Information Privacy and Security

Adil Gokturk

Syracuse University, MS in Applied Data Science Program

IST 618

Surveillance State of China

Topics

- Introduction: The Surveillance State of China
- Mass Surveillance Data
- The Controversial Chinese Company, Global Tone Communications Technology—GTCOM
- Ethical dilemmas
- The Policy to Protect Privacy

Surveillance State of China

This is not a dystopian fictional novel. China is the world's largest and highly effective surveillance state. China's massive network of surveillance system is collecting data to supervise its citizens. The Chinese government monitor its citizens thorough internet, camera surveillance and other advance tech applications.

The Wall Street Journal Columnist, Shan Li and Philip Wen argues that The Chinese government using "a widely downloaded mobile app and translation service to hoover up billions of pieces of data inside its borders and around the world"(Shan Li, 2019). According to another report published by German cybersecurity company Cure53, the app has been associated to a digital-age "Little Red Book of Chairman Mao's quotations and that has signed up more than 100 million registered users provides a potential backdoor for Chinese Communist Party to log users' locations, calls and contact lists (Shan Li, 2019). According to research form the Australian Strategic Policy Institute in Canberra, the Chinese government have been "required to its employees, students, civilians to download the app, and asking them to actively engage by earning points on the app by, among other activities, taking quizzes, watching videos" (2019). This particular report is also backed by Australian government and Western Defense contractors, says Li and Wen.

Mass Surveillance Data

According to 2019 Humans Rights Watch World Report, Chinese authorities dramatically stepped up repression and systematic abuses against the 13 million Turkic Muslims, including Uyghurs and ethnic Kazakhs, in China's northwestern Xinjian region (HRW, 2019). The report argues that,

> “The Authorities increasingly deploy mass surveillance systems to tighten control over society. In 2018, the government continued to collect, on a mass scale, biometrics including DNA and voice samples; use such biometrics for automated surveillance purposes; develop a nationwide reward and punishment system known as the “social credit system”; and develop and apply “big data” policing programs aimed at preventing dissent. All of these systems are being deployed without effective privacy protections in law or in practice, and often people are unaware that their data is being gathered, or how it is used or stored (HRW, 2019).

The China’s massive surveillance system is the by far the largest on Earth. The Economist argues that the current forms of monitoring include the abundant “use of closed-circuit television cameras. In 2009 China had 2.7m of them; now it may have overtaken America as the country with the largest number of CCTV devices. According to Jack Ma, head of Alibaba, China’s largest internet firm, the company’s hometown of Hangzhou has more surveillance cameras than New York, a somewhat larger city” (Economist, 2016).

The Controversial Company, Global Tone Communications Technology—GTCOM

There is a grift and complex cooperation between the Chinese government and the major Chinese multinational companies. Li and Wen (2019) argues that the Australian Strategic Policy Institute’s report found strong indication that the Chinese company, Global Tone Communications Technology Co.—GTCOM, “generated military and other state-security intelligence” using data the company harvested. The report(Shan Li, 2019) also says the data could help “support the party-state’s development of tools for shaping public discourse.”

The report indicates that the GTCOM’s parent entities, China Translation Corp. and China Publishing Group, are under the direct supervision of China’s Central Propaganda Department. GTCOM has collaboration agreements with foreign academies in Sydney, Vienna and somewhere in the West(Shan Li, 2019). The company’s director of big data, Mr. Liang Haoyu, demonstrated in his 2017 presentation available on its website, that “the company was trying to build up technologies such as voice and facial recognition for “real-time monitoring” of security risks” (Shan Li, 2019).

> Mr. Liang Haoyu also said: “In the future, [GTCOM] will be able to find the requested facial structure through image recognition and provide technical support and assistance for state security,” said. The presentation also claimed that “90% of military-grade intelligence data can be obtained from open data analysis”(Shan Li, 2019).

GTCOM is not the only company in China that cooperates with the Chinese government to harvest its citizens’ data. For instance, Alibaba Group also helped the Chinese authorities to collect data by helping them to build one of the most downloaded apps called “*Xuexi Qiangguo*” in China. According to an analysis by the Open Technology Fund, the code found in the app provides “superuser” access to mobile devices , which includes the ability to modify files and install software that logs keystrokes. To able use the app, users have to agree to allow access to a trove of personal data, as well as to cameras, microphones, call logs and locations (Shan Li, 2019). The Fund’s analysis also states that “ the app also has weak encryption software that can be easily cracked, leaving email, biometric data and other information exposed. That could provide a path to efficiently collect and analyze messages and other data on millions of users” (Shan Li, 2019).

Ethical Dilemmas

Apparently, government authorities, politicians and giant tech companies' collaboration is not new. Google, Facebook, data-brokers and marketing companies such as Cambridge Analytica collaboration even during the controversial 2016 American Presidential Election campaigns(ur Rehman, 2019). Despite ongoing investigation on numerous data breach and political manipulation arguments, the massive amount of personal data—over 80 million US citizens' Facebook account breach, "relatively" didn't cause a serious harm to civil liberties, the Economist argues (2016).

Evidently, China treats personal data differently from the Western World. Apparently, laws and regulations relatively limit what companies may do with the data and the authorities extent which governments can get their hands on it (Economist, 2016). The privacy and data use protection laws, rules, regulation and policies in the Western world are imperfect, but they do not exist in China.

Shoshana Zuboff's book *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* highlights the close and potential danger of a new mutant form of capitalism that could be a major threat against the civilization (Naughton, 2019). Zuboff argues that the usage of behavioral data is "the exploitation of behavioral predictions covertly derived from the surveillance of users (Naughton, 2019)," which is not so far from the Chinese authorities' approach on data usage.

The Economist (2016) argues that "the national-security law and the new cyber-security law give the Chinese government unrestricted access to almost all personal data. Civil-liberty advocates who might protest are increasingly in jail. Apparently, the national security is the major setback, even in the Western Democracies. Let's just try to remember the extensive coverage of the Patriot Act of 2001. The Act has restrictions, limitations, privacy breaches as well as it has constitutional rights violations such as 4th amendment.

Apparently big data and its applications in democracies are not designed for social control, the Economist(2016) argues. Evidently, China's approach serve to design for social control on its citizens. Because of the leaders of China believe that "the interest of the party and society to be the same, instruments of social control can be used for political purposes" (Economist, 2016).

The Policy to Protect Privacy

Apparently, it is highly difficult to design a global policy to protect personal privacy. There is no consensus between the global players of nation states, even in European Union. The players—nation sates perceptions are different –yes, even in the Western world. But the worst part is that there is a rising trend of autocracy, nationalism, and sadly fascism, even in the European Union. Therefore, it seems like it would take some time to design a perfect policy to protect privacy.

Though, it would be good start, if there would be a global consensus on privacy as a fundamental human right and essential to a Democratic society as the constitutional core of human dignity(Jones, 1991). Data ownership also another setback to design a policy to protect privacy. I believe the personnel data would be solely owned by the person and he/she/LGBT has the right to be forgotten whenever he/she/LGBT wants.

The ownership of data is the most crucial part of the Policy argument. Who owns the data and who will protect that right? Companies? Government or another non-profit or non-governmental organizations or private citizens?

Apparently, China is the worst possible example as the world’s first totalitarian and the largest surveillance state. Therefore, any totalitarian regimes or digital dictatorships would not be the case. The path to perfect policy requires economic wellbeing, stability, education, and security. Noticeably, none of these pillars are exist in the current situation of the global societies. However, that doesn’t mean that we can’t do anything.

Global education awareness and initiative would be a good start for the Policy makers to convince global community that the data ownership and privacy is a fundamental human right. What make us human is that we believe we have freedom of choice. The unethical usage of data such as physiological manipulative corporate or political marketing by using AI makes us puppets not humans. Consequently, to being free and still have a freedom of choice, policy makers focus on the usage and collection method of data.

The de-centralized data collection and usage would be another crucial aspect of privacy that the policy makers always consider. I believe that the de-centralized ethical usage of data and the ownership of the data will not just protect the data but it will define the privacy. Apparently, privacy and fair usage of data has long way to go, but it seems not impossible.

References

China invents the digital totalitarian state. (2016). Economist, T. [Mobile application software]. Retrieved from https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state

HRW (Producer). (2019, December 11, 2019). 2019 Humans Rights Watch World Report. Retrieved from https://www.hrw.org/world-report/2019/country-chapters/china-and-tibet

Jones, M. G. (1991). Privacy: A Significant Marketing Issue for the 1990s. *Journal of Public Policy & Marketing, 10*(1), 133-148. Retrieved from http://www.jstor.org/stable/30000256

Naughton, J. (2019, 01/20/

2019 Jan 20). 'The goal is to automate us': welcome to the age of surveillance capitalism. *The Observer,* p. 16. Retrieved from https://search.proquest.com/docview/2168774265?accountid=14214

http://nq5hl7cp9d.search.serialssolutions.com/directLink?&atitle=%27The+goal+is+to+automate+us%27%3A+welcome+to+the+age+of+surveillance+capitalism&author=Naughton%2C+John&issn=00297712&title=The+Observer&volume=&issue=&date=2019-01-20&spage=16&id=doi:&sid=ProQ_ss&genre=article

Shan Li, P. W. (2019, Oct. 14, 2019). This App Helps You Learn About China, While China Learns All About You. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/china-broadens-data-collection-through-propaganda-app-and-translation-service-11571058689

ur Rehman, I. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice*, 1-11. Retrieved from https://search.proquest.com/docview/2234441812?accountid=14214

http://nq5hl7cp9d.search.serialssolutions.com/directLink?&atitle=Facebook-Cambridge+Analytica+data+harvesting%3A+What+you+need+to+know&author=ur+Rehman%2C+Ikhlaq&issn=&title=Library+Philosophy+and+Practice&volume=&issue=&date=2019-01-01&spage=1&id=doi:&sid=ProQ_ss&genre=article