Catholic University Journal of Law and Technology

Volume 31
Issue 1 *Fall 2022*

Article 3

2022

The Rise of 5G Technology: How Internet Privacy and Protection of Personal Data Is a Must in An Evolving Digital Landscape

Justin Rabine

THE RISE OF 5G TECHNOLOGY: HOW INTERNET PRIVACY AND PROTECTION OF PERSONAL DATA IS A MUST IN AN EVOLVING DIGITAL LANDSCAPE

Justin Rabine

With the rise of 5G technology, there is growing concern regarding user privacy.[1] 5G stands for "fifth generation" mobile technology, and its biggest draw is increased speed in comparison to the fourth generation of mobile technology, 4G.[2] 5G internet allows for shorter latency periods, which is the wait time a device spends to process information on the internet.[3] For example, 5G internet technology allows a user to download a full-length movie in fifteen seconds, whereas 4G technology takes a user six minutes to download the same movie.[4] However, this increased internet speed raises concern about user privacy, because the speed and accuracy of 5G technology allows someone to track another individual's physical location in almost real time within centimeters of the persons actual location.[5] The government of the United States also utilizes increased download speed and accurate pinpointing of user information for counterterrorism efforts.[6] These heightened download speeds and identification capabilities, combined with the lack of disciplinary measures against nongovernment users tracking individuals' data, creates a massive potential for abuse.[7] This combination is comparable to a video game hacker using in-game player locations to gain leverage over other players in a game.[8] Data collection groups claim that most user data is anonymous, yet, parties can

---

1 *See generally* Edward C. Baig, *5G Is Speedy, but Does It Also Raise the Stakes on Privacy, Security, Potential Abuse?*, USA TODAY, https://www.usatoday.com/story/tech/2019/03/27/will-new-5-g-wireless-network-threaten-your-privacy/3032281002/ (Mar. 28, 2019) (discussing ways attackers may pry into user privacy using 5G technology).

2 Drew FitzGerald et al., *Everything You Need to Know About 5G*, WALL ST. J. (Nov. 10, 2020), https://www.wsj.com/articles/everything-you-need-to-know-about-5g-11605024717#:~:text=It%20achieves%20that%20speed%20by,roughly%20six%20minutes%20on%204G (describing strength of 5G and its differences from 4G).

3 *Id.*

4 *Id.* (discussing 5G speed in rates of full-length movie downloads relative to 4G).

5 Drew FitzGerald, *5G Race Could Leave Personal Privacy in the Dust*, WALL ST. J. (Nov. 11, 2019), https://www.wsj.com/articles/5g-race-could-leave-personal-privacy-in-the-dust-11573527600 ("New 5G networks, however, will be able to track smartphone users with more precision, pinpointing a device within centimeters rather than meters. 'People know that they're being tracked online . . . [p]eople don't realize that they can be in the same situation in the physical world.'").

6 *See generally* USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (enabling government officials to track data of users suspected of terrorism or terroristic plots, thereby bypassing the Fourth Amendment for special cases subjectively deemed to be so by those government officials).

7 *See generally* Baig, *supra* note 1.

8 FitMC, *The Fall of Minecraft's 2b2t*, YOUTUBE (July 24, 2021), https://www.youtube.com/watch?v=elqAh3GWRpA (discussing how hacker group Nerds Inc., utilized a bug called the NoCom exploit, to simultaneously track all player data and location on the server in real time in order to locate and destroy player bases and steal resources).

remove that anonymity with relative ease, allowing any contractor that purchases the data to obtain location data directly from used applications.[9]

The first countries to implement 5G technology across their nations will have a great technological advantage compared to their peers.[10] If a nation were to spearhead consumer privacy protection in the 5G domain, such protection may become a worldwide standard and could influence other countries, including China or the United States, to conform to that standard.[11] The United States and China are in a race to be at the forefront of the 5G technology boom and capitalize on the opportunities the technology presents.[12] In 2017, China enacted the National Intelligence Law (NIL), which requires Chinese telecom operators to provide the Chinese government technology and services.[13] Foreign companies that have Chinese controlling shareholders are also subject to Chinese control.[14] This type of access raises alarms as to data privacy issues, especially in competing nations such as the United States.[15]

5G technology is primed to permeate all aspects of Americans' digital lives

---

9 *See* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x ("U.S. Special Operations Command . . . a branch of the military tasked with counterterrorism . . . bought access to Locate X [one of two data location streams] to assist on overseas special forces operations. The other stream is through a company called X-Mode, which obtains location data directly from apps, then sells that data to contractors, and by extension, the military. . . . The Locate X data itself is anonymized, but the source said, 'we could absolutely deanonymize a person.'").

10 *See* Stuart Brotman, *Consumer Privacy Protection Deserves 5G Policy Attention*, LAW360 (Nov. 26, 2019), https://www.law360.com/articles/1222862/consumer-privacy-protection-deserves-5g-policy-attention ("Federal Communications Commissioner Jessica Rosenworcel noted the Defense Innovation Board's assessment that 'the country that owns 5G will own innovations and set the standards for the rest of the world.'").

11 *Id.* ("As a practical matter, this would force China and other countries supplying this equipment [to implement 5G technology] to conform to a U.S. standard. In turn, this would address the ongoing U.S. national security concerns regarding foreign hardware provisioning and also help the U.S. create a de facto worldwide standard for 5G consumer privacy protection.").

12 Kirsten S. Lowell, Note, *The New "Arms" Race: How the U.S. and China Are Using Government Authorities in the Race to Control 5G Wearable Technology*, 12 GEO. MASON J. INT'L L. 75, 76–77 (2021) (discussing the race to fully implement domestic 5G technology between the United States and the People's Republic of China so each could capitalize on the economic and innovative opportunities the new technology might provide them).

13 *Id.* at 96 (detailing the Chinese National Intelligence Law requiring that "any organization and citizen, shall in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work they are aware of.").

14 *Id.* (discussing how the Chinese National Intelligence Law requires telecommunication operators and companies from foreign countries with Chinese controlling shareholders to provide Chinese intelligence services or military access to technology and services).

15 *See id.*

through its widespread use in social media applications, cellular services, and technological devices, such as cell phones and tablets.[16] The United States failed in implementing strong privacy laws and instead put in place the Patriot Act that weakened privacy protections.[17] The United States' inability to set in place privacy laws as a model for the world to follow has inadvertently allowed the Chinese government to have nearly unfettered access to American personal information, and 5G technology has exacerbated this problem.[18]

American legislation protects an individual's right to privacy in specific, narrow situations, such as the Children's Online Privacy Protection Act (COPPA), the Electronic Communications Privacy Act (ECPA), the Fair Credit Reporting Act (FCRA), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Video Privacy Protection Act (VPPA).[19] However, there is no broad enactment to protect personal information more generally, especially in the context of 5G technology.[20] A broad enactment of privacy rights protections would help prevent the erosion of individual liberty, which would, in turn, protect human dignity.[21]

There is also privacy legislation that originates from the European Union.[22]

---

16 *See generally* Christian de Looper & Andrew Martonik, *What Is 5G? Speeds, Coverage, Comparisons, and More*, DIGITALTRENDS (Apr. 30, 2022), https://www.digitaltrends.com/mobile/what-is-5g/ (detailing the evolution of 5G technology, how it works, the speed at which it works, what carriers provide 5G coverage, and recommendations for cellular devices with 5G capabilities).

17 *See generally* USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 281 (creating a government exception in which government officials can track users and user internet data who are suspected of terrorism or terrorist plots, thereby legally bypassing the Fourth Amendment for special cases deemed special subjectively by American government officials).

18 *See* Lowell, *supra* note 12, at 81 (providing a detailed discussion on the workings of 5G technology).

19 *See generally* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ (contrasting the United States' mix of various laws, which are designed only to target specific types of data in special, albeit outdated, circumstances, to the European Union's General Data Protection Regulation, which "requires companies to ask for some permissions to share data and gives individual rights to access, delete, or control the use of that data."); *What is Privacy?*, PRIV. INT'L (Oct. 23, 2017), https://privacyinternational.org/explainer/56/what-privacy (discussing why privacy is necessary to protect individual liberty and human dignity in the technological age).

20 *See* Klosowski, *supra* note 19.

21 *See id.*

22 *See, e.g.*, Nicholas F. Palmieri III, Note, *Data Protection in an Increasingly Globalized World*, 94 IND. L.J. 297, 306 (2019) ("Unlike China and the United States, the

The European Union attempts to govern data protection and user privacy through the General Data Protection Regulation (GDPR), which allows for protection of personal information of citizens of European Union member states.[23] The Charter of Fundamental Rights of the European Union (the Charter), a legally binding document protecting freedoms and rights enjoyed by citizens of European Union member states, outlines protected fundamental human rights including the general right to privacy and the right to protection of personal data.[24] However, a lack of centralized enforcement and an increase in member states' desire to implement national security measures has withered away much of the strength that the GDPR and the Charter were intended to protect.[25]

Congress should implement an umbrella privacy protection law to replace the current array of niche privacy laws.[26] Fourth Amendment protections should be expanded to a person's data even though they may not physically own it.[27] To provide better privacy protection in the 5G era and beyond, Congress can restrict how the government purchases location data of 5G internet users and implement tighter restrictions on businesses that download private data.[28] Furthermore, this protection of privacy through 5G technology should focus on restricting the purchase of location data and personal data.[29] Courts should adopt broader protection for individuals under the Fourth Amendment to not require a person to physically own something – such as virtual data – for it to obtain Fourth

---

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

23 *Id.*

24 *See generally* Charter of Fundamental Rights of the European Union, Oct. 26, 2012, (C326) (outlining the fundamental rights, freedoms, and principles recognized by the European Union and protected by the Union's member states).

25 *See* Karl Colbary, Note, *Outsourcing the Police: How Reliance on the Private Sector for Law Enforcement Threatens Privacy Legislation Around the World*, 41 NW J. INT'L L. & BUS. 213, 228 (2021) (discussing how the GDPR, although it may do good in protecting the privacy of individuals, is unlikely to be able to curtail large government surveillance because of competing interests of law enforcement and national security); *see also* Melanie Smith, *Challenges in the Implementation of EU Law at National Level*, EUR. PARLIAMENT BRIEFING 1, 9 (Nov. 2018), https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/608841/IPOL_BRI(2018)608841_EN.pdf (illustrating how "greater centralisation of decision making was a key success indicator in achieving swift implementation" and how the European Union lacked that necessary centralization).

26 *See generally* Klosowski, *supra* note 19.

27 *See generally* PRIV. INT'L, *supra* note 19.

28 *See generally id.*

29 *See generally id.*

Amendment protection.[30] To provide privacy protection, courts should also restrict the government's purchase of location data of 5G internet users and restrict businesses downloading private data when such persons are users of 5G.[31] An umbrella privacy protection law restricting the government's purchase of location data of 5G internet users and restricting business downloading of private data through 5G technology usage will protect Americans' liberty and dignity while using 5G technology.[32]

Part I of this Note provides an overview of 5G technology and how the United States and China are currently implementing the technology. Part II discusses the current climate around the right to privacy and the laws governing privacy in different countries, specifically those laws in the European Union, China, and the United States. Lastly Part III analyzes how to improve on current solutions that address the ongoing lack of privacy laws.

I. 5G TECHNOLOGY: A GAME OF MILLIMETERS, METEORIC SPEEDS, AND MISSED POTENTIAL

5G is the latest generation of wireless network technologies and will increase bandwidth to faster speeds than any previous generation of mobile phone technologies.[33] This increased speed illustrates the powerful potential of 5G technology in comparison to its predecessors.[34] Additionally, the current networking and technological posture of China, the European Union, and the United States explain why 5G could have a massive effect on user privacy moving forward.[35]

---

30 Carpenter v. United States, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) ("Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents."); *see generally* Daniel Woislaw, *With 5G Arriving, the Supreme Court Needs to Rule on What Digital Privacy Means*, PAC. LEGAL FOUND. (Jan. 1, 2020), https://pacificlegal.org/with-5g-arriving-the-supreme-court-needs-to-rule-on-what-digital-privacy-means/ (discussing potential court cases that the Supreme Court may use for guidance in its decision on Fourth Amendment protection rights for digital privacy rights, especially in the scenario of society's progression towards 5G).

31 *See generally* Klosowski, *supra* note 19.

32 *See* PRIV. INT'L, *supra* note 19.

33 CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10265, OVERVIEW OF LEGAL CHALLENGES TO THE FCC'S 5G ORDER ON SMALL CELL SITING 4 (2019) (discussing the implementation of 5G technology and its range of benefits).

34 *See id.* (illustrating how 5G technology works and its benefits over 4G networks).

35 *See generally* JOHN R. HOEHN & KELLEY M. SAYLER, CONG. RSCH. SERV., IF11251, NATIONAL SECURITY IMPLICATIONS OF FIFTH GENERATION (5G) MOBILE TECHNOLOGIES 17 (2022) (illustrating the contrast in rollout speed of 5G technology in America to the rollout speed of 5G technology in China).

A. What is 5G?

5G is the latest and fastest generation of wireless network technologies.[36] 5G will provide increased bandwidth for faster download and upload speeds than any previous generation of mobile phone technologies.[37] 5G's increased speed is possible through improvements in existing 4G networks and using new higher radio frequencies that range from 30 to 300 gigahertz to accomplish the mammoth task.[38] These higher radio frequencies require newer, smaller towers (cell sites).[39] These smaller towers must be placed closer together and can be installed on various structures, such as streetlights, utility poles, and buildings.[40] In contrast, older towers provided service by being spaced further apart.[41]

The three types of airwaves that carry 5G signals are low-band, mid-band, and high-band spectrum waves.[42] Radio wavelength is measured in centimeters, but the wavelength of 5G frequencies is measured in millimeters.[43] High-band spectrum is measured with millimeter waves, which cover the shortest range but provides the highest speeds and the greatest rate of data transference.[44] These millimeter waves are the driving innovation behind the success of the 5G network.[45] Millimeter waves are 10 to 100 times higher in frequency than those used for 4G and Wi-Fi networks.[46] Millimeter waves provide increased bandwidth and speed, but, because they are small, they cannot travel long distances or penetrate buildings meaning that many small cell site towers must be placed near each other to be effective.[47]

---

36 LINEBAUGH, *supra* note 33 (illustrating how 5G technology is the newest wireless network technology and the benefits that the newest generation of wireless network technology provides).

37 *Id.* (discussing the range of benefits of 5G technology and the steps for its implementation).

38 *See id.* (detailing how 5G technology will be successfully implemented nationwide).

39 *Id.* (discussing how the 5G network employs smaller cell sites in close proximity to one another).

40 *Id.* (illustrating where the small cell sites may be installed).

41 *Id.* (discussing physical technology of 5G infrastructure and places where small cell sites can be blended into existing structures).

42 Jared Council, *Why the U.S. Rollout of 5G Is So Slow*, WALL ST. J. (May 25, 2021), https://www.wsj.com/articles/5g-us-rollout-11621897471.

43 Tim Childers, *5G Network: How Does It Work, and Is It Dangerous?*, LIVE SCI. (Feb. 1, 2021), https://www.livescience.com/65959-5g-network.html ("Millimeter waves use frequencies from 30 to 300 gigahertz, which are 10 to 100 times higher than the radio waves used today for 4G and Wi-Fi networks. They're called millimeter because their wavelengths vary between 1 and 10 millimeters, whereas radio waves are on the order of centimeters.").

44 Council, *supra* note 42 (showing how millimeter waves cover short ranges but provide greatest speed and bandwidth).

45 Lowell, *supra* note 12, at 81.

46 *See id.* (showing how millimeter waves of 5G technology are significantly higher than those of previous technology).

47 *Id.* (asserting that this inability of 5G millimeter waves to penetrate obstacles will

The three main benefits to 5G technology are faster speeds, support of a larger number of simultaneous connections, and faster response times between internet machines such as cell phones or personal computers.[48] 5G technology enables increased speeds of data transfer and improved bandwidth compared to 4G technology.[49] These 5G download speeds are so instant that downloading a 3-gigabit game onto a cellular device takes only about twenty-four seconds, which is about thirty-five times faster than 4G internet technology and over 4,000 times faster than 3G internet technology.[50] The technological improvements 5G creates are expected to increase the support of interconnected and autonomous devices, including smart homes, self-driving vehicles, automatic agricultural systems, intuitive industrial machinery, and advanced robotics.[51]

Furthermore, whichever country successfully implements 5G first will have a technological advantage over its peers.[52] The benefits of 5G can only be achieved through production of the hardware that enables the technology to operate.[53] The countries that control the production of the hardware necessary for 5G will have an advantage in acquiring those three 5G benefits over those who do not possess such hardware.[54]

B. 5G in China, the European Union, and the United States

China is currently the world's leader in 5G hardware production and is poised to be the first country to deploy a 5G wide-area network.[55] A wide-area network provides network connectivity to computers and internet accessible devices over large distances.[56] Due to China's unique position as a leader of 5G technology,

---

lead to small cell sites necessarily becoming so ubiquitous that "[i]n the future it will be nearly impossible to go anywhere without seeing a small cell.").

48 Council, *supra* note 42 (analyzing benefits of a 5G internet technology infrastructure initiative).

49 *See* HOEHN & SAYLER, *supra* note 35 (detailing national security concerns related to rollout of 5G for both domestic and military uses).

50 Elliot Bentley & Sarah Krouse, *How Fast 5G Mobile Internet Feels*, WALL ST. J. (Feb. 22, 2019), https://www.wsj.com/graphics/how-fast-5g-mobile-internet-feels/ (showing a visualization comparing 5G, 4G, and 3G downloading speeds of the game "Fortnite").

51 HOEHN & SAYLER, *supra* note 35 (discussing devices that 5G is expected to support).

52 *Id.* (illustrating how not only consumer goods could be interconnected using 5G technology, but also how 5G technology could improve various aspects of military operations).

53 *Id.* (discussing the need for an installation of a high number of cell sites utilizing millimeter waves are needed to enable proper utilization of 5G).

54 *See generally id.* (explaining the different segments of the electromagnetic spectrum that must be used to produce 5G technologies to render interpretation of the advantages).

55 *Id.*

56 *What is a WAN? WAN vs. LAN*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/what-is-a-wan/ (last visited Nov. 12,

Chinese companies are well-positioned as global 5G suppliers.[57] National security experts are concerned that Chinese companies such as Huawei are introducing intentional vulnerabilities in the technology for malicious purposes.[58] The Chinese National Intelligence Law (NIL) gives the Chinese government intelligence services backdoor access to private data retained by Chinese telecom operators.[59] The NIL also raises further concerns about personal information privacy when combined with the intentional vulnerability concerns.[60]

The European Commission – the European Union's politically independent executive branch – committed over €700 million between 2013 and 2020 to accelerate 5G technology research and innovation through its "Horizon 2020 Programme."[61] European Union investment intends to improve network and internet structure in emerging technological fields.[62] The European Union has an aggressive plan to provide uninterrupted 5G coverage in urban areas along its main paths of transportation by 2025 and coverage to all populated areas by 2030.[63] This aggressive European plan depends closely upon access to radio signals, which will provide a basis for wireless technologies.[64] In adequately using European radio signals, the European Union can provide superior 5G services across vast swaths of territory.[65]

Although 5G internet connectivity technology is fast, the same cannot be said about its rollout speed, especially in the United States.[66] The benefits surrounding 5G technology are hampered when the infrastructure standards

---

2022).

57 HOEHN & SAYLER, *supra* note 35.

58 *Id.* (discussing how national security experts are concerned about the vulnerabilities present in Chinese-made 5G infrastructure products and how such vulnerabilities may be exploited to conduct cyberattacks or espionage against foreign militaries or industries).

59 *Id.*

60 *See id.*

61 *Shaping Europe's Digital Future*, EUROPEAN COMM'N, https://digital-strategy.ec.europa.eu/en/policies/5g (last visited Nov. 20, 2022) (outlining the efforts of the European Union to successfully implement 5G technology across its member states).

62 *Id.* (illustrating the desires of the European Union to invest in the emerging technological fields of machine-to-machine communication and the Internet of Things).

63 *Id.* (providing a plan outset by the European Union ensuring "uninterrupted 5G coverage in urban areas and along main transport paths by 2025," and setting goals "to cover all populated areas with 5G by 2030.").

64 *Id.* ("The deployment of 5G networks depends closely upon access to radio spectrum, the basis of wireless technologies. As the rate of connected devices and their use increases, spectrum resources and their uses have to be harmonised across Europe to allow for interoperability of infrastructure across borders.").

65 *See id.*

66 *See* Council, *supra* note 42 (discussing the slow implementation of 5G technology in the United States after being publicized back in 2019 when the first 5G capable phones made their debut on the market).

required are not met.[67] Infrastructure standards are necessary because 5G technology, like its predecessors, has a limited range, which limits accessibility for consumers.[68] These shortfalls can occur because tangible accessibility is unavailable or because investors are unwilling to invest large sums of money into the project.[69] The main reason behind the slow rollout rate in the United States is that telecommunications companies are hesitant about investing in 5G internet technology after there was little return on their investments into 4G internet technology years ago.[70] 5G requires a great density of cell towers to be the most effective because the millimeter wave range is extremely short and individual American population centers are not dense in relation to one another.[71] There are two major reasons that investment in 5G has been limited.[72] First, this infrastructure overhaul would take a great sum of money from investors, who are already hesitant about investing their capital after being burned previously.[73] Second, the overhaul would take a great deal of time as companies must get the necessary permits, locate correct building sites for prime optimization, and deploy the fiber-optic cables necessary to carry data from cell tower to cell tower.[74] The rollout speed of 5G technology in the United States is therefore slowed because consumers are unable to access the technology and potential investors do not provide enough investment into the technology.[75]

The limited rollout speed of 5G technology in American cities can be contrasted with the increased rollout speed of America's greatest economic

---

67 *See id.*

68 *See id.* ("5G at its best is a fundamentally different network than 4G, ... mean[ing] it requires different technology and equipment that [has] to be installed—not a simple process.").

69 *See id.* ("When 4G made its debut around 2010, there were about a dozen technology providers offering wireless network equipment, . . . including Nortel in Canada and Motorola in the U.S. Today, the global provider market comprises five main players: Nokia, Ericsson, Samsung, ZTE and Huawei.").

70 *Id.* (quoting John Roese, Dell Technologies Inc.'s chief technology officer and a former executive with other telecom carriers such as Huawei Technologies Co. and Nortel Networks Inc., "[t]hey got burned once before . . . . So[,] they're very cautious about it[,]" referring to disappointing returns on 4G network investments for telecom carriers, which instead brought a boon to technology companies that offered apps and other services over those networks supplied by the telecom carriers).

71 *Id.* (quoting Stefan Pongratz, an analyst at Dell'Oro Group, "millimeter-wave 5G requires the greatest density of cell towers to be effective," and "adding density takes time.").

72 *See id.*

73 *Id.*

74 *Id.* ("Installing new equipment can involve finding a site, getting proper permitting and, in some cases, digging up streets to deploy the fiber-optic cables that carry data to and from cell towers . . . .").

75 *Id.*

competitor, China.[76] Only two-thirds of the American population are expected to have access to 5G technology by 2023.[77] As of February 2021, 5G technology was available in 341 Chinese cities compared to only 279 cities in the United States.[78] The Chinese government has contributed to China's recent 5G technology boom by limiting foreign competition in China's 5G technology sector. Specifically, the Chinese government has imposed new regulations on foreign investment and 5G-related imports.[79] The Chinese government also provides subsidies for domestic 5G technology research, development, manufacturing, and raw material.[80] Furthermore, the Chinese government leverages its military and government intelligence agencies to provide ample industrial espionage on foreign competitors.[81] The United States government, on the other hand, has taken a back seat approach to the development of a national 5G system, relying largely on capitalist market forces to provide competition and innovation.[82] China's centralized approach of aggressive investment in its rollout of 5G in Chinese cities appears to have been more successful thus far, as the country remains the leader in 5G implementation over its American rival.[83]

II. INTERNET PRIVACY LAWS IN CHINA, THE EUROPEAN UNION, AND THE UNITED STATES

The protection of personal information, and a user's ability to control such information, is increasingly at the forefront of the international stage.[84] By requiring Chinese telecom operators to provide Chinese government officials with technology and services, the 2017 NIL limited foreign access to Chinese citizens' personal information.[85] The European Union governs data protection

---

76 *Id.*

77 *Id.* (analyzing a possible benchmark date somewhere between late 2021 and late 2023 for the two-thirds benchmark).

78 *The State of 5G*, VIAVI SOLS., https://www.viavisolutions.com/en-us/literature/state-5g-deployments-2021-posters-en.pdf (last visited Nov. 20, 2022).

79 Lowell, *supra* note 12, at 77 (discussing ways that the Chinese government supports 5G technology through its authoritarian, anti-capitalist policies).

80 *Id.*

81 *Id.*

82 *Id.* (comparing the Chinese system of 5G technology implementation to the capitalist system present in the United States where the government does not have a national plan to develop the 5G technology system and instead primarily relies on private companies to compete against each other, to innovate, and to create their own network, which the United States believes will yield greater results in the technological innovation).

83 *See id.*

84 *See* Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL OF RTS. J. 975, 976–97 (1999).

85 Lowell, *supra* note 12, at 96.

and user privacy using the GDPR, which protects personal information of member states' citizens that is stored across the globe.[86] The United States provides privacy protection to Americans, but only in restricted instances and through a number of narrowly tailored laws.[87]

A. Impact of 5G Technology on Personal Information and User Privacy

Tensions are rising over concerns pertaining to privacy rights in information privacy, specifically in personal information and a user's ability to control such information.[88] Personal information is normally considered information that a user has shared through services requiring authorization in an online forum such as through a bank or method of payment.[89] Personal information ranges from social security numbers, addresses, telephone numbers, banking records, credit card purchases, phone calls, and medical treatments.[90] A government can use any of this "assigned personal information" to identify an individual and track the individual through his or her activities and habits.[91] The information can be used for a variety of purposes by governments, businesses, and individuals without the user's knowledge.[92]

The ultimate uses and potential misuses of users' personal information gives rise to concerns surrounding security and information privacy.[93] New technology and improved uses of current technology distort the differences between simple surveillance in the protection of the general populace and the use of personal information to provide more targeted and invasive surveillance of individuals in a potentially unjust manner.[94] Furthermore, current legislation aimed at protecting privacy may be deemed ineffective with the rapid

---

86 Palmieri III, *supra* note 22.

87 *See generally* Klosowski, *supra* note 19.

88 Kearns, *supra* note 88, at 976–77 (discussing the right to privacy of personal information and surveillance technology that infringes on an individual's right to privacy, noting the ways in which the advancing technology potentially impacts individual privacy interests).

89 *Id.* at 976.

90 *Id.* at 976 (detailing a list of various pieces of personal information that may be compromised by invasive technologies bent on infringing on user privacy).

91 *Id.* at 977.

92 *Id.*

93 *Id.*

94 *Id.* ("New technology and new uses of current technology, however, blur the distinction between surveillance activity and the use of personal information. New surveillance technology can obtain and store personal information about an individual, while personal information can be used in new ways akin to surveillance. This merging of two categories of technology presents new challenges for the right to privacy and amplifies existing challenges.").

development of surveillance technologies, which oftentimes outpace laws that are intended to regulate its use.[95] All of these privacy concerns are amplified with the rise of 5G as a new technology and its increased speed to perform such surveillance functions.[96] With the implementation of 5G technology, individuals will begin seeking protection of their personal information in the online forum. Therefore, it is an important endeavor to compare current legal systems and consider where these systems fall short in protecting users' personal information.[97]

B. Chinese Cybersecurity and Privacy Law

The NIL requires Chinese telecommunications operators to provide Chinese government officials with technology and services; it has been deemed a serious threat to the privacy of data for non-residents of China because their personal data is more susceptible to Chinese government oversight.[98] As China began installing 5G communication networks overseas, this threat was addressed by certain American-aligned nations removing such equipment to avoid entanglements with the NIL.[99] In 2019, the United States banned Huawei from the U.S. communication network and all Huawei-made networking equipment from being used in America because the company posed a threat to national security.[100] It did so because it threatened the integrity of American communications networks due to the company's connection to the Chinese government and its adherence to the NIL.[101] Huawei was banned from the United Kingdom on July 14, 2020, and later banned from India in August 2020 for the similar reasons.[102] Huawei-manufactured equipment already installed in the United Kingdom is to be removed by 2027, which will provide the United

---

95 *Id.* at 1002 ("[E]xisting legislation aimed at protecting privacy generally is ineffective when new technologies emerge . . . . [A]s information and surveillance technologies continue to develop more rapidly and are used for a greater variety of purposes, these technologies increasingly will outpace the laws that legislatures have designed to regulate their use.").

96 *Id.* at 977.

97 *See id.* at 1001.

98 Lowell, *supra* note 12, at 97.

99 *Id.* (highlighting India's and the United Kingdom's removal of Huawei's 5G infrastructure equipment from each country's respective 5G networks).

100 *Id.* (detailing the reasons for which Huawei was banned in the United States, the driving factor of which is its threat to national security and the threat to the nation's communications networks' integrity).

101 *Id.* ("In June 2020, the FCC's Public Safety and Homeland Security Bureau designated 'Huawei and ZTE as posing national security threats to the integrity of communications networks.'").

102 *Id.* (discussing the removal of Huawei equipment from India's and the United Kingdom's 5G infrastructure networks).

Kingdom with greater security in removing privacy vulnerabilities it would otherwise have due to the NIL.[103]

The situations in which information must remain in China is outlined in the second draft of Article 7 of the NIL's Draft Measures.[104] Article 7 requires personal information to remain within China when: (1) there are more than 500,000 individuals from China involved in the company's harvested data; (2) the information includes data related to chemical biology, healthcare, military, national defense nuclear facilities, or the population of China; (3) large scale engineering activity data, marine environment, or sensitive geographical information; (4) data related to system vulnerabilities and security protection measures; and (5) any other factor relating to data that may potentially affect China's national security and public interest in any way and for any reason.[105] A network operator must obtain consent from the party involved in the subject of the personal information before said personal information can be transferred outside of China.[106]

Due to the NIL's expansive categories of information that must remain in China, there are narrow exceptions in which data would *not* need to be stored within China.[107] One example is where a network operator that is located in China provides products and services only to foreign entities and not individuals residing in China.[108] This network operator would never involve personal information of any Chinese citizen in their business or involve data that would fall within the vague concept of important data in the process of its operations.[109] These narrow situations in which user data is allowed to be stored in non-Chinese based entities illustrate China's effective protection of user information from foreign entities.[110] However, the NIL's shortcomings arise in that it

---

103 *Id.* (detailing how the United Kingdom ordered the removal of Huawei 5G infrastructure that was already installed to be removed by 2027).

104 Sara Xia, *China Data Protection Regulations (CDPR)*, CHINA L. BLOG (May 20, 2018), https://www.chinalawblog.com/2018/05/china-data-protection-regulations-cdpr.html (detailing the requirements for whether a company which collects personal information within China must store that information in China and outlining the requirements under the second draft of Article 7 of the National Intelligence Law's Draft Measures).

105 *See id.* (providing a detailed list of the requirements for which data gathered within China must remain within China).

106 *Id.*

107 *See id.* ("But a network operator located in China that provides only products or services to foreign entities and whose operation does not involve any personal information of Chinese citizens or important data will not be considered to be a domestic operation and therefore will not be subject to China's cross-border data transfer rules.").

108 *Id.*

109 *See id.*

110 *See generally id.* (discussing how draft Guidelines for Cross-Border Transfer Security Assessment applies both Chinese and foreign entities that supply products and services to

provides no protection against domestic businesses and governments seeking to abuse such personal information.[111]

C. Cybersecurity and Privacy Law Within the European Union

The GDPR is the European Union's second iteration of regional laws governing data protection and user privacy.[112] The GDPR protects users' names, addresses, racial data, cultural data, IP addresses, health data, and other personal information stored across the world rather than just within European Union member states.[113] The second iteration of the GDPR – replacing its outdated predecessor – gives the political and economic union a unique chance to compare how the laws worked in the first iteration to best further the goal of providing adequate data protection and privacy.[114] However, the GDPR does not guarantee absolute protection against data processing.[115] Some examples as means for permissible data processing include user consent, legal obligations for processing the data, substantial public interest, and the protection of vital interests of a person.[116] Nevertheless, some types of personal data may receive heightened protection requiring specific measures to be met before the data can be processed.[117] These measures include explicit user consent for such disclosure, substantial public interest for the data to remain private, and protection of a person who cannot legally give explicit consent for the information to be processed.[118] The GDPR provides citizens of European Union member states a strong baseline for internet privacy protection that member states can expand upon further, even if such protections are not absolute.[119]

The Charter of Fundamental Rights of the European Union (the "Charter")

Chinese consumers and restrict them from transmitting user data outside the country).

111 *See generally id.*

112 Palmieri III, *supra* note 22.

113 *Id.* at 309 ("[T]he GDPR protects names, addresses, racial data, cultural data, IP addresses, health data, and a plethora of other personal information, not just within EU Member States, but across the globe.").

114 *Id.* at 306 (providing the benefits of entering the second iteration of the GDPR, thereby providing the European Union the unique opportunity of determining the first version's flaws).

115 *See id.* at 309.

116 *Id.* ("Although the GDPR lists consent as one possible means for permissible data processing, other permissible purposes for processing include: other legal obligations, the public interest, and protection of a natural persons' vital interests.").

117 *Id.*

118 *Id.*

119 *Id.* at 309–10 ("However, it is important to remember that the GDPR is meant to set a baseline level of data protection, with individual Member States required to implement their own laws in accordance with the GDPR.").

also includes articles that discuss privacy and data protection.[120] The Charter outlines fifty-four different fundamental rights, freedoms, and principles that the European Union recognizes, and the Charter is legally binding in every European Union member state.[121] Article 7 of the Charter recognizes general privacy protection.[122] Article 8 of the Charter recognizes the right to protection of personal data.[123] These articles provide necessary protection for the member states' citizens because personal data that may not be protected otherwise by the governing bodies of the member states is thereby protected by the articles encompassed in the Charter.[124] Ultimately, these two articles of the Charter grant citizens of European Union member states significant privacy rights for their personal data.[125]

Although the GDPR and the Charter are useful protections, they are not without their weaknesses.[126] A scholar has pointed out that the GDPR's major weakness is its lack of enforcement power.[127] The GDPR is unlikely to curtail large scale government surveillance due to inadequate enforcement and the significant competing interests of law enforcement and national security.[128] Thus, interests in law enforcement and national security weaken the GDPR.[129]

The tradeoff between protection of individual privacy data and interests in law enforcement and national security is highlighted in an agreement between the United States and the European Union, wherein privacy was sacrificed for national security.[130] In 2017, the United States and the European Union entered into an agreement called the E.U.-U.S. Privacy Shield, which allowed companies to freely transfer user data from Europe to the United States.[131] The European Union's adoption of the agreement can be viewed as an endorsement of surveillance schemes present in the United States, like the *Carnivore* system, which the Federal Bureau of Investigation (FBI) uses to monitor dangerous

---

120 Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 373 (2019) (discussing the portions of the Charter that recognizes privacy and data protection as essential rights to all Europeans).

121 *See generally* Charter of Fundamental Rights of the European Union, *supra* note 24.

122 *Id.* at 397.

123 *Id.*

124 *See* Rustad & Koenig, *supra* note 120.

125 *Id.*

126 *See generally* Colbary, *supra* note 25.

127 *Id.*

128 *Id.*

129 *Id.*

130 *Id.* (discussing how the European Union was willing to sacrifice individual privacy for the compelling interest of law enforcement and national security).

131 *Id.* (discussing the E.U.-U.S. Privacy Shield, which indicates that the European Union's member states may begin establishing similar surveillance schemes as those that appear in the United States, all while avoiding breaching the rules set forth in the GDPR).

individuals.[132] The E.U.-U.S. Privacy Shield does not directly pertain to national security or law enforcement but instead allows the transference of data between the jurisdictions freely, disregarding individual privacy.[133] Under the agreement, only American citizens or non-citizens within U.S.' borders are afforded the protections guaranteed in the United States Constitution.[134] The Constitution does not, therefore, prohibit unreasonable searches and seizures or impose a warrant requirement to prevent such searches and seizures against non-American individuals outside the United States.[135] This agreement provides an indication to individual member states that each European Union member state may also establish similar surveillance programs – like those in the United States – while still conforming to the standards established in the GDPR.[136]

Although the European Union enacted the GDPR to bolster internet privacy, member states in the European Union have also built their own mass surveillance programs, which the European Union courts said were legal.[137] The European Court of Human Rights (ECHR) is an international court that interprets human rights, and it began reviewing certain legislation authorizing bulk interception of foreign communication and mass surveillance.[138] In 2018, the ECHR directly addressed foreign mass surveillance and upheld Swedish legislation that authorized the gathering of covert bulk signals intelligence, which is favorable

---

132 *Id.*; *see also* Judson Jennings, *Carnivore: US Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH.10, ¶¶ 33–35 (2001) (discussing the Carnivore system often used by the FBI for surveillance and quoting an FBI agent's interrogation with Congress about the system); *see also infra* notes 155–59 and accompanying text.

133 Colbary, *supra* note 25 ("Though the E.U.-U.S. Privacy Shield does not directly implicate national security or law enforcement – it allows providers to transfer data freely between the two jurisdictions . . . .").

134 Letter from Maria McFarland Sanchez-Moreno, Co-Dir., U.S. Program, Hum. Rts. Watch, & Iverna McGowan, Head of Eur. Insts. Off. & Advoc. Dir., Amnesty Int'l, to Věra Jourová, Comm'r for Just., Consumers & Gender Equal. Eur. Comm'n (July 26, 2017) (on file with Human Rights Watch) (providing that people in the European Union who are not United States persons will not garner the benefit of the constitutional provisions that are available to United States persons).

135 *Id.*

136 Colbary, *supra* note 25 (showing that even though the agreement does not provide for an explicit surveillance scheme to assist in national security or law enforcement, the E.U.-U.S. Privacy Shield "indicates that the E.U., or at least [its] individual member states, may establish similar programs without running afoul of the GDPR.").

137 *Id.* at 229 ("While the European Union was enacting the GDPR and E.U. Courts were deciding cases like Google v. Spain, member states of the E.U. were also building their own mass surveillance programs which were, in turn, legitimized by E.U. courts.").

138 *See* Asaf Lubin, *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights*, JUST SEC. (Aug. 2, 2018), https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/ (discussing the legitimization of foreign mass surveillance–namely American–occurring and broadening in the European Union and the European Court of Human Rights' decisions regarding these encroachment on European privacy rights).

to the government.[139] Sweden enacted the Signals Intelligence Act in 2009 and established that inter-border communications are transferred, collected, and then inspected by the Swedish government body responsible for state security – the Defense Radio Establishment.[140] Thus, not only have government-implemented mass surveillance systems become widespread in Europe, but the court tasked with protecting human rights and providing privacy and security from surveillance systems legitimized them, further narrowing European privacy rights.[141] The GDPR bolstered privacy rights in European Union member states, while still allowing those same member states to limit privacy rights by enacting stronger surveillance systems and national security measures.[142]

D. American Internet Privacy Laws and Regulations

The United States provides privacy protections to Americans but only in restricted instances and through a myriad of narrowly tailored laws.[143] Some acts, such as the ECPA and the FCRA, protect types of specified personal data obtained through ongoing communication while also limiting who gets to view such data after the communication's conclusion.[144] Comparatively, rather than protecting an individual's health data absolutely, HIPAA only protects communications between healthcare patients and medical businesses, such as

---

139 *See id.* (citing Centrum För Rättvisa v. Sweden, App. No. 35252/08, ¶1 (June 19, 2018), https://www.statewatch.org/media/documents/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf).

140 *See* Lubin, *supra* note 138 ("The case was initially brought in 2008 after the Swedish parliament extended the powers of the Defense Radio Establishment (Försvarets radioanstalt, or FRA), Sweden's primary SIGINT [(Signals Intelligence)] agency, to allow the bulk interception of communications and communications data running through cables.").

141 *See id.*

142 *See id.*; *see also* Colbary, *supra* note 25, at 229 (discussing the legitimization of mass surveillance programs by European Union courts).

143 *See Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL AND PREVENTION (Jun. 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html; *Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (last visited Nov. 20, 2022).

144 *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–23 (Westlaw though Pub. L. 117–166) (restricting the government from wiretapping telephone calls and restricting employers from monitoring employee communications, while not protecting against modern internet surveillance tactics concerning data stored on servers, in the cloud, or in internet search databases); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012) (limiting those who can view an individual's credit report and how such information is obtained).

doctors, insurers, and hospitals.[145] COPPA, a more modern privacy law centered on the Internet, limits a company's collection of personal data for internet users who are under thirteen (13) years of age.[146] However, some privacy laws may be outdated and offer no modern practical privacy protections to Americans, like the VPPA, which only prevents the disclosure of VHS rental records.[147] Other privacy laws may give specified and qualified groups access to private information with the consent of the information owner, like the Family Educational Rights and Privacy Act (FERPA), which gives parents, students, and other schools the right to inspect education records maintained by the school with the consent of the student.[148] Other acts, such as the Gramm-Leach-Bliley Act (GLBA), require the disclosure of data usage to the consumer before consumption.[149]

However, in the case of the GLBA, there is no restriction on how the companies use the collected data, so long as the companies disclose such usage beforehand to the consumer.[150] Some states have privacy protection laws as well, such as the California Consumer Privacy Act of 2018 (CCPA), which grants consumers the right to delete personal information collected from them by businesses and the right to opt-out of the sale of their personal information.[151] The United States Constitution also provides protections via the Fourth Amendment, which protects individuals from unreasonable searches and seizures by government officials.[152] However, these rights are juxtaposed against national security and safety interests such as those interests raised in the

---

145 CTRS. FOR DISEASE CONTROL AND PREVENTION, *supra* note 143 (detailing that "[t]he Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge").

146 FED. TRADE COMM'N, *supra* note 143 ("COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.").

147 Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) (1988) (protecting against the disclosure of consumers' video tape rental and sales records by video tape service providers).

148 *See generally* Family Educational Rights and Privacy Act Regulations (FERPA), CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/phlp/publications/topic/ferpa.html (last visited Feb. 25, 2022) (illustrating how the act requires consent by eligible individuals for the inspection of education records maintained by a school).

149 Gramm-Leach-Bliley Act, 15 U.S.C. §6802(b) (requiring consumer financial products to explain their data sharing practices, while also providing the consumer's right to opt out).

150 *Id.* §6802(a).

151 *See generally* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100 – 1798.199.100 (Deering 2018) (outlining the protections granted to consumers where businesses seek to collect and sell consumers' personal information).

152 U.S. CONST. amend. IV.

Patriot Act and the Carnivore system, which push the boundaries of privacy protections.[153]

In pursuit of ensuring public safety and thwarting terrorism in the 1990s, the FBI developed a surveillance system called *Carnivore*.[154] Carnivore is an FBI designed computer surveillance program that sorts through contents of a suspected terrorist or person of interest's e-mails and other wireless messages and determines whether the candidate should be reviewed further by FBI personnel.[155] The Wall Street Journal exposed the program to the general public in July 2000.[156] The FBI faced public backlash and opposition to its usage and expansion of Carnivore in July of 2001, even when it announced the goal of the expansion was to curb crime.[157] The public tune changed, however, following the September 11, 2001 terrorist attacks when the FBI determined that Osama bin Laden succeeded in the terrorist plot using wireless technology and the internet in the forms of encrypted emails and steganography.[158] This discovery "prompted Congress to implement new legislation" to regulate electronic communication and combat cybercrime shrinking user privacy in the process.[159]

The Patriot Act was such an act passed following the terrorist attacks on September 11, 2001.[160] The Patriot Act gives law enforcement agencies, namely the FBI, broad power to investigate, counter, and prosecute domestic or

---

153 USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272, 278; *see also* Jennings, *supra* note 132, at ¶¶ 33–35 (discussing the FBI's use of the Carnivore system, which the FBI often utilizes for surveillance purposes, and quoting Congress's interrogation of an FBI agent about the system).

154 Jennings, *supra* note 132, ¶ 6 ("According to a prominent member of the computer security industry, the FBI claims to have used Carnivore in approximately twenty-five investigations prior to August, 2000; the majority of the cases are said to have involved counter terrorism . . .").

155 Stephen W. Tountas, *Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?*, 11 WASH. U. J.L. & POL'Y 351, 351–52 (2003) ("The FBI designed Carnivore to sift through the contents of a suspect's e-mail and, when appropriate, to record the suspect's e-mail address for further review. In response to privacy concerns, the FBI pointed to the rise in cybercrime as a national security threat justifying the use of programs such as Carnivore. In July of 2001, despite much criticism, the FBI announced its goal to further curtail crime by expanding Carnivore's capabilities to include the monitoring of both incoming and outgoing wireless messages.").

156 *Id.* at 351.

157 *Id.* at 351–52.

158 *Id.* at 352.

159 *Id.*

160 *See* USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (showing that the Patriot Act was enacted by the Senate and the House of Representatives of the United States of America on October 26, 2001, "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.").

international suspicious activity that may relate to terrorism.[161] The Patriot Act also gives law enforcement agencies authority to intercept communications believed to be related to terrorism across all wire, oral, and electronic mediums.[162] Advocates of the Patriot Act point to the benefits of swift response to suspicious activities, stronger terrorism prevention, and an increase in accuracy for locating potential threats to national security.[163]

However, opponents of the Patriot Act argue that the Act allows law enforcement agencies to investigate anyone the agencies see fit, thus overrunning a citizen's right to privacy in the name of safety.[164] Thus, there is a tension between the Patriot Act's benefits and drawbacks in achieving its goal of preventing terrorism and ensuring the safety of the American people.[165] Congress's further enactment of the Patriot Act, coupled with the justification of the Carnivore technology, demonstrates its focus on national security interests, even if that diminishes individual privacy rights and security of personal information.[166] Looking forward, 5G technology's expansion will provide the government more power in its surveillance of individuals, as the flow of information and ability to tap into user information will only grow.[167]

The United States does not currently have any laws in place protecting citizens' personal data when it is transferred abroad.[168] Unlike China, where personal data is kept within the country, a transfer of American personal data outside of the country can occur without any storer or maintainer of personal data being notified.[169] Critics argue that this potential for breach becomes even

---

161 *See id.* at 276 (illustrating that the United States Treasury is to "reimburse any Department of Justice component for any costs incurred in connection with . . . providing support to counter, investigate, or prosecute domestic or international terrorism . . . .").

162 *See id.* at 278 (granting the FBI "authority to intercept wire, oral, and electronic communications relating to terrorism.").

163 *See* James Chen, *USA Patriot Act*, INVESTOPEDIA (Oct. 31, 2021), https://www.investopedia.com/terms/p/patriotact.asp (stating that advocates feel "the Act has made anti-terrorism efforts more streamlined, efficient, and effective" and that federal agents use roving wiretaps while tracking international terrorists trained to avoid surveillance by rapidly changing locations and communication devices).

164 *See id.*

165 *See id.*

166 *See* Tountas, *supra* note 155, at 374 ("Whereas it might once have seemed improbable for Carnivore to regulate wireless technology, the Patriot Act all but implemented the necessary changes for an expeditious transition. Although questions remain as to whether wireless regulation is a sensible solution, Congress's enactment of the Patriot Act clearly demonstrates its view that the security of the United States must come before the security of personal information.").

167 *See id.*

168 *See* Michael T. Hubbard, *Personal Data of U.S. Citizens Transferred Abroad Needs Protection*, 11 NAT'L L. REV. 308, 308 (2019) (discussing how there are currently little to no restrictions on the transfer of American personal data to outside of the country).

169 *Id.*

riskier as the world becomes more interconnected with 5G technology and the advent of more advanced technology such as newer telecommunication devices and autonomous vehicles.[170] American businesses use savvy lawyers to try to mitigate information breach risks by prohibiting the transfer of key data outside of the country.[171] These lawyers impose view-only access on data abroad and try to limit the disclosure of consumers' personal information to reliable democracies.[172] However, proponents of stronger personal data privacy laws argue that the mitigation barriers preventing data breaches do not provide necessary comprehensive protection.[173] Furthermore, the United States Constitution provides no explicit provision ensuring the right to privacy, with the exception of the Fourth Amendment and its relation to protection against unreasonable searches and seizures by the government.[174] If there is a lack of attention to American citizens' personal data storage and transmission foreign governments will have unfettered access to Americans' personal data stored abroad.[175]

III. POTENTIAL SOLUTIONS FOR USER PRIVACY FOR 5G AND BEYOND

The debate around privacy, especially with the advent of 5G, is a debate about modern freedoms, which must precariously balances the weights of freedom, safety, and government power.[176] The United States provides vast economic freedoms, so the creation of a comprehensive internet privacy law from scratch would be no simple task.[177] Instead, a better approach is to realize the best features of other countries' data privacy laws and apply them to the American situation through a refined legal amalgamation of sorts, while still adhering to the current American climate on counterterrorism efforts.[178] This merger of laws will provide a more robust system of privacy protection for American citizens and help navigate the challenges that come with 5G and future technologies,

---

170 *Id.*

171 *Id.* ("The U.S. does not likewise protect the personal data of its citizens outside of its borders. To mitigate such risks, savvy U.S. lawyers do often prohibit the transfer of key data outside of the country.").

172 *Id.* (illustrating that U.S. lawyers "impose view-only access abroad, or limit the disclosure of sensitive data to reliable democracies").

173 *Id.*

174 *See* Tammy Katsabian, *Employees' Privacy in the Internet Age Towards a New Procedural Approach*, 40 BERKELEY J. EMP. & LAB. L. 203, 239 (2019) (emphasizing the lack privacy protections for Americans by the government from the government).

175 Hubbard, *supra* note 168, at 308.

176 PRIV. INT'L, *supra* note 19.

177 *See generally* USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272.

178 *See supra* notes 12, 22, 120, 143–54 and accompanying text.

while still ensuring the American government has enough power to thwart terrorist endeavors.[179]

A. The Desirable Takeaways from China's NIL

American citizens would benefit from broad protections of their personal data through focused requirements on personal information, like those provided by the NIL, so that their data remains within the territory of the United States and protected from foreign entities.[180] Similarly, citizens' personal information is retained within China's borders, and the Chinese government can ensure that its citizens' personal data is not left vulnerable to foreign infringement and misuse.[181] Because of 5G's high upload and download speeds for accurate location tracking and transference of other information, the government has unlimited data on, not only Chinese citizens, but anyone who falls under the limits imposed by the NIL.[182] Furthermore, the NIL benefits Chinese citizens in that any personal information requested by a foreign entity must first receive permission from the subject in question before the personal information's dissemination.[183] The NIL's provisions provide substantial protection for Chinese citizens' personal data from foreign entities; implementing such protections into American privacy law may reap similar benefits.[184]

The NIL provisions protect citizens from foreign entities that try to acquire personal data.[185] The NIL requires Chinese telecommunications services to provide Chinese intelligence services with access to such technology, including the personal data stored in these systems.[186] Huawei often provides these systems to other countries.[187] Because the data is stored by a Chinese company, it is stored within China, giving the government access to it.[188] Alongside the

---

179 *See* Lowell, *supra* note 12, at 76.

180 *See* Xia, *supra* note 104.

181 *Id.*

182 *See* Linebaugh, *supra* note 33, at 1; *See* Xia, *supra* note 104 (listing the relevant circumstances in which data must remain within the borders of the People's Republic of China as outlined under Article 7 of the second draft of the Draft Measures compiled in the NIL, including the required consent necessary from the subject in question pertaining the personal information being transferred outside of China's borders).

183 *See* Xia, *supra* note 104 ("To transfer personal information outside China, a network operator must first obtain consent from the subject of the personal information. This consent must either be in writing or by some other sort of affirmative action by the subject of the data.").

184 *See id.*

185 *See* Lowell, *supra* note 12, at 96.

186 *See id.*

187 *See id.*

188 HOEHN & SAYLER, *supra* note 35 ("Some analysts interpret this law as requiring Chinese companies to cooperate with intelligence services, including compelling installation

far-reaching powers of the NIL, this system thereby grants the Chinese government the same unfettered access to individuals' personal data that it seeks to protect against from foreign entities raising privacy concerns.[189] Coupling this government overreach of personal data privacy with increasingly advanced 5G speed and near real-time location tracking runs counter to the goals of internet privacy.[190] These infringements of personal privacy give too much power to the central government's monitoring ability and, if implemented in America, may appear counterintuitive to the perception of freedom and will come across as overbearing.[191] Therefore, the United States should not mirror this authoritarian structure used in China.[192]

The Chinese model for internet privacy rights of personal information would not fit well onto an American model due to the autonomy and separation American businesses enjoy compared to the dominance the Chinese government exerts on its businesses.[193] China has an authoritarian structure that provides access to any Chinese business headquartered in China, similar to the relationship between China and Huawei.[194] Because Huawei is a major Chinese telecommunications company, and the Chinese government has expressed interests favoring national security over privacy rights of personal information, the Chinese system of governance in the form of the NIL would adversely affect the personal information privacy interests of Americans.[195] The NIL erodes any form of privacy protection that internet users under Chinese corporations would possess because it gives the government direct access to all the information gathered by China's heavily government-influenced businesses.[196] Therefore, a direct implementation of the entire NIL would be adverse to American interests so long as the American government heavily influences American businesses as

---

of backdoors to provide private data to the government.").

189 *See id.*

190 *See id.*

191 *See* Lowell, *supra* note 12, at 96 (showing how a company owned entirely by the state could endanger national security of other countries when its government prompts it to relinquish access of private user data to the government).

192 *Id.*

193 *See id.* at 99 ("Once China has access to new technology, it can copy it, hack it, or leave bugs behind to find breaches in its security. There is no specific law protecting the privacy of American citizens from foreign intelligence for wearable technology. Additionally, foreign governments, like China, have laws where they can access any Chinese business.").

194 *See id.*

195 *See id.* ("China's plan for domination can be exemplified through Huawei, one of China's most significant threats to the U.S. Huawei is a major Chinese telecommunications company. Huawei and other Chinese companies are under the control of the Chinese government.").

196 *See id.*

the Chinese government influences Chinese companies.[197] However, American businesses have greater autonomy from the American government in relation to their Chinese counterparts, so the American legislature could tailor the NIL to best fit the personal information privacy protection needs of its citizens.[198]

In implementing a system with similarities to the NIL in America, critics will argue that the drawbacks of increased government surveillance outweigh the security gained from protecting citizens' personal information.[199] However, these concerns can be addressed by amending and tailoring the law to best fit the needs of the government and its citizens.[200] Since the goals of the Chinese government in implementing such a law are to further China's sphere of influence and create adversary vulnerabilities, the Chinese government's prerogative is to give greater surveillance strength to the central government regardless of its own citizens' lack of privacy.[201] In contrast, the goals of the American plan for its citizens should be in favor of protecting its citizens' interests in privacy protection for personal data, compared to the sacrifice of all citizen privacy to government overreach as found in China.[202] An American privacy law could instead keep two parts of the NIL: (1) requiring citizens' personal data to remain within American territory, and (2) requiring the citizen's consent before disseminating personal data.[203] Cherry-picking useful parts of the NIL can accurately address concerns regarding an increase in government overreach and control while still maintaining user privacy interests.[204]

B. Improving a Plan with the Laws of the European Union

Another example of data privacy protections that the United States can use comes from the European Union's GDPR.[205] The GDPR protects personal

---

197 *See id.*

198 *See id.* at 108 ("In the race to 5G, the U.S. needs aggressive laws to protect its control of technology over foreign countries.").

199 *See* HOEHN & SAYLER, *supra* note 35.

200 Xia, *supra* note 104.

201 HOEHN & SAYLER, *supra* note 35 ("Some experts are concerned that vulnerabilities in Chinese equipment could be used to conduct cyberattacks or military/industrial espionage . . . However, they note that vulnerabilities could also be intentionally introduced for malicious purposes.").

202 *Id.*

203 Xia, *supra* note 104 (illustrating that the NIL requires the storage of "personal information and important data collected and generated within the territory of the PRC" and that, in order to "transfer personal information outside China, a network operator must first obtain consent from the subject of the personal information.").

204 *Id.*

205 *See* Palmieri III, *supra* note 22; *see also* Charter, *supra* note 24, at Art. 7–8 (granting all Europeans in European Union member states "the right to respect for his or her private and family life, home and communications," recognizing that "[e]veryone has the right to

information pertaining to a vast number of categories, and the Charter recognizes many fundamental rights, freedoms, and principles, including general privacy protection and protection of personal information, for citizens of European Union member states.[206] The intent of these two proclamations is to grant broader privacy protections to citizens of European Union member states, especially in the digital realm.[207] However, the GDPR still faces weaknesses in its enforcement mechanisms.[208] Large-scale government surveillance and under-enforcement of the GDPR's protections greatly weaken its strength.[209] The problem of large-scale government surveillance was exacerbated by the introduction of the E.U.-U.S. Privacy Shield, which allowed personal data of citizens of European Union member states to be freely transferred throughout the United States.[210] Although the GDPR and the Charter set out to protect personal data in the digital realm, the lack of enforcement and the introduction of large-scale government surveillance via American counterterrorism strategies cripple the laws' effectiveness.[211]

The European Union lacks the necessary centralized decision making due to its complex, and oftentimes conflicting, collection of member states' independent national parliaments.[212] This improper enforcement can be largely blamed on the decentralized aspect of the European Union.[213] In order for swift implementation of policies and continued protection of rights to occur, greater centralized decision making must be present.[214] Therefore, because the European Union lacks necessary centralized decision making and authority, its policies, like the GDPR and the Charter, are limited and fail to provide the protections that each provides.[215]

Critics will be quick to point out that supplanting the digital privacy protection portions of the GDPR and the Charter in the American legal system would echo the problems with under-enforcement and government surveillance that the

---

the protection of personal data concerning him or her," and discerning that personal "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified").

206 *See* Palmieri III, *supra* note 22, at 306; *see also* Charter, *supra* note 24, Art. 7–8.

207 *See* Palmieri III, *supra* note 22, at 306; *see also* Charter, *supra* note 24, Art. 7–8.

208 Colbary, *supra* note 25 (discussing that although the GDPR may do good in protecting the privacy of individuals it is unlikely to be able to curtail large government surveillance because of competing interests of law enforcement and national security).

209 *Id.*

210 *See id.*

211 *See id.*

212 Smith, *supra* note 25, at 9–10.

213 *Id.* at 9.

214 *Id.*

215 *See id.*

European Union faces since the United States enforces large scale counterterrorism surveillance.[216] However, the difference between the United States and the European Union lies in each entity's governing structure and how each can properly enforce legislation like the GDPR.[217] Whereas the United States can enforce legislation like the Patriot Act and compel other legal entities like the European Union to adopt similar counterterrorism measures, the European Union falls short of such inter-member enforcement and external diplomatic negotiations.[218] The European Union is often viewed by critics as a decentralized collection of member states that need to enter into agreements, such as the E.U.-U.S. Privacy Shield, to avoid severing ties with its stronger ally.[219] The privacy protections guaranteed in the GDPR and the Charter would be easier for the United States to enforce since they have proved to be centralized enough to enforce the Patriot Act and counterterrorism surveillance measures upon foreign political entities.[220] Furthermore, the United States, in adopting parts of the GDPR and the Charter from the European Union, alongside parts of the NIL from China, can provide privacy carve-outs for its citizens from its own counterterrorism surveillance measures.[221]

The American legislature should pass a law establishing personal data privacy rights for its citizens.[222] This law could echo the protections guaranteed by the GDPR and the Charter, and the American court system can vindicate such rights if violated.[223] These stronger court protections for passed legislation present in America would allow actual execution of personal data privacy rights unlike those that are trampled by surveillance measures in the European Union.[224]

C. Reconciling Current American Laws

Already existing laws in the United States have laid the groundwork for personal information privacy protection, but lawmakers should incorporate these existing laws into a more comprehensive privacy protection law.[225] Encouraging

---

216 *See id.*; *see also* Jennings, *supra* note 132, ¶¶ 33–35.

217 *See* Colbary, *supra* note 25, at 228 ("As discussed above, there are a number of reasons that the GDPR may be under enforced by member states.").

218 *See id.*

219 *Id.* at 229.

220 *Id.* at 228.

221 *Id.*

222 *See* Palmieri III, *supra* 22, at 306 (outlining the GDPR and the personal data privacy rights provided therein).

223 *See id.*; Rustad & Koenig, *supra* note 120.

224 *See* Colbary, *supra* note 25.

225 *See* Brotman, *supra* note 10 ("On the equipment side, a more defined U.S. regulatory role by the FCC could help reinforce consumer privacy protection that is offered for 5G services in the competitive marketplace. This might take the form of requiring that all 5G

rigorous privacy standards in the process of using 5G technology in business could benefit the competitive marketplace in the United States and can further enhance protections adopted from the NIL, the GDPR, and the Charter.[226] The United States has a number of niche privacy protection provisions that its legislators could incorporate in new privacy protection laws in their application to portions of the NIL, GDPR, and the Charter.[227] The Federal Communications Commission (FCC) could implement such privacy standards that would enhance consumer privacy protection in 5G hardware production.[228] The FCC should require 5G carriers to purchase 5G networking equipment and equip 5G cellular towers that are properly equipped with technical capabilities that enhance consumer privacy protection on the provided networks.[229] This enhanced consumer privacy protection would force countries that supply the equipment, such as China, to conform to an American model of 5G consumer protection.[230] FCC regulation on 5G equipment for privacy protection would adequately address any underlying concerns with foreign hardware.[231] Such hardware would be guaranteed to meet U.S. standards, which would in turn create a 5G consumer privacy protection worldwide standard and ensure that 5G technology and equipment is unlikely to be hacked or provide a backdoor entry for governments like China.[232]

Threats to privacy and personal data do not only come in the form of foreign entities and domestic business, but such threats to citizens' digital privacy may also arise from the American government itself.[233] Enacting a requirement that the FBI obtain a warrant before being able to surveil an individual's personal data from private companies rather than having free reign in investigative pursuits would help mitigate potential government threats to privacy where citizens are using 5G technology.[234] Many opponents of the Patriot Act find that the Act grants the government too broad of power allowing government counterterrorism agencies, like the FBI, to investigate anyone the agencies see

---

carriers certify to the FCC that the 5G networking equipment they are purchasing is embedded with a set of technical capabilities that will allow the carriers to offer enhanced consumer privacy protection on their 5G networks.").

226 *See id.*

227 *See supra* notes 12,19, 22, 120 and accompanying text.

228 Brotman, *supra* note 10.

229 *Id.*

230 *Id.*

231 *See id.* (emphasizing that the establishment of FCC regulations surrounding 5G hardware would properly "[a]ddress the ongoing U.S. national security concerns regarding foreign hardware provisioning and also help the U.S. create a de facto worldwide standard for 5G consumer privacy protection.").

232 *Id.*

233 USA Patriot Act of 2001, Pub. L. No. 107–56, §§ 201–02, 115 Stat. 278.

234 *See generally* Chen, *supra* note 163.

fit.[235] In these endeavors, the FBI has imprisoned suspected terrorists at Guantanamo Bay without proper legal representation or even an explanation as to why the individuals were arrested violating these prisoners' due process.[236] A terrorist threat should not be taken lightly, and swift action should be executed to minimize a potential loss of human life.[237] Some individuals have even been found to lack ties to terrorism.[238] To balance freedom of digital privacy with safety, some counterterrorism surveillance initiatives must be taken, which could be taken from the Patriot Act – just not to the level of surveillance that was taken under the Patriot Act, like the bulk collection of phone records.[239] However, the inclusion of the CCPA, or the required consent provision of the NIL, would declaw much of the Patriot Act in its pursuit to remove digital privacy and the protection of personal information.[240] The Patriot Act could still be enforced to ensure that proper counterterrorism measures are taken, but instead of unfettered access to every citizens' personal data, the FBI investigation of suspected terrorists could be more constrained from its height following the September 11, 2001 terrorist attacks.[241]

D. Why New User Information Laws Matter

Creating a stronger privacy law framework in the digital realm is important because 5G technology and other future technologies will continue to change user information landscape.[242] 5G provides the ability to upload and download massive quantities of information instantly, as well as provide instant and accurate location updates in cases of wearable technologies.[243] With 5G technology being so powerful, whoever controls the market for its implementation, and the collection of its data, will set the standard for laws surrounding it.[244] China is the main competitor for American dominance in the

---

235 *Id.* (asserting that opponents of the Patriot Act argue it effectively lets the U.S. government investigate anyone it sees fit).

236 *Id.* ("Suspected terrorists have been imprisoned at Guantanamo Bay, Cuba, and other sites with delayed due process.").

237 *See generally id.*

238 *Id.*

239 *See generally id.*

240 California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100 (Deering 2018); *see also* Lowell, *supra* note 12, at 96, 99.

241 *See generally* Chen, *supra* note 163 (showing the advantages and disadvantages of the Patriot Act and the act's practical implications if left unchecked).

242 *See* Lowell, *supra* note 12, at 75 (showing that "[W]hile the broad introduction of wearable 5G technologies may revolutionize daily life, the amount of personal data they collect is immense, and the potential for national security risks is even more significant.").

243 *Id.*

244 *See id.* at 101 (illustrating "the U.S.'s race to control the 5G market and to control the data acquired from wearable technology" because "[W]hoever wins the race will set the

realm of 5G technology, and China has outpaced American efforts to implement 5G and reap the technology's benefits.[245] Moreover, China has also created the NIL, which can provide the Chinese government backdoor access to American citizens' personal data.[246] Therefore, since the United States is lagging behind Chinese efforts in developing and implementing 5G technology, and China is making efforts to collect individuals' personal data, the United States government should create comprehensive personal data privacy laws to protect American citizens' interests.[247] Furthermore, technology in general will continue to advance, and laying the groundwork for personal data privacy protections now can save time and effort in the future through simple legal updates accounting for advancements in digital technology.[248]

The United States and its allies should look upon the Chinese model, which makes all information that is important to Chinese sovereignty accessible to the Chinese government, with great caution.[249] The Chinese provide strong protection against foreign countries, but that information is subject to nearly unlimited control by the Chinese government.[250] A successfully implemented American policy could take advantage of the protectionist portions of the Chinese plans, but not the government mandate for information provision providing better privacy protection for all digital information collected through the use of 5G technology.[251] Congress could implement portions of China's NIL and the portions of the European Union's GDPR and Charter so as to protect the personal data of Americans, especially from opportunistic and adversarial prying eyes.[252] Implementing a policy through either the FCC or as a comprehensive federal law will set the international standard for such privacy laws before the

---

standard for 5G, which will include the country's technology.").

245 *See generally* Council, *supra* note 42.

246 *See generally id.*; Xia, *supra* note 104.

247 Xia, *supra* note 104.

248 *See* Lowell, *supra* note 12, at 75–76 ("The benefits of 5G technology are vast as system speed is a precursor to innovation. The increase in speed will be felt throughout the world, impacting every part of our lives and our economy. Innovations driven by 5G technology may drive new opportunities for work, higher GDP, and foster even more significant innovation.").

249 *See* Brotman, *supra* note 10 (outlining China's National Intelligence Law, requiring Chinese telecom operators to provide the Chinese government technology and services of user data).

250 *Id.*

251 Xia, *supra* note 104 (discussing China's National Intelligence Law and the policies which businesses must comport with when doing business in China).

252 *See* Hubbard, *supra* note 168 ("Both China and Russia have enacted legislation restricting the transfer of personal data of their citizens outside of their respective countries, and for many years, the European Union has prohibited the transfer of personal data of EU citizens outside of the EU without adequate protection, including appropriate contract terms.").

Chinese government can do so, which will better protect American interests.[253]

IV. CONCLUSION

Protecting personal data of Americans can be a small step in the right direction for a broader and more comprehensive privacy protection plan especially with the rise of 5G technology.[254] Creating an amalgamation of existing privacy law can provide protections that will deter foreign governments and groups from gaining unfettered access to Americans' private and personal data.[255] Increased download and upload speeds alongside instant and accurate location updates in cases of wearable technologies create digital privacy concerns under the technological growth of 5G.[256] Threats to American citizens' privacy, like hackers and national adversaries, can use this speed to download users' personal information and real time location in mere seconds.[257] Because the United States is falling behind in the race to implement 5G technology, the country's best strategy would be to pass laws to protect citizens' personal data privacy from opportunistic threats abroad.[258] The United States should continue to use the Patriot Act to provide the country with an adequate counterterrorism surveillance defense, but it should declaw the act to only allow the FBI to perform surveillance checks against individuals with whom the FBI has issued a warrant against.[259] The battle over 5G technology and personal data has only just begun and – similar to any war effort – the United States will need to innovate to come out ahead.[260] However, the best innovations do not need to be built from scratch, as other countries have provided frameworks upon which American innovation can be built.[261]

---

253 Lowell, *supra* note 12, at 96.

254 *See id.* ("As Congress continues to debate federal privacy legislation, it should (like the EU) require adequate safeguards to protect the personal data of U.S. citizens transferred abroad.").

255 *Contra* Hubbard, *supra* note 168 (discussing the lack of the protection for personal data in the U.S. as compared to foreign countries).

256 Lowell, *supra* note 12, at 75.

257 *See* Bently & Krouse, *supra* note 50 (showcasing the high speed at which a large mobile game can be downloaded to a cellular device, and then further applying that same speed to user personal information).

258 *See* Hubbard, *supra* note 168.

259 *See generally* USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272

260 *See generally* Brotman, *supra* note 10 (noting that the country that leads in 5G technology will set the standard for the rest of the world).

261 *See generally* Lowell, *supra* note 12, at 96 (discussing the NIL and its mechanics in privacy protection); *see also* Palmieri III, *supra* note 22, at 306 (discussing the GDPR and its privacy protections, as well as its drawbacks).