International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
http://ijcjournal.org/

The Health of Privacy Protection in a 5G World

Bukola Abigail Afolabi*

Email: abbukenzo@gmail.com

Abstract

The 5G network is prized for its super speed, low latency, seamless connectivity, and high capacity; and it is believed that just like the 4G era birthed tech giants like Uber and Airbnb, 5G would produce business mammoths that would be unique to its dispensation. While the market drools in anticipation of those newborns, it is important to pan out how privacy protection would fair under 5G. This paper discusses how 5G would impact the ongoing privacy protection struggle. As 5G unwinds and its benefits are enjoyed, there will be too many things happening that may overwhelm average consumers in the United States and create some form of apathy towards privacy protection discussions.

Keywords: 5G; big data; smart cities; privacy protection.

1. Introduction

The fifth generation (5G) network is prized for its super speed, low latency, seamless connectivity, and high capacity that promise to change the landscape of augmented reality, virtual reality, smart campuses, and remote telemedicine, among others [1]. It is believed that just like the 4G era birthed tech giants like Uber and Airbnb, 5G would produce business mammoths that would be unique to its dispensation. While the market drools in anticipation of those newborns, it is important to pan out how privacy protection would fair under 5G. This paper discusses why privacy protection should be prioritized at this stage of rolling out the 5G network.

Anticipating the fate of privacy protection under 5G is necessary at this stage because, one, as noted in a recent study that surveyed 500 U.S. federal government employees, “new cybersecurity risks” and “increased cybersecurity risks” are the two most critical challenges to adopting 5G, after budget concerns. Since the benefits of 5G are available to all, including malicious actors, when an organization integrates 5G, it expands “the attack surface” for cyber threat actors. If privacy policies remain the same, it may mean cyber attackers will have more to gain from data breaches than before.

Two, the research [1] found that 5G would increase data volume capacity of organizations. Business entities will be able to significantly collect, store, and process more data more efficiently than before. This may soon relegate today’s big data to *small data* status. Privacy protection efforts must track this development to ensure data is handled appropriately. There may be need to review data retention policies, for instance.

---

* Corresponding author.

Current policies, whether for the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act, Children's Online Privacy Protection Act, Payment Card Industry Data Security Standard (PCI DSS), or State Privacy Laws, are based on pre 5G technologies. There should be policies that reflect the reality of 5G-native technologies and capabilities as they evolve. Lastly, 5G is still at infancy per adoption by organizations [1]; it will be cheaper to introduce relevant restraints at this stage. It follows therefore that the concern for data privacy protection should receive the same attention cybersecurity receives as organizations are weighing the option of adopting and integrating 5G.

2. Big Data and Privacy Protection

Big data is data or information assets with five 5 V's: volume, velocity, variety, veracity, and value; referring to data size, speed, format, accuracy, and relevance, respectively; and having an economical and progressive way of processing data for insight gleaning and decision making is considered a necessity when talking about big data [2]. Such technology determines how data is sorted and the value you can generate at a competitive rate – the competitiveness is in terms of speed and cost. Value creation from data must be fast and cheap for the technology involved to be market relevant. The explosion in data collection avenues and scope appears to coincide with the realization of how invaluable big data can be to decision making [3,4,2].

Stakeholders in both public and private sectors now see the need to gather as much as possible and glean as much as possible from data. This scramble for all forms of data puts the consumers in an important but vulnerable position. Information about the consumers has become a commodity, the new crude oil, but there are genuine situations that the information could not be held back, because it is crucial to service provision. In such instances, the consumers will have to do some privacy tradeoffs [5] to enjoy the needed service.

No hospital will want to admit an anon patient. More than names and addresses, hospitals need additional information about the patients to treat them and manage their health. Banks must have the records of their customers' transactions. A phone manufacturer like Apple, must be able to track their users' devices, and by extension, the users themselves, to provide services like "find my device." To get weather updates, users must allow the app to track their locations always, the list can be unending. The data collected by these apps and devices are viable merchandize for business entities, and trophies for hackers [6]. But consumers are not often aware of this data market or at least, how it operates. It is such that your data may be sitting in the database of a company you have never had anything to do with. This was the case of T-Mobile data breach that exposed about 40 million people and some of them never had a T-Mobile line [6].

3. Privacy Protection Policies Today

The U.S. government, though embraces a relatively hands-off approach to data governance [7], works with the public through its agencies to keep an eye on the corporate world on privacy issues. For instance, Privacy by Design was introduced by the Federal Trade Commission (FTC) in 2012 to mandate organizations to inbuild consumer privacy protections at every phase of designing and developing a product [2]. Ten years down the line in 2022, FTC maintains a posture that assures the public of the agency's commitment to privacy protection. FTC

recently hosted a public forum on commercial surveillance and data security as part of Advanced Notice of Proposed Rulemaking. Members of the public are invited to ask several questions to determine if new rules would be needed to hold the commercial surveillance economy responsible [8]. Questions that fall under harms to consumers, harms to children, discrimination, consumer consent, notice, transparency, and disclosure among others, would receive attention from the agency.

U.S. populace also have the luxury of the government and the business world counterbalancing each other's interests in protecting the privacy of the consumers [9]. U.S. businesses may draw on public support to decline to cooperate with government's request to have a backdoor access to a feature of their technology, like WhatsApp's end-to-end encryption, that protects consumers' privacy. In a way though, it may be the only way for the businesses to secure the trust of the market and to avoid being bombarded with myriads of lawsuits by the consumers. Even before current robust privacy policies, the fair information practices (FIPs) which consider individuals' rights, and how information is collected, used, stored, and disclosed, among others, was a good placeholder that evolved into a backdrop for today's privacy law [2].

Aside from holding the corporate world accountable, U.S. law also expects the U.S. government to observe "reasonable privacy" in the discharge of its duties to the citizens [2]. Hence, privacy protection in the United States strives to set boundaries for organizations, public or private, when dealing with citizens' or consumers' data. But this effort is not centrally coordinated [7]. The involvement of state governments that birthed legislations like the California Consumer Privacy Act of 2020, and the California Privacy Rights Act slated for January 2023 [10], among others, support the need for the U.S. government at the federal level to provide leadership in this area. Businesses and malicious actors (domestic or foreign) may find it easier to take advantage of loopholes in individual state privacy laws, than federal privacy laws.

On the Chinese's side, the attention seems to be on the state's interest. The corporate world may have nothing to worry about as long as the government is satisfied. The Chinese government has been able to rein in internet content and access with the use of "the Great Firewall [7]." The government also introduced the public security informatization (PSI) to steer public policing towards preemption from its traditional reactionary approach using data collection and synthesis [11]. Aside from the hundreds of millions of surveillance cameras monitoring the citizens, businesses, small or big, in China primarily run to satisfy the demands of the state, including sharing of user's personal data. This apparently gives the Chinese government unending access to data under the umbrella of security.

Put differently, in the Chinese context, there seems to be loyalty only to the interest of the government while every other issue, including privacy protection, takes care of themselves. The COVID-19 pandemic, which forced the world to live online, seems to have also stimulated China to come up with privacy protection policy that attracts global attention. China is dubbed the most prepared country for the roll out of 5G technology [12], but the first comprehensive Chinese law, Personal Information Protection Law (PIPL), to control online data and protect personal information was only introduced last year – 2021 [13]. It allegedly draws from the General Data Protection Regulation (GDPR) of the European Union to establish an extraterritorial framework for treating personal information doing business in China[13,14].

The topic of Chinese companies sharing data with the Chinese government is not new to American public. It was one of the reasons TikTok and WeChat received U.S. government's attention under the tenure of President Donald Trump. The Trump administration ordered the company should be sold to a U.S. person. The process was halted under the Biden administration as TikTok promises to meet the demands of the U.S. government. The Biden Administration replaced the Trump-era ban with mandate for the Commerce Department to embark on national security review of apps connected to U.S. enemies, China inclusive[15,16].

4. The Impact of 5G

The magic of 5G is the magnitude of change it throws at the world of technology. The fastest wireless generation speed achievable under the Fourth Generation Long Term Evolution (4G LTE) was 10-20 megabits per second download, which was a significant advancement over the Fourth Generation (4G) 2-10 megabits per second download; both were introduced in the same year – 2010. But with 5G, the speed is 200-634 megabits download [17]! While several organizations are still at the stage of deliberating on how to adopt the new technology, the difference in those numbers shows how irrelevant today's speed of doing business could become very soon. But our attention is on privacy protection in this superfast computing environment.

It is believed that 5G has new cyber risks and increased cyberattacks on its trails [1]; this is especially related to the Internet of Things (IoT) [17]. Mobile carriers are interested in bringing IoT to the 5G space which will substantially boost smart cities, homes, cars, and other devices. These devices become targets for malicious actors to conduct their operations, including eavesdropping and denial of service attack. Avenues for data collection increases and points of vulnerability skyrocket. Consumers will have to keep track of updates and patch releases for their devices, homes, and cars, to be relatively safe.

Furthermore, the emergence of new technologies may change the value of currently unprotected data. In data analysis, we talk of composite key, which will do the work of a unique identifier like a primary key. What if access to the first and last name of someone, plus access to the vehicle identification number (VIN) of their self-driving car will have the same implication tomorrow as having access to their social security number (SSN) today? That may require an overhaul of several processes, including changing how names are displayed on items that are shipped. Online stores may have to generate another way of shipping items to buyers without giving out their names. The use of drones for delivery may make this less difficult to handle. But the need for a powerful and instant intervention may be more obvious than it is understood today. While privacy protection may not be guaranteed, the Chinese government currently seems more positioned for taking such action.

5. Conclusion

As 5G unwinds and its benefits are enjoyed, it will become cheaper – the number of users will drive down the cost – and the budget issue that tops the list today may no longer be a concern. But privacy protection is a topic that will linger and evolve as more 5G-native technologies are unveiled. There may be too many things to track, that an average consumer in the United States may get overwhelmed, creating some form of apathy towards privacy protection discussions

Ironically, that mental stress may not be there on the Chinese side because privacy protection is more of a government decision based on national interest than an attempt to protect consumers' privacy. This, however, may begin to change depending on how PIPL is implemented. U.S. policy makers, the corporate world, and the public can blunt off the perceived negative impact of 5G by engaging in deliberate effort to integrate privacy protection into it while adopting its technologies and developing solutions that do not postpone discussions about consumer privacy. Most importantly, the United States may be long overdue for a nationally coordinated privacy protection campaign

References

[1] GDIT, "5G Research Report - Enterprise to the Edge: Agency Guide to 5G," General Dynamics Information Technology, 2022.

[2] J. Pavolotsky, "Privacy in the Age of Big Data," *The Business Lawyer,* vol. 69, no. No. 1, pp. 217-225, 2013.

[3] T. Gundu, "Big Data, Big Security, and Privacy Risks," *Journal of Information Warfare,* vol. 18, no. No. 2, pp. 15-30, 2019.

[4] J. Brookes, J. Bonomo and T. M. Bonds, "America's 5G Era: Balancing Big Data and Privacy," RAND Corporation, 2022.

[5] D. E. Pozen, "Privacy-Privacy Tradeoffs," *The University of Chicago Law Review,* pp. 221-247, 2016.

[6] T. Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," Wirecutter, 6 September 2021. [Online]. Available: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/. [Accessed 4 December 2022].

[7] M. P. Goodman and D. Gerstel, "Sharpening America's Innovative Edge," Center for Strategic and International Studies (CSIS), 2020.

[8] FTC, "Commercial Surveillance and Data Security Rulemaking," Federal Trade Commission, 11 August 2022. [Online]. Available: https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking. [Accessed 18 November 2022].

[9] Ethics Unwrapped, "The FBI & Apple Security vs. Privacy," McCombs School of Business, 2022. [Online]. Available: https://ethicsunwrapped.utexas.edu/case-study/fbi-apple-security-vs-privacy. [Accessed 20 December 2022].

[10] A. R. Friedman, S. S. Sparling, R. Wilcox and A. Manes, "Client Alerts: Comparing the 5 Comprehensive Privacy Laws Passed by US States," Kramer Levin, 10 June 2022. [Online]. Available: https://www.kramerlevin.com/en/perspectives-search/comparing-the-5-comprehensive-privacy-laws-passed-by-us-states.html. [Accessed 20 December 2022].

[11] L. Ruan, "When the Winner takes it all: Big Data and Public Security," Australian Strategic Policy Institute, 2018.

[12] P. Triolo, "China's Uneven High-Tech Drive," Center for Strategic and International Studies (CSIS),

2020.

[13] Cooley Alert, "China's New National Privacy Law: The PIPL," Cooley, 30 November 2021. [Online]. Available: https://www.cooley.com/news/insight/2021/2021-11-30-china-new-national-privacy-law. [Accessed 6 December 2022].

[14] K. (. Dai and D. Jet (Zhisong) Deng, "Practical Guidance: China Personal Information Protection Law (PIPL) FAQs," Bloomberg Law, 6 April 2022. [Online]. Available: https://pro.bloomberglaw.com/brief/china-personal-information-protection-law-pipl-faqs/. [Accessed 6 December 2022].

[15] B. Allyn, "Biden Drops Trump's Ban on TikTok And WeChat — But Will Continue The Scrutiny," NPR, 1 June 2021. [Online]. Available: https://www.npr.org/2021/06/09/1004750274/biden-replaces-trump-bans-on-tiktok-wechat-with-order-to-scrutinize-apps. [Accessed 6 December 2022].

[16] J. Whalen and E. Nakashima, "Tech Policy: Biden revokes Trump's TikTok and WeChat bans, but sets up a security review of foreign-owned apps," The Washington Post, 9 June 2021. [Online]. Available: https://www.washingtonpost.com/technology/2021/06/09/tiktok-ban-revoked-biden/. [Accessed 6 December 2022].

[17] S. Fonyi, "Overview of 5G Security and Vulnerabilities," *The Cyber Defense Review*, pp. 117-134, 18 November 2019.

[18] M. Halpert, "More Than A Dozen Killed In 15 Mass Shootings Over Labor Day Weekend," Forbes, 6 September 2022. [Online]. Available: https://www.forbes.com/sites/madelinehalpert/2022/09/06/more-than-a-dozen-killed-in-15-mass-shootings-over-labor-day-weekend/#:~:text=Big%20Number,began%20tracking%20incidents%20in%202014.. [Accessed 16 November 2022].

[19] GVA, "Mass Shootings in 2022," Gun Violence Archive, 2022. [Online]. Available: https://www.gunviolencearchive.org/reports/mass-shooting. [Accessed 16 November 2022].