir. 2015).

179. O'CONNOR, *supra* note 159.

180. Zhao & Bonnici, *supra* note 150.

181. *See* O'CONNOR, *supra* note 159 ("Companies need clearer rules, and individuals need to be able to incentivize companies to secure data.").

182. *Id. See also* Guy Chazan, *SAP Raises Fears Over EU Data Privacy Rules*, FINANCIAL TIMES (Jan. 15, 2017), https://www.ft.com/content/22d5e078-d9a1-11e6-944b-e7eb37a6aa8e ("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. . . .").

183. MARY MADDEN AND LEE RAINIE, PEW RESEARCH CENTER, AMERICANS' VIEWS ABOUT DATA COLLECTION AND SECURITY (2015).

184. *Id.*

aftermath of Facebook's Cambridge Analytica scandal,[185] and the heated debate over Edward Snowden's revelation of PRISM.[186]

American citizens' attitude toward data gathering might be explained by the fact that they have long been exposed to the concept of privacy. Firstly, the right to privacy is inherent in the common law,[187] which the American Colonies adopted from England in the sixteenth century.[188] In 1970s, the landmark Supreme Court case, *Roe v. Wade*, focused on the constitutionality of laws that restricted access to abortions.[189] One of the decision's main conclusions is that a "zone of privacy" exists under the Constitution, and the right to privacy includes the abortion decision.[190] This well-known decision and all the controversies around it changed the conversations about privacy, and left American believing that privacy was something they could expect as citizens.[191] By the nineteen-eighties, reality shows and confessional memoirs further made Americans realize "how valuable a commodity privacy is."[192] The 2016 election and Facebook's Cambridge Analytica scandal made it clear that personal information might even be an imminent national security concern.[193] Recently, the soaring number of data breach reports make Americans even more anxious.[194]

b. Chinese Citizens Generally Embrace Data Gathering

In contrast to the U.S., the concept of "privacy as a fundamental human right" is relatively new to Chinese citizens for various reasons.[195] First, the Chinese word for privacy (*yinsi* 隐私) has a negative connotation, which often reminds Chinese people of "illicit secrets," selfishness and conspiracy.[196] More

185. *See* Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is The FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 514 (2018) (describing how the Cambridge Analytica scandal provoked intense reaction).

186. *See generally The Resilient Foundation of Democracy: The Legal Deconstruction of the Washington Post's Condemnation of Edward Snowden*, 93 IND. L.J. 533, 535–37 (2018) (providing background information on the controversy surrounding Edward Snowden).

187. Louis Menand, *Why Do We Care So Much About Privacy?*, NEW YORKER (June 18, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy.

188. RC Dale, *The Adoption of the Common Law by the American Colonies*, 24 A.L. REG. 553, 553 (1882).

189. Roe v. Wade, 410 U.S. 113 (1973).

190. *Id.* at 152–54.

191. Alexandra Samuel, *What Roe v. Wade Means for Internet Privacy*, JSTOR (July 17, 2018), https://daily.jstor.org/what-roe-v-wade-means-for-internet-privacy.

192. *Id.*

193. Duncan Hollis, *The Influence of War; The War for Influence*, 32 TEMP. INT'L & COMP. L.J. 31, 38 (2018).

194. *See* Hurst, *supra* note 63 (explaining that GDPR requires mandatory reports of data breaches, which is an important factor contributing the growing number of data breach reports).

195. Aaronson & Leblond, *supra* note 129.

196. Zhang Xinbao (张新宝), *Woguo Yinsiquan Baohu Falü Zhidu De Fazhan* (我国隐私权法律保护制度的发展) [*The Development of China's Privacy Law*], *Guojia Jianchaguan Xueyuan Xuebao* (国家检察官学院学报) [*Journal of National Prosecutors College*], Vol. 18, no. 2, Apr. 2010, at 11, available at http://www.cqvip.com/qk/82198x/201002/33633704.html; *see also* Kenneth Neil Farrall, *Global Privacy in Flux: Illuminating Privacy Across Cultures in China and the U.S.*, INT'L J. OF COMM., 2 (2008), 993, 1011 ("[M]uch of China's neo-Confucian scholarship has considered [the Chinese equivalent of 'private'] to be synonymous with selfish interests.").

specifically, one meaning of the character 隐 is "secret,"[197] and the character 私 can mean "selfish."[198] Second, privacy in China is more about being left alone physically than freedom from data gathering.[199] Third, the widespread nationalist sentiment among Chinese citizens, against the backdrop of the Chinese government's plan to develop its big data industry,[200] compels many Chinese citizens to think that data gathering might benefit the country and therefore is generally a good thing.[201] Finally, Chinese citizens are generally not aware of the rampant intrusions upon their right to privacy,[202] probably because of the inadequate reports on data gathering by Chinese media[203] and the fact that Chinese citizens are busy enjoying the conveniences brought by big data applications. The latter is demonstrated by the popularity of Alipay's Sesame Score among Chinese citizens.[204] Alipay is a "super app."[205] It is like a combination of Amazon, Apple News, Groupon, American Express, Citibank, and YouTube, all of which siphon up data from users.[206] The Sesame Score makes use of the data-collecting powers of Alipay to calculate a credit score based on an individual's activities.[207] People with medium-to-high scores enjoy a wide range of perks, including renting cars without a deposit, special waiting rooms at rail stations, and even better rates for currency exchange.[208] Young college students without any credit history are able to instantly borrow money from Alipay because of their previous spending on Alibaba's e-commerce platforms.[209] Imagine Jeff Bezos helping to pay your tuition if you spend enough on Amazon.

A recent survey also confirms Chinese citizens' support of data gathering.[210] Only 1.4 percent of the respondents disapprove of the Social Credit

197. Online Chinese Dictionary, https://www.chinese-dictionary.org/ (search "隐").

198. Online Chinese Dictionary, https://www.chinese-dictionary.org/ (search "私").

199. Aaronson & Leblond, *supra* note 129; Farrall, *supra* note 196 (Chinese people value territorial privacy).

200. *See infra* Section II.A.

201. *See* Hurst, *supra* note 63 (mentioning that Chinse people value economic growth more than privacy); Aaronson & Leblond, *supra* note 129 ("[Chinese citizens have been subject to government propaganda on the importance of data collection for security and social stability.").

202. Aaronson & Leblond, *supra* note 129.

203. *See* David Bandurski, *Beijing Eyes Stake In Every Influential Chinese Media Company—Should They Worry?*, FORBES (Oct. 16, 2017), https://www.forbes.com/sites/insideasia/2017/10/16/beijing-eyes-stake-in-every-influential-chinese-media-company-should-they-worry/#7fd27ca8715d (detailing how Beijing tightened its control of Chinese media).

204. John Gapper, *Alibaba's Social Credit Rating Is A Risky Game*, FINANCIAL TIMES (Feb. 20, 2018), https://www.ft.com/content/99165d7a-1646-11e8-9376-4a6390addb44.

205. Mara Hvistendahl, *Inside China's Vast New Experiment In Social Ranking*, WIRED (Dec. 14, 2017), https://www.wired.com/story/age-of-social-credit/.

206. *Id.*

207. *Id.*

208. Charlie Campbell, *How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens*, TIME, http://time.com/collection/davos-2019/5502592/china-social-credit-score/ (last visited Feb. 23, 2020).

209. Masha Borak, *Debt: The Secret Sauce of Alibaba's Singles Day Success*, TECHNODE (Nov. 22, 2017), https://technode.com/2017/11/22/huabei-singles-day/.

210. Nik Dawson, *China's Social Credit System: Privacy Invasion or State Innovation?*, BITS & ATOMS (Sept. 1, 2018), https://bitsandatoms.co/chinas-social-credit-system-privacy-invasion-or-state-innovation/#easy-footnote-bottom-13-297.

System.[211] As many as eighty percent of the respondents approve of it.[212] Interestingly, the governmental part of the Social Credit System enjoys a higher approval rate than its commercial counterparts, like the Sesame Score.[213] However, it is important to note that concerns over data and privacy are on the rise in China.[214] A survey jointly conducted by Tencent and China Central Television showed that 76.3 percent of the respondents believe that some forms of AI are a threat to their privacy.[215]

C. Chinese Tech Industry's Edge over Its U.S. Counterparts

The differences between the U.S. and China regarding how big data and privacy is viewed and treated, as discussed in Section III.B. of this Note have an immediate impact on the two countries' technology industries.

As for the AI industry, which is mostly fueled by data, the U.S. is currently ahead of China.[216] According to the World Intellectual Property Organization (WIPO), IBM still has the biggest AI patent portfolio followed by Microsoft.[217] But as previously discussed in Section III.A.2, China is catching up fast.[218] It has published more academic papers on AI than the U.S. since 2005.[219] Although questions remain about the quality of these Chinese papers, it is expected that the two countries will have an equal share of high-quality publications in AI by 2020.[220]

In the social media area, American companies are facing challenges. Recently, Apple had to disable the entire Group FaceTime function because of a flaw that allowed users to eavesdrop on their friends.[221] In April 2018, Facebook's CEO, Mark Zuckerberg, spent about eleven hours testifying on data privacy before Senate committees in the wake of the Cambridge Analytica scandal.[222] Facebook later announced its "pivot to privacy," but few were

211. Genia Kostka, *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval* 12 (July 23, 2018), https://ssrn.com/abstract=3215138.

212. *Id.*

213. *Id.* at 13.

214. Zen Soo, *The Increasing Use Of Artificial Intelligence Is Stoking Privacy Concerns In China*, SCMP, (Mar. 5, 2018), https://www.scmp.com/business/companies/article/2135713/increasing-use-artificial-intelligence-stoking-privacy-concerns.

215. *Id.*

216. Tom Simonite, *China Is Catching Up to the US in AI Research—Fast*, WIRED (Mar. 13, 2019, 10:00 AM), https://www.wired.com/story/china-catching-up-us-in-ai-research/.

217. Tom Miles, *U.S., China Take the Lead in Race for Artificial Intelligence: U.N.*, REUTERS (Jan. 13, 2019, 2:08 AM), https://www.reuters.com/article/us-tech-un/u-s-china-take-the-lead-in-race-for-artificial-intelligence-u-n-idUSKCN1PP0U6.

218. Simonite, *supra* note 216; *see supra* Section III.A.2 (discussing the leap that China has taken in rapidly incorporating Big Data analytics).

219. Simonite, *supra* note 216.

220. *Id.*

221. Richard Morgan, *Apple Says FaceTime Spying Bug Won't Be Fixed Until Next Week*, N.Y. POST (Feb. 1, 2019, 1:23 PM), https://nypost.com/2019/02/01/apple-says-facetime-spying-bug-wont-be-fixed-until-next-week/.

222. Nicholas Fandos, *Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy*, N.Y. TIMES (Apr. 10, 2018), https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html.

convinced that the new plan would work.[223] As of March 2019, because of its privacy practices, Facebook was under investigations by the Federal Trade Commission, the Securities and Exchange Commission, and prosecutors from the Northern District of California and the Eastern District of New York.[224] Mark Zuckerberg argued during his testimony that some leeway was needed for American companies to innovate or they would "fall behind Chinese competitors."[225] There is some truth to his remark. Tencent, a Chinese technology giant, is collecting user data incessantly through its ubiquitous social media apps, including QQ and WeChat.[226] It processes and monitors users' messages, and even collects deleted messages, which will be shared with the Chinese government when requested.[227] However, almost no one in China bats an eye, and WeChat is growing more influential day by day.[228] WeChat's ecosystem also poses a serious challenge for Apple's App Store with the former offering countless "instant apps" within its own program.[229]

On the fintech front, there is no real American equivalent of Ant Financial. Ant Financial is an affiliate company of Alibaba and manages the Sesame Score, which is discussed in more details in Section III.B.3, and it is valued at about one hundred and fifty billion USD, more than the publicly traded Goldman Sachs.[230] What makes Ant Financial valuable is its ability to make use of big data to "make funds for consumers."[231] The closest American company to Ant Financial might be LendUp, whose mission is to "provide anyone with a path to better financial health."[232] But LendUp struggled at its early stage and had to be split up, because it failed to build the credit for the working poor that it promised

223. Bhaskar Chakravorti, *Facebook's Fake Pivot To Privacy*, FORBES (Mar. 11, 2019, 7:49 PM), https://www.forbes.com/sites/bhaskarchakravorti/ 2019/03/11/facebooks-fake-pivot-to-privacy/#cff4b86b37a5.

224. Fred Vogelstein, *Facebook's Sloppy Data-Sharing Deals Might Be Criminal*, WIRED (Mar. 14, 2019, 2:17 PM), https://www.wired.com/story/facebooks-sloppy-data-sharing-deals-might-be-criminal/.

225. *See* Sacks, *supra* note 137 (quoting 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.").

226. 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/#726df2db4424.

227. 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/.

228. *See* Arjun Kharpal, *Everything You Need To Know About WeChat — China's Billion-User Messaging App*, CNBC (Feb. 4, 2019, 11:45 PM), https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html ("WeChat becomes like an app store as it tries to keep users connected to its ecosystem.").

229. 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.

230. Evelyn Cheng, *How Ant Financial Grew Larger Than Goldman Sachs*, CNBC (Jun. 8, 2018, 11:05 AM), https://www.cnbc.com/2018/06/08/how-ant-financial-grew-larger-than-goldman-sachs.html.

231. *Id.*

232. Tim Lucas, *Improving Financial Health By Improving Credit Scores*, LENDUP (Feb. 13, 2017), https://www.lendup.com/blog/improving-financial-health-by-improving-credit-scores.html.

to serve,[233] and it was not able to lower default rates by statistical modeling,[234] although it claimed that it had developed "a big data analytic engine to get a better picture of the borrower."[235] These failures may be caused by LendUp's limited data sources.[236]

D. Data Localization

Why does it matter that it is easier in one country to gather data than in another country due to reasons like legal systems and social attitude, if data can always flow freely between countries? The reason is that it cannot, due to data localization.

The United States of America, the European Union (EU) and China are on their way to dominate big data.[237] Each of these three "data realms" has adopted a different approach to develop its data-driven sectors.[238] While the US has little constrain on cross-border data flow, the EU and China both have some kinds of measures to restrict the free flow of data, and China even constrains the data flow within its borders.[239]

1. Data Localization in the EU

The EU's General Data Protection Regulations (GDPR), became effective in May 2018.[240] One of the most important features of the law is data localization.[241] The GDPR requires that personal data can only be transferred outside of the EU when the destination has an adequate level of data protection.[242] Even if a company within the EU only has slight doubt of the destination's data protection, the transfer would be illegitimate.[243] Nonetheless, the E.U. is very willing to let its member states share data with each other, which helps create a single market for data storage and processing services.[244] The

233. Dan Primack, *Fintech Company LendUp is Splitting Up*, AXIOS (Oct. 19, 2018), https://www.axios.com/fintech-company-lendup-splitting-up-be92e13b-ec9e-4526-9f3e-d1923c441229.html; *see also* James Rufus Koren, *Google-Backed Lendup Fined By Regulators Over Payday Lending Practices*, LOS ANGELES TIMES (Sept. 27, 2016, 11:25 AM), https://www.latimes.com/business/la-fi-lendup-cfpb-20160926-snap-story.html (quoting the California Department of Business Oversight, "LendUp also misled borrowers about how the company's loans could help improve their credit scores and lead to lower-rate loans in the future.").

234. Elizabeth Dwoskin, *'Big Data' Doesn't Yield Better Loans*, WALL ST. J. (Mar. 17, 2014, 11:19 PM), https://www.wsj.com/articles/consumer-group-finds-big-data-doesnt-yield-better-loans-1395097486.

235. Christina Farr, *LendUp Uses 'Big Data' To Bring Better Small-Dollar Loans To People In Need*, VENTUREBEAT (Oct. 10, 2012, 8:49 AM), https://venturebeat.com/2012/10/10/lendup/.

236. *See* Dwoskin, *supra* note 234 (explaining that companies including LendUp had to use data like how quickly a user scrolls through the lender's website and whether the user fills out an application in capital letters).

237. Aaronson & Leblond, *supra* note 129.

238. *Id.*

239. *Id.*

240. Andrew Rossow, *The Birth Of GDPR: What Is It 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/#4c9ca74a55e5.

241. *Id.*

242. *Id.*

243. *Id.*

244. Council of the European Union Press Release, EU to Ban Data Localisation Restrictions as Ambassadors Approve Deal On Free Flow Of Data (Jun. 29, 2018).

Bulgarian minister for Transport, Information Technology and Communications noted that "[t]his legislation will ensure that data is allowed to flow freely, allowing companies and public administrations to store and process non-personal data wherever they choose in the EU" and "[t]hese rules will provide legal certainty and trust in the increasing use of data-driven innovations for the benefit of all citizens."[245]

2. Data Localization in China

As discussed, the Chinese government's focus when passing the CSL is actually national security.[246] Understanding this, one would not be surprised by the data localization feature of the CSL.[247] The CSL requires that any firm operating in China must store the data collected in China on servers located in the country.[248] Additionally, publishers of online content must have necessary technical equipment and related severs in the country.[249] Furthermore, the CSL covers not only personal data, but also any "important data" concerning "critical information infrastructure," which has been given a broad but vague definition by the Chinese government.[250] Apple, therefore, has to store the iCloud accounts of all its Chinese customers in a data center in China, along with the cryptographic keys, which had always been kept in the United States.[251]

Various other Chinese legislations and regulations other than the CSL have included data localization requirements.[252] For example, in 2011, the People's Bank of China issued a notice to urge banking financial institutions to protect personal financial information.[253] The notice prohibits banks from "storing, processing or analyzing outside China any personal financial information (PFI) collected in China, or providing PFI collected in China to an offshore entity."[254] The Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems issued in 2013 prohibit "the transfer of personal data abroad without express consent

245. *Id.*

246. *See* Sacks, *supra* note 137 ("The CSL is better understood as the 'keystone in an arch' of the Xi government's larger buildout of a legal framework for security controls in cyberspace.").

247. *Id.*

248. Aaronson and Leblond, *supra* note 129.

249. *Id.*

250. Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, UNIV. OF WASH. JACKSON SCHOOL OF INTERNATIONAL STUDIES (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

251. Aaronson and Leblond, *supra* note 129.

252. Wei, *supra* note 250.

253. Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 686 (2015).

254. Zhongguo Renmin Yinhang Guanyu Yinhangye Jinrong Jigou Zuohao Geren Jinrong Xinxi Baohu Gongzuo de Tongzhi (中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知) [Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions] (promulgated by the People's Bank of China, Jan. 21, 2011), http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=.

of the data subject or explicit regulatory approval."[255] Similar requirement is included in a "trial guidelines" issued in 2014 regarding healthcare.[256]

3. U.S. Challenges the Data Localization Trend

With the degree of data localization measures increasing rapidly, the U.S. seems to advocate for the free flow of cross-border data. The U.S. Congress enacted the CLOUD Act, effective March 23, 2018, authorizing the U.S. government to enable law enforcement access to data across borders by creating agreements with foreign governments.[257] The act was designed to fix the mutual legal assistance treaties, which forced governments to take a time-consuming process to access data stored abroad.[258] In October, 2018, two U.S. Senators even sent a letter to the Indian Prime Minister Narendra Modi to "soften India's stance on data localization," and warned Modi that his measures represented trade barriers between the two countries.[259]

IV. RECOMMENDATIONS

A. A Single Federal Law Protecting Personal Data Is Needed.

It is time for the Congress to enact laws specially designed for personal data protection. Currently, the patchwork of laws protecting personal information confuses companies.[260] While this might prevent some good faith small business from abusing data gathering algorithms, it fails to deter big corporations' wanton data gathering[261] and it would also make good faith companies unnecessarily cautious.[262]

255. Dianxin He Hulianwang Yonghu Geren Xinxi Baohu Guiding (电信和互联网用户个人信息保护规定) [Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the Ministry of Indus. & Info. Tech. July 16, 2013, effective, Sept. 1, 2013), https://www.lexology.com/library/detail.aspx?g=7174e101-e09f-46b6-9cb6-13d82c562b0c.

256. Wei, *supra* note 250.

257. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018); Nigel Cory & Alan McQuinn, *Will The US Capitalize On Its Opportunity To Stop Data Localization?*, THE HILL (Sept. 9, 2018, 9:00 AM), https://thehill.com/opinion/cybersecurity/405422-will-the-us-capitalize-on-its-opportunity-to-stop-data-localization.

258. Cory & McQuinn, *supra* note 257.

259. Aditya Kalra, *Exclusive: U.S. Senators Urge India To Soften Data Localization Stance*, REUTERS (Oct. 13, 2018, 5:02 AM), https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN.

260. O'CONNOR, *supra* note 159.

261. Issie Lapowsky, *Get Ready for a Privacy Law Showdown in 2019*, WIRED (Dec. 27, 2018, 7:00 AM), https://www.wired.com/story/privacy-law-showdown-congress-2019/.

262. Sacks, *supra* note 137; *see also 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 (recommending that the federal government provide legal clarity while maintaining the flexibility to innovate so that organizations can know they are in compliance).

1. An Overview of CCPA and GDPR

It makes sense to examine some examples that Congress could follow. In June 2018, California's state legislature passed the California Consumer Privacy Act of 2018 (CCPA), a "historic privacy bill."[263] The CCPA became effective on January 1, 2020.[264] The CCPA grants Californians broad rights: for example, the right to know what information a business will collect and has collected in the past twelve months;[265] the right of consumers to request a business to delete the consumer's personal information collected by the business;[266] the right of consumers to direct a business that sells the consumer's personal data to stop doing so.[267] The CCPA of 2018 is the first American law to follow in the footsteps of the EU General Data Protection Regulation (GDPR).[268] Similar bills have been introduced in Hawaii, Illinois, Massachusetts, Nevada, New Jersey, New York, Oregon, Pennsylvania, Rhode Island, Texas, and Washington.[269]

The GDPR is the reason behind the massive wave of emails in 2018 that were titled something like "we updated our privacy policy."[270] The regulation came into effect on May 25, 2018, and is deemed "the most important change in data privacy regulation in 20 years."[271] Some rights provided by the GDPR are closely copied by the CCPA, for instance, the rights to delete are quite similar in the two laws.[272] In general, both laws are broad, at least from the point of view of tech giants, but the GDPR has a much wider range of obligations.[273] Generally speaking, if a company is in compliance with GDPR, it is likely to be in compliance with CCPA, too.[274] However, in the area of individual rights, the CCPA provides more specific and easily "exercisable rights" to consumers.[275]

While the CCPA and the GDPR offers examples for the lawmakers in Congress, they are not welcomed in the United States, at least not always. A

263. Lapowsky, *supra* note 261.

264. Thomas Germain, *California's Privacy Law Is Finally Here. Now What?*, CONSUMER REPORTS (Jan. 2, 2020), https://www.consumerreports.org/privacy/california-privacy-law-ccpa-california-consumer-privacy-act/.

265. Cal. Civ. Code § 1798.100 (2018).

266. *Id.*

267. *Id.*

268. Mark G. McCreary, *The California Consumer Privacy Act: What You Need to Know*, N.J. L.J. (Dec. 1, 2018, 10:00 AM), https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know/.

269. *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.

270. Alex Hern, *What is GDPR and How Will it Affect You?*, THE GUARDIAN (May 21, 2018, 9:40 AM), https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you.

271. EU GDPR, https://eugdpr.org/ (last visited Nov. 19, 2019).

272. Cal. Civ. Code § 1798.105 (2018); GDPR Art. 17.

273. James Clark & Jim Halpert, *California's Consumer Privacy Act and the GDPR - Where Do They Overlap?*, 18 PRIVACY & DATA PROTECTION 7, 8–10 (2018).

274. Geoffroy De Cooman, *GDPR and CCPA Compliance: The 5 Differences You Should Know*, PROXYCLICK (Oct. 7, 2019), https://www.proxyclick.com/blog/gdpr-and-ccpa-compliance-5-differences.

275. *Id.*; *but see* Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 106–110 (2018) (noting that the CCPA fails to clearly define "public available information"; its deletion requirement and 12-month requirement are vague; and there are confusing overlaps between CCPA and federal statutes).

federal law mirroring the CCPA is unlikely to pass Congress because tech giants would strongly oppose it.[276] When GDPR's requirements were first made public, it also did not receive rave reviews from the United States, and many feared that GDPR might actually increase the likelihood of breaches, and its enforcement body had too much power over companies everywhere in the world, not just the EU.[277] But that attitude is softening. For example, a component of the privacy conversation in the 116th Congress will be about GDPR's impact on the U.S., suggested the chairman of the Information Technology Subcommittee of the House Committee on Oversight and Government Reform.[278] Tim Cook also called for GDPR-style privacy laws in the U.S., and in his mind, personal data is "weaponized against [Americans] with military efficiency."[279] Similarly, Mark Zuckerberg stated that "the GDPR in general is going to be a very positive step for the internet."[280]

2. A Proposal Against the Background of CCPA and GDPR

a. Pass a federal privacy law as soon as possible

As time flies by, the most pressing issue right now, however, might not be what kind of federal privacy law is needed. Some federal privacy law would be better than none, because the lack of such federal law will be more damaging as the situation remains stagnant leading to a tsunami of privacy violations with the Internet of Things.[281] Also, different state-level GDPR-like bills are being introduced at a fast pace,[282] and having to comply with all the state laws would be a "logistic nightmare" for American companies.[283] Some might argue that the Congress needs adequate time to come up with an ideal bill.[284] But it is wiser to enact the statute first, and then amend it if necessary, which is how California deals with its CCPA.[285]

---

276. David Meyer, *'We Look Forward to Improvements.' Big Tech Plans to Fight Back Against California's Sweeping New Data Privacy Law*, FORTUNE (July 2, 2018, 6:26 AM), http://fortune.com/2018/07/02/california-data-privacy-ab-375-big-tech-fightback/.

277. Lindsay Rowntree, *An American Perspective: The Three Worst Things About the EU GDPR*, EXCHANGEWIRE (July 7, 2016), https://www.exchangewire.com/blog/2016/07/07/an-american-perspective-the-three-worst-things-about-the-eu-gdpr/.

278. 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.

279. Rachel England, *Tim Cook Calls for GDPR-Style Privacy Laws in the US*, ENGADGET (Oct. 24, 2018), https://www.engadget.com/2018/10/24/tim-cook-calls-for-gdpr-style-privacy-laws-in-the-us/.

280. Justin Jaffe & Laura Hautala, *What the GDPR Means for Facebook, the EU and You*, CNET (May 25, 2018, 8:58 AM), https://www.cnet.com/how-to/what-gdpr-means-for-facebook-google-the-eu-us-and-you/.

281. *See* Goyal, *supra* note 56 (suggesting the "Internet of Things" would make data gathering much easier).

282. AKIN GUMP, *supra* note 269.

283. 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.

284. *See* Charlie Warzel, *Opinion: Will Congress Actually Pass a Privacy Bill?*, N.Y. TIMES (Dec. 10, 2019), https://www.nytimes.com/2019/12/10/opinion/congress-privacy-bill.html (arguing that, because privacy is a complex and important issue, it would be a mistake for Congress to rush passing a bill).

285. *CCPA Amendment Tracker*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/resources/article/ccpa-amendment-tracker/.

b. Adopt the Framework of GDPR/CCPA

The GDPR in its entirety might not be suitable for the United States, and the CCPA might place too much responsibility on technology companies,[286] but a framework offered by these two laws may be used to facilitate the process of enacting a similar federal law.[287] Moreover, quite a few American companies are already in compliance with GDPR,[288] and such compliance usually warrants compliance with CCPA.[289] Thus, adopting the framework will ease American companies' compliance burden.[290]

c. Avoid mistakes made by GDPR or CCPA

The federal law should provide flexibility for companies to innovate. Both GDPR and CCPA contain key terms that are too broad.[291] More carefully defined terms will help companies to comply with the law and keep innovating without too much burden.[292] For example, the federal law should better define "publicly available information" if it decides to follow CCPA and exclude such information from its scope.[293]

The federal law should regard various non-compliances, not just actual data breaches, as violations subject to fines. In other words, it should opt for the GDPR approach when it comes to preventing data breaches. A company will not be fined under CCPA when there are no actual data breaches, even if the company fails to take adequate preventive measures.[294] This approach does not serve consumers' interests as "incentives for companies to protect data" skew toward "self-flagellating disclosures" rather than prevention.[295]

The federal law should explore a reasonable algorithm for calculating fines. Under CCPA, organizations can be fined for a maximum of 7500 USD for each intentional breach, while under GDPR organizations can be fined for a maximum of 20 million Euros or four percent of their annual revenue for either

286. Rashid, *supra* note 278.

287. *See* INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, COMPARING PRIVACY LAWS: GDPR VS. CCPA 5, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (explaining that the laws are functionally very similar, but differ in significant ways, such as core legal framework; scope of application, nature and extent of collection limitations; and rules concerning accountability).

288. *Pulse Survey: GDPR Budgets Top $10 Million for 40% of Surveyed Companies*, PRICEWATERHOUSECOOPERS (last visited Feb. 18, 2020), https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act/pulse-survey-large-companies-spend-over-100-million.html.

289. Geoffroy De Cooman, *GDPR and CCPA Compliance: The 5 Differences You Should Know*, PROXYCLICK (Oct. 7, 2019), https://www.proxyclick.com/blog/gdpr-and-ccpa-compliance-5-differences.

290. *Id.*

291. *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.

292. *See* Sam Sabin, *Fresh Off GDPR, Companies Puzzle Over Complying With California's Privacy Law*, MORNING CONSULT (Dec. 18, 2018, 12:00 PM), https://morningconsult.com/2018/12/18/fresh-off-gdpr-companies-now-have-to-prepare-for-californias-privacy-law/ ("[CCPA] creates 'unworkable obligations.'").

293. Stuart L. Pardau, *The California Consumer Privacy Act: Towards A European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 106 (2018).

294. CAL. CIV. CODE § 1798.155 (2018).

295. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

intentional or negligent violations.[296] The GDPR may be too harsh in terms of the amount of fines and the lack of intention requirement, unnecessarily hindering companies' willingness to innovate, which is especially harmful to startups.[297] In contrast, CCPA's punishment provisions are toothless when tech giants violate the statute because the maximum fine is only 7,500 dollars, and there needs to be an actual data breach which also needs to be caused by the company's intentional violation.[298] This Note suggests that the federal law should instead have an algorithm resembling the following: a company can be fined for a maximum of two percent of its global revenue for its first violation, and four percent for its second violation, etc. This way, startups will not have too much anxiety over unintentional mistakes made when innovating, and tech giants will not merely treat the fines as transaction costs.

d. Assign the FTC a clear role in Regulating Data Privacy

Many companies question the FTC's authority to regulate privacy practices, which greatly weakens the efficiency of enforcement of several existing privacy laws.[299] A proposed federal privacy law should delineate the FTC's role in this area. An alternative option might be to establish a new federal agency to regulate all privacy related issues.

B. Data Localization vs. Data Globalization

Should the United States join the trend of data localization, just like many other major economies? The countries that restrain cross-border data flows have their legitimate reasons: data localization may provide one country with better information security against foreign intelligence agencies; it could help protect citizens' right of privacy; it could also play an important role in anti-terrorism.[300] But whether or not those issues would be addressed by data localization at all remains a question.[301] More importantly, restriction of data flow creates more problems than it might solve.[302]

---

296. Sabin, *supra* note 292. *See* CAL. CIV. CODE § 1798.155 (2018); GDPR Art. 83 (stating that whichever of the two amounts is higher will be the maximum amount, which means if a company's annual revenue is 20 million euros, one violation will cost it all its revenue).

297. Guy Chazan, *SAP Raises Fears Over EU Data Privacy Rules*, FIN. TIMES (Jan. 15, 2017), https://www.ft.com/content/22d5e078-d9a1-11e6-944b-e7eb37a6aa8e ("[T]he 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. . . .").

298. CAL. CIV. CODE § 1798.155(b) (2018).

299. *See supra* Section III.B.2 (discussing how some companies argue that the FTC lacks jurisdiction in policing data-security practices).

300. Selby, *supra* note 85. *See* Joshua D. Blume, *Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy, Localization, And Cybersecurity Laws*, 49 GEO. J. INT'L L. 801, 816 (2018) (discussing how some privacy laws have localization requirements, which "leave citizens more vulnerable").

301. Daniel Castro, *The False Promise of Data Nationalism*, INFO. TECH. & INNOVATION FOUND. (Dec. 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf (discovering that the security of data does not depend on where it is stored).

302. *Id*. ("[D]ata nationalism will similarly lead to poor economic outcomes.").

Data localization acts as barrier to trade and investment.[303] It affects digital communication, social media service and personal records.[304] The uncertainty caused by possible information flow disruption would see lower levels of foreign investment by big companies.[305]

Data localization usually hurts privacy and data security, which the countries restricting data flow claim to protect.[306] It may be difficult for multinational companies to exercise control over their data when the data is decentralized as a result of a balkanized Internet.[307] Additionally, the localization requirements adopted by several different countries require certain data to be stored in multiple places around the world, which increase the probability of error, including failure to update all the data sets when a record is deleted in one country.[308]

The United States might continue defending free data flow by upholding existing agreements within the WTO framework.[309] Data localization is likely to be in violation of the General Agreement on Trade in Services (GATS).[310] It is true that the GATS provides an exception where data localization is "necessary to secure compliance with laws or regulations" relating to "protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[311] But to be covered by this exception, any data localization should be "necessary" to protect privacy.[312] The same restriction applies to the national security exception,[313] which China uses to justify its cybersecurity law.[314]

The United States should also urge other countries to loosen their data localization requirements by bilateral agreements. Restrictions on data localization requirements have appeared in the Trans-Pacific Partnership Agreement, in the digital trade chapter in NAFTA,[315] and in the Trade in Services Agreement.[316] Even if the trend of data localization is inevitable, its

303. *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, ALBRIGHT STONEBRIDGE GROUP (Sept. 28, 2015), https://www.albrightstonebridge.com/news/data-localization-challenge-global-commerce-and-free-flow-information.

304. *Id*.

305. *Id*.

306. Bret Cohen, Britanie Hall & Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and The Global Economy*, 32 ANTITRUST ABA 107, 108–09.

307. *Id.* at 108.

308. *Id*.

309. Finbarr Bermingham & Adam Behsudi, *Donald Trump's Block on WTO Judges Creates 'Doomsday Scenario' for World Trade Disputes*, SOUTH CHINA MORNING POST (Nov. 21, 2019, 6:00 PM), https://www.scmp.com/economy/china-economy/article/3038697/donald-trumps-block-wto-judges-creates-doomsday-scenario (stating that WTO's appeals body will be paralyzed by Donald Trump blocking crucial reappointments of judges).

310. Blume, *supra* note 300, at 807.

311. GATS art. XIV(c)(ii).

312. *See id*. (stating that it is necessary to protect the privacy of individuals).

313. GATS art. XIV *bis* 1(b).

314. Blume, *supra* note 300, at 827–28.

315. NAFTA art. 19.11.

316. Jeremy Malcolm, *TISA Proposes New Global Rules on Data Flows and Safe Harbors*, ELECTRONIC FRONTIER FOUND. (Oct. 24, 2018), https://www.eff.org/deeplinks/2016/10/tisa-proposes-new-global-rules-data-flows-and-safe-harbors.

extent still matters.[317] At a minimum, the U.S. should ensure that other major countries do not lean toward more extreme versions of data localization. Also, as China further embraces globalization, it is in China's interest to realize that data localization creates the problem of reinventing the wheel, and that balkanizing the internet[318] would eventually harm the global economy, which would in turn inevitably slow their economic growth.[319] The big data gathered by Chinese government and Chinese companies are like the abundant cheap labor in this country, and combined with American investment and American intelligence, the data could surely benefit both countries.[320]

V. CONCLUSION

Data gathering often violates citizens' right to privacy, but it cannot be denied that big data is fundamentally able to change the world. In particular, big data is the lifeblood of AI. Additionally, AI-driven advantages in technology and the economy may compound with interest.

Because of Chinese citizens' support for data gathering, the absence of a single law governing data protection, and the data localization required by the Chinese government, Chinese companies are likely to enjoy the exclusive benefit from China′s unabashed fervor for collecting data. This advantage could further turn into an edge in the development of AI. In the U.S., the patchwork of laws protecting personal data act as a barrier for good faith companies to gather necessary data for innovation, which is exacerbated by the lack of public support for the big data industry.

With the Internet of Things around the corner, data privacy violations are likely to skyrocket. Meanwhile, the Chinese government is determined to make use of the country's abundant data for the battle to define generations of technology to come. Therefore, the U.S. might want to adopt a single Federal law governing personal data as soon as possible.

Also, the trend of data localization, which is joined by China and the EU, is making the situation worse for the U.S. To maintain its economic and technology advantage, the U.S. should resist the global trend of data localization, through WTO or free trade agreements.

317. Chris Mirasola, *U.S. Criticism of China's Cybersecurity Law and the Nexus of Data Privacy and Trade Law*, LAWFARE (Oct. 10, 2017), https://www.lawfareblog.com/us-criticism-chinas-cybersecurity-law-and-nexus-data-privacy-and-trade-law.

318. *See supra* section II.C. (data localization would greatly worsen the balkanization of the Internet).

319. *Id.*

320. *See supra* section II.A. (China's cheap labor once benefited both the U.S. and China).