Is Privacy Dead?

By: Nir Kshetri and Joanna F. DeFranco

Kshetri, Nir and J. DeFranco (2020). "Is Privacy Dead?", *IEEE IT Professional,* vol. 22.*(5)* pp. 4-12, https://doi.org/10.1109/MITP.2020.2992148

Abstract:

People value their privacy. According to a survey conducted in the U.S., 90% of respondents viewed it important to control the information about them collected. Yet, it seems very little control is possible. With the many advances in technology, collecting, monitoring, and transferring personal information (PI) can be done with ease. Making a discussion regarding privacy urgent. Privacy is an ethical issue. The ACM addressed privacy in their Code of Ethics and Professional Conduct in Section 1.6 titled Respect Privacy by stating, 'computing professionals should only use information for legitimate ends and without violating the rights of the individuals and groups.' In addition, the implications of PI data collection are often not explained to the user, as such, the IEEE Code of Ethics addressed this topic by stating to 'improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems.' Nevertheless, powerful entities such as governments and big companies have been aggressively collecting personal data in an unprecedented scale in legal as well as deceptive and illegal ways. Misuse, breach and leak of such information have become an even bigger concern. This creates a data market based on an ethically questionable foundation.

Keywords: privacy | Google | companies | surveillance | artificial intelligence | ethics

Article:

People generally value their privacy. According to a survey conducted in the U.S., 90% of respondents viewed it important to control the information about them collected [1]. Yet, it seems very little control is possible. With the many advances in technology, collecting, monitoring, and transferring personal information (PI) can be done with ease. Making a discussion regarding privacy urgent. Privacy is an ethical issue. The ACM addressed privacy in their *Code of Ethics and Professional Conduct* in Section 1.6 titled *Respect Privacy* by stating, "computing professionals should only use information for legitimate ends and without violating the rights of the individuals and groups." In addition, the implications of PI data collection are often not explained to the user, as such, the *IEEE Code of Ethics* addressed this topic by stating to "improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems."

Nevertheless, powerful entities such as governments and big companies have been aggressively collecting personal data in an unprecedented scale in legal as well as deceptive and illegal ways. Misuse, breach and leak of such information have become an even bigger concern. This creates a data market based on an ethically questionable foundation [2].

Organizations that benefit from personal data such as phone and Internet companies, device makers, and application developers often claim that they have obtained users' permission to constantly collect PI. However, users are almost never explicitly asked if they want all of their activities to be tracked and traced. Most users' lack of understanding of how tracking works is arguably a key factor that has enabled these companies to collect personal data. An example is how consent is requested for data collection. It is often granted by a user because the request is made in an obscure, confusing, and verbose fashion. Or worse, having the user agree to misrepresented default settings. For example, Facebook's "tag suggestions" default feature was actually a facial recognition tool. In July 2019, Facebook was fined $5 billion for engaging in deceptive practices [3]. The obscurity in which PI is dealt with is clearly an ethical issue. However, is facial recognition and surveillance okay when the surveillance benefits a majority? China's approach to artificial intelligence (AI) development has been described as "techno-utilitarian." The utilitarian approach is a fundamental ethics principle where a decision is made based upon the greatest good for the greatest number of people. Thus, the protection of personal privacy and individual rights receives less emphasis. Some critics have noted that such arguments have been used to justify the use of AI for surveillance purpose and to suppress minorities and political opponents such as Muslims in the Xinjiang province [4].

Facebook also inappropriately shared information of 87 million of its users with the political consultancy Cambridge Analytica [5]. The data was used to build a system that profiled individual U.S. voters and targeted them with personalized political advertisements [6]. In addition to companies collecting PI for their own agenda, it is concerning that they are not protecting this information from nefarious hackers. In October 2017, Yahoo revealed that PI such as email addresses, names, and phone numbers of all its three billion users was stolen [7].

Indeed, misuse and abuse of PI has been a worldwide trend. For instance, a survey conducted by the China Consumers Association in 2018 revealed that 85% of Chinese had suffered data leaks such as phone numbers being sold to spammers and bank account details stolen by criminals [8]. Many Chinese consumers who receive credits from the fintech companies feel that they are victimized by misuse and abuse of their personal data. In a *China Youth Daily* poll, 76% of respondents believed there was such abuse [9]. A key factor that has contributed to the declining privacy is that markets of personal data are characterized by a high degree of opacity. While consumers participate in the data economy, as mentioned earlier, they lack awareness regarding data tracking, use, and transfer. This has contributed to organizations' tendency to collect too much data and provide too little security and privacy [10].

The situation is further complicated by the fact that information aggregators deliberately collect information from public and semiprivate sources and distributes it for economic gains. In addition to text, private information in multimedia forms such as pictures, voices, and videos are increasingly available [11]. Processes and technology solutions for securing unstructured data such as voices and videos are in nascent phase and governance issues are not addressed for such data.

The seriousness of this issue has increased by the fact that regulations do not adequately protect consumers from the revelations of their information [12]. Moreover, ethical standards and codes of conduct related to organizations' collection and use of personal data are not well established. Most companies also lack best practices and privacy policies to handle sensitive PI. Due to the lack of regulations and guidelines, some uses of consumer information are dangerous, creepy, and annoying. The worst part is that the practices are not necessarily considered as illegal.

POWERFUL ENTITIES' ENGAGEMENT IN DECEPTIVE PRIVACY PRACTICES

Corporations tracking consumers for economic gains and governments spying on citizens for political controls have led to an increasingly pervasive privacy violation. Some illustrative examples of powerful entities that have engaged in deceptive privacy practices are presented in Table 1. Most of the profits of companies such as Alibaba, Facebook, and Google involve monetizing users' data. Such a business model, however, has fundamental privacy issues [13]. In addition to big companies, governments have been using private data for the purpose of surveillance and control over their citizens. The Chinese government is probably the best example that illustrates such a trend (see Table 1).

Table 1. Some powerful entities' engagement in deceptive privacy practices.

Entity	Unfair and harmful practices involving private data	Remarks
Facebook	• Allowed third-party developers to collect data about app users' 'friends' violating an agreement to not collect 'friend' data. • Private information of about 87 million users was shared illegally with Cambridge Analytica. • Content labelling projects to develop Al programs: contract workers of an outsourcing firms were given access to millions of users' personal information.	July 2019: fined $5 billion by the FTC
Google	• 2013: publicly acknowledged that its Street View mapping project violated privacy. • Project Nightingale: secret data sharing scheme with Ascension in which sensitive patient information was accessed by at least 150 employees. • Flaw in Google Plus: exposed personal data of hundreds of thousands of subscribers.	• Street View mapping: settled the case – employees are required to follow privacy rules and required to inform the public how to defend against such violations. • Project Nightingale and Google Plus flaws: argued that it followed relevant regulations.
Alibaba	• 2017: Alibaba users enrolled in Sesame Credit without their knowledge. • Abuse of personal data to collect debts.	Argued that the practice of contacting borrowers' friends/relatives to help with collecting debts is common.
Chinese government	Use of a secret system of advanced facial recognition technology to track the Uighurs.	Exported AI-based surveillance tools to other countries.

Facebook

There have been several accusations that Facebook violated fair uses of personal data. It was reported to have data-sharing agreements with at least 60 device makers such as Apple and

Samsung and many other companies. Sensitive data about users' friends, such as relationship status, religion, and political leaning were allegedly shared [14]. In April 2014, Facebook announced that it would not allow third-party developers to collect data about the app users' friends. However, it failed to fulfill this agreement. Developers were to stop data collecting as of April 2015. In addition, it was reported that user data was shared via third party apps until June 2018.

The Facebook–Cambridge Analytica data scandal has been among the most discussed issues in deceptive handling of personal data. In early 2014, as mentioned above, Cambridge Analytica allegedly obtained the private information of about 87 million Facebook users. The data was collected illegally without the users' knowledge and used to build a system that profiled individual U.S. voters and to predict as well as influence their choices on election day [15].

Facebook's content labeling projects undertaken to develop its AI programs also allegedly violate users' privacy. As of mid-2019, it was reported to have 200 such projects that employed thousands of people globally. In one such project, about 260 contract workers in India of the outsourcing firm Wipro were given access to millions of Facebook users' photos, status updates, and other contents that were posted since 2014. The items posted were categorized in terms of various dimensions such as the subject of the post, the occasion in which it was posted and the author's intention [16].

Google

Several of Google's services have been accused of violating personal privacy. One example is the Google Street View [17]. As of December 2019, Google covered the world's 98% of the places where people live and 10 million miles of Street View imagery [18]. Google's Street View imagery provides a lot of useful information about homeowners. For instance, researchers have found that by analyzing features that are visible on a house's picture (e.g., detached/terraced house, block of apartments, age, conditions, etc.). This information is very interesting to insurance companies as they can more precisely predict car accidents by profiling homeowners, thus, maximizing their profitability [19].

In 2013, Google publicly acknowledged that its Street View mapping project violated privacy when it collected PI such as people's passwords and e-mail. In order to settle a case filed by 38 U.S. states about the project, Google agreed to have its employees follow privacy rules as well as explicitly inform the public how they can defend themselves against such privacy violations [20].

Google has also been accused of secretly collecting sensitive healthcare data without patients' knowledge and giving its employees access to such information. The accusation is concerned with the initiative "Project Nightingale" carried out with St. Louis-based Catholic hospital Ascension, which is the second-largest health system in the U.S. Ascension's 2600 hospitals, doctors' offices, and other facilities across 21 U.S. states allegedly participated in the secret data sharing scheme without the knowledge the provider's doctors or patients. Patients' sensitive information collected and shared under the initiative included lab results, doctor diagnoses and hospitalization records, patient names and dates of birth. The stated goal of the initiative is to improve medical outcomes with cloud-based AI services. Tens of millions of patients' data were accessed by at least 150 Google employees [21]. Some Ascension employees had expressed concerns that Google employees' access to patients' private health information violates privacy.

After media reports of the potential misuse of patients' sensitive information, Google published a FAQ (*https://cloud.google.com/blog/topics/inside-google-cloud/our-partnership-with-ascension*), which argued that the initiative followed all relevant regulations [13]. However, such practices of collecting large amounts of PI about patients without their knowledge or consent and for purposes that they do not expect or understand obviously lack an ethical foundation [22]. It also violates the transparency *principle* the Fair Information Practices.

Google also reportedly found a flaw with its social-networking site Google Plus, which exposed personal data such as birth dates and contact information of hundreds of thousands of subscribers. The company, however, decided not to disclose the flaw to users due to fears of regulatory scrutiny. In this case also, Google argued that it followed relevant legal requirements in its decision not to inform users [23].

Alibaba

Alibaba and its affiliates have allegedly engaged in misleading and deceptive conducts in handling personal data of its customers. For instance, Alibaba's mobile and online payment platform, Alipay users, without their knowledge, were enrolled in its credit scoring system, Sesame Credit, which is a credit scoring and loyalty program system developed by Alibaba's affiliate Ant Financial Services Group [24]. Alipay's end-of-year feature allows its users to analyze their spending patterns for the year. At the 2017 end, the feature started enrolling the users to Sesame. Sesame Credit allegedly failed to meet the PI security standards by collecting consumers' data and sharing the analysis with partners. It was reported that there was a small section at the landing page's bottom, which contained an agreement to automatically enroll the users in Sesame Credit. It was checked by default [25]. China's cyber watchdog the Cyberspace Administration of China expressed concerns that Ant Financial compromised consumer privacy and failed to comply with the country's PI security standards.

Alibaba's affiliates have also allegedly abused personal data to collect debts. A common practice among Chinese financial services companies has been to share customers' irresponsible behaviors such as debt default with others in the defaulter's common social group memberships such as friends in social networking applications. Such practices would lead to potential harms, such as embarrassment, a damaged reputation and loss of social status of the affected consumer. One such example is Alibaba's Ant Check Later, which allows users to delay payments and pay in installments. An online user reported that he was contacted by Ant Check Later for information about his friend, who owed money to the payment service. Ant Financial Services reportedly said that the practice of contacting a borrower's friends or relatives to help with collecting debts is common in the financial sector [26].

China

Chinese consumer fear of and anger against corporate misuse of personal data is arguably providing a convenient distraction, and a basis on which the Chinese government has intensified its own data collection initiatives for surveillance [27]. Especially with the help of its technology companies, the Chinese government has elevated the notion of AI-based surveillance to a new height.

Specifically, China is allegedly using a secret system of advanced facial recognition technology to track the Uighurs (e.g., an ethnic minority in China). An article published in the *New York Times* described the use of facial recognition technology to track the Uighurs as an “automated racism,” which is integrated into networks of the country's surveillance cameras. The system looks exclusively for Uighurs based on their appearance and keeps records of their movements. Such records can be used for search and review [28].

While some law enforcement agencies and AI providers described the practice as “minority identification,” the tools are exclusively used to identify Uighurs. Uighurs have typical facial and other features that make them more similar to people from Central Asia than China's majority Han population. Due to such differences, it is easy for facial recognition software to identify and single out Uighurs [29].

In non-Xinjiang cities, police run facial recognition systems to investigate a person that appears like a Uighur [30]. Chinese police were reported to be using such systems to target Uighur in wealthy cities such as Hangzhou and Wenzhou and the coastal province of Fujian. Likewise, law enforcement agencies in central China's Sanmenxia city reportedly ran a system 500 000 times in a month in early 2019 to know whether residents were Uighurs or not. Likewise, in 2018, law enforcement agencies from the Shaanxi province wanted to acquire a smart camera system with functionalities to “support facial recognition to identify Uighur/non-Uighur attributes” [31].

The pervasiveness of tracking and surveillance systems has created an environment of fear and anxiety among Uighurs. A tech-savvy Uighur was reported to saying: “We turn off our phones before we talk politics” [32].

China has also sold AI and facial recognition software in foreign countries. For instance, the Philippine's Bonifacio Global City has been equipped with mass-surveillance systems developed by China's Huawei (e.g., a Chinese telecom company). Huawei works with the police and the cameras are linked to data collection tools such as a number plate recognition system. The system gathers evidence and identifies suspects using facial-recognition technology [33]. Privacy advocates have been concerned about potential misuse of data [34]. Other countries such as Serbia, Turkey, Russia, Ukraine, Azerbaijan, Angola, Laos, Kazakhstan, Kenya, Uganda, [35] Ecuador, Bolivian, and Peru [36] are also using China-developed facial recognition software.

PRIVACY ISSUES ASSOCIATED WITH VARIOUS PHASES OF DATA CYCLES

Privacy concerns are linked with the collection and storing of data as well as data sharing and accessibility by third parties and various other data user types. Such concerns related to different phases of data lifecycle are presented in Table 2.

Table 2. Privacy concerns related to various phases of data lifecycle.

Phase	Key issues	Examples
Collection	Some organizations engage in illegal and/or unethical data collection practices and mechanisms without the knowledge of the concerned person.	Nissan's collection of data related to the location, speed and direction of the owners of its LEAF model.
Storing	The methods and mechanisms of storing data lack robust cybersecurity mechanisms, which may lead to breach and leak of personal information.	December 2019: There was a Facebook database breach where more than 267 million Facebook users' personal information was stolen.
Sharing	When two companies exchange a consumer's personal data, the transaction negatively affects the consumer's privacy, which may also put the consumer at a strategic disadvantage.	Walgreens illegally shared medical information from patient prescriptions to data mining companies, which anonymized the data and then sold to pharmaceutical companies.
Accessibility	Most organizations lack systematic approaches for ensuring that appropriate access mechanisms are in place for third parties, permanent and temporary employees and other user types.	In a Facebook's content labelling project, about 260 contract workers of Wipro in India were inappropriately given access to millions of users' personal information.

Collection

Some organizations engage in illegal and/or unethical data collection practices and mechanisms without the knowledge of the concerned person. In 2012, it was revealed that Nissan reported location, speed, and direction of the owners of its LEAF car model to websites that other users could access through a built-in RSS reader. Nissan did not warn its customers that the information was being shared with third parties without their consent. Likewise, there were reports that iPhones and Android phones secretly sent information about users' locations to Apple and Google. [37] Research conducted in a field known as "side-channel attacks" has indicated that even if users turn off their phones' location services, it is possible to get data from other sensors in the phones to track them. Data companies do not require users' permission to access such data [38].

New technological developments have provided new ways of collecting PI since regulatory guidelines have not been well established for such technologies. For instance, the guidelines for drone use are not well-developed. During 2004–2013, the FBI reportedly spent more than $3 million on drones to track individuals in the U.S. The American Civil Liberties Union argued that the FBI and other agencies need to have strong privacy guidelines in place before deploying surveillance drones [39].

Storing

The methods and mechanisms used by most organizations to store data lack robust cybersecurity mechanisms, which may lead to breach and leak of PI. In December 2019, a security researcher reportedly found a database of more than 267 million Facebook users with PI such as the names, phone numbers, and unique user IDs. The information was freely available online for at least ten days for anyone to download. Almost all the victims were U.S.-based. The database had been downloaded to a hacker forum. It was suspected that cybercriminals had harvested the data and they were shared among them [40].

Sharing

When two companies exchange personal data about a consumer, the transaction negatively affects the consumer's privacy, which may also put the consumer at a strategic disadvantage. If the affected consumer is not compensated, the data market can harm the consumer and leave them in a worse-off condition. This could result in an even worse situation when the affected consumer is not made aware of the transaction. [41]

Additionally, organizations often believe that it would be impossible to identify a person if they anonymize data before sharing to third parties. This is often a convenient but possibly false assumption. Researchers have presented a variety of methods and techniques that can be used to anonymize personal data and reassociate with specific consumers [42]. Big data-based predictive models have a high probability of revealing personally identifiable information. Thus, anonymization is nearly impossible.

The identified person may also suffer physical, psychological, or economic harms. For instance, in 2011, customers of the U.S. drugstore Walgreens filed a lawsuit accusing the drugstore of illegally selling medical information from patient prescriptions. Walgreen allegedly sold the prescription information to data mining companies. The information was anonymized and then sold to pharmaceutical companies. The plaintiffs argued that Walgreens unfairly benefitted from the commercial value of their prescription information [43].

Accessibility

A further source of violation is that organizations lack systematic approaches for ensuring appropriate data access mechanisms for various user types such as third parties, permanent and temporary employees [44]. As mentioned earlier, companies such as Google and Facebook gave access of users' PI to their own employees and third parties (see Table 1), as such it is worth noting that insider data breaches have been identified as a key threat of privacy violation. Especially there have been many instances of data breaches in outsourcing destinations with weak privacy laws. To take an example, in 2003, a Pakistani medical transcriber working for a U.S.-based medical center threatened to post confidential voice files and patient records on the Internet if her pay was not increased [45].

SUMMARY

PI provides huge economic and political advantages to powerful entities such as governments and big enterprises. These entities have thus engaged in legal, extralegal illegal, and deceptive means to gather as much PI as possible. In addition to abuse and intentional misuse of personal data, due to these entities' poor cybersecurity practices, such data also falls into the hands of criminals and nefarious actors.

Various types of privacy violations take place in different phases of data lifecycle such as collection, storing, sharing, and accessibility. Most companies' involvement with personal data has been on the first two, which can be attributed to a steep decrease in the costs of collecting and storing data. New technologies such as drones, computer vision, and AI have redefined surveillance. By using more sophisticated technologies such as AI to process PI, adversaries may inflict more economic and psychological harm on a person.

Businesses and governments in nations across the world differ in their relative tendencies to misuse private information. In some way, China and Europe are similar from the privacy standpoint. People have a tendency to trust the government, but companies are often mistrusted since they are viewed as entities that only care about profit. In China, the government is also putting more restrictions on companies' data collection initiatives. On the other hand, the government itself has intensified its surveillance of citizens and companies. In this way, while the economic advantages offered by private information to big enterprises may decrease, political advantages of such information to the government has increased.

A number of uses of personal data currently fall into a regulatory grey area. Due to high economic values of personal data, organizations have adopted business models with questionable privacy practices in order to monetize such data. In most cases, violations of privacy are not penalized. Even if the violators are caught, the penalties are often insignificant. Given the PI data market is extremely lucrative, is there little hope to keep our privacy intact? Can the manipulation, profiling, and criminal activity be reduced or stop? In order for the data market to function more efficiently, clearer government policies and procedures regarding consumer rights and obligations of organizations handling consumer data are needed. Furthermore, consumer education on privacy needs to be a high priority by all. Consumers need to be more vigilant about scrutinizing applications used, reading privacy policies, and reducing their PI footprint on the Internet. In addition, companies need to do their part to build a higher public trust by taking measures to protect consumer data to prevent from theft and misuse. Such measures require increasing investment in cybersecurity.

DISCLAIMER

The authors are completely responsible for the content in this article. The opinions expressed here are their own.

ACKNOWLEDGMENTS

The authors thank Jeff Voas (Editor-in-Chief of IEEE Computer magazine) for his suggestion to write this article and for his edits and suggestions.

REFERENCES

1. A. W. Geiger, "How Americans have viewed government surveillance and privacy since Snowden leaks," Jun. 4,2018. [Online]. Available: https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/

2. J. King, "Change your phone settings so Apple, Google can't track your movements," Jan. 14,2019. [Online]. Available: https://theconversation.com/change-your-phone-settings-so-apple-google-cant-track-your-movements-109059

3. “FTC imposes $5 billion penalty and sweeping new privacy restrictions on facebook,” Jul. 24,2019. [Online]. Available: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

4. J. Thornhill, “Formulating values for AI is hard when humans do not agree,” Jul. 22,2019. [Online]. Available: https://www.ft.com/content/6c8854de-ac59-11e9-8030-530adfa879c2

5. N. Bose and S. Heavy, “U.S. FTC finds Cambridge Analytica deceived facebook users,” Dec. 6,2019. [Online]. Available: https://www.reuters.com/article/us-usa-privacy-cambridgeanalytica/us-ftc-finds-cambridge-analytica-deceived-facebook-users-idUSKBN1YA1YZ

6. C. Cadwalladr and E. Graham-Harrison, “Revealed: 50 million facebook profiles harvested for Cambridge Analytica in major data breach,” Mar. 17,2018. [Online]. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

7. G. P. Slefo, “The 10 biggest brand data breaches of the decade,” Dec. 27,2019. [Online]. Available: https://adage.com/article/year-end-lists-2019/10-biggest-brand-data-breaches-decade/2222096

8. Y. Yang, “China's data privacy outcry fuels case for tighter rules,” Oct. 1,2018. [Online]. Available: https://www.ft.com/content/fdeaf22a-c09a-11e8-95b1-d36dfef1b89a

9. Wantchinatimes.com, “Online credit services in China accused of abusing personal data,” Sep. 27,2015. [Online]. Available: http://www.wantchinatimes.com/news/content?id=20150927000087&cid=1203

10. Y. Carrière-Swallow and V. Haksar, “The economics of data,” Sep. 23,2019. [Online]. Available: https://blogs.imf.org/2019/09/23/the-economics-of-data/

11. B. Hoanca, “If privacy is dead, what can we do instead?” Jun. 29,2017. [Online]. Available: https://technologyandsociety.org/if-privacy-is-dead-what-can-we-do-instead/

12. S. Goswami, “Will the US get a federal privacy law?” Dec. 27,2019. [Online]. Available: https://www.reuters.com/article/us-usa-privacy-cambridgeanalytica/us-ftc-finds-cambridge-analytica-deceived-facebook-users-idUSKBN1YA1YZ

13. H. Mccracken, “5 things Google got right in 2019 – and 5 it got wrong,” Dec. 24,2019. [Online]. Available: https://www.fastcompany.com/9044129.5/5-things-google-got-right-in-2019-and-5-it-got-wrong

14. T. Chan, “Facebook gave use data to 60 companies including Apple, Amazon, and Samsung,” Jun. 4,2018. [Online]. Available: https://www.businessinsider.com/facebook-gave-device-makers-apple-and-samsung-user-data-2018-6

15. C. Cadwalladr and E. Graham-Harrison, “Revealed:50 million Facebook profiles harvested for Cambridge Analytica in major data breach,” Mar. 18,2018. [Online]. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

16. M. Vengattil and P. Dave, “Facebook ‘labels’ posts by hand, posing privacy questions,” *Reuters*, 2019. [Online]. Available: https://www.reuters.com/article/us-facebook-ai/facebook-labels-posts-by-hand-posing-privacy-questions-idUSKCN1SC01T

17. B. Hoanca, “If Privacy Is Dead, What Can We Do Instead?” Jun. 29, 2017. [Online]. Available: https://technologyandsociety.org/if-privacy-is-dead-what-can-we-do-instead/

18. C. Gartenberg, “Google reveals just how much of the world it's mapped with Street View and Earth, Dec. 13.2019. [Online]. Available: https://www.theverge.com/2019/12/13/21020814/google-world-mapped-street-view-earth-square-miles

19. Emerging Technology, “How a Google Street View image of your house predicts your risk of a car accident,” Apr. 30,2019. [Online]. Available: https://www.technologyreview.com/s/613432/how-a-google-street-view-image-of-your-house-predicts-your-risk-of-a-car-accident/

20. D. Streitfeld, “Google concedes that drive-by prying violated privacy,” Mar. 12,2013. [Online]. Available: https://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html

21. R. Copeland, “Google's ‘Project Nightingale’ gathers personal health data on millions of Americans,” Nov. 11,2019.

22. J. Brill, “Demanding transparency from data brokers,” Aug. 15,2013. [Online]. Available: http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html

23. R. Copeland, “Google's ‘Project Nightingale’ gathers personal health data on millions of americans,” Nov. 11, 2019. [Online]. Available: https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

24. “China's cyber watchdog scolds Ant Financial over user privacy breach,” CNBC, Jan. 10,2018. [Online]. Available: https://www.cnbc.com/2018/01/10/chinas-cyber-watchdog-scolds-ant-financial-over-user-privacy-breach.html

25. H. Wei, “Alipay makes changes after privacy criticism,” China Daily, Jan. 5,2018. [Online]. Available: http://www.chinadaily.com.cn/a/201801/05/WS5a4eb557a31008cf16da5288.html

26. N. Kshetri, “Big Data's role in expanding access to financial services in China,” *Int. J. Inf. Manage.*, vol. 36, no. 3, pp. 297–308, 2016.

27. Y. Yang, “China's data privacy outcry fuels case for tighter rules,” Oct. 1, 2018. [Online]. Available: https://www.ft.com/content/fdeaf22a-c09a-11e8-95b1-d36dfef1b89a

28. P. Mozur, “One month, 500,000 face scans: How china is using A.I. to profile a minority,” Apr. 14,2019.

29. P. Mozur, “One month, 500,000 face scans: How China is using A.I. to profile a minority,” Apr. 14, 2019. [Online]. Available: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

30. A. Zenz, “Xinjiang's new slavery,” Dec. 11,2019. [Online]. Available: https://foreignpolicy.com/2019/12/11/cotton-china-uighur-labor-xinjiang-new-slavery/

31. P. Mozur, “One month, 500,000 face scans: How China is using A.I. to profile a minority,” Apr. 14, 2019. [Online]. Available: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

32. J. Palmer, “Will China use big data as a tool of the state?,” 2015. [Online]. Available: http://aeon.co/magazine/technology/will-china-use-big-data-as-a-tool-of-the-state/

33. N. Mandhana, “Huawei's video surveillance business hits snag in Philippines,” The Wall Street J., 2019. [Online]. Available: https://www.wsj.com/articles/huaweis-video-surveillance-business-hits-snag-in-philippines-11550683135

34. B. O'Rourke and G. Choy, “Big brother Huawei kitted out this Philippine city. Is China watching?” South China Morning Post, 2019. [Online]. Available: https://www.scmp.com/week-asia/economics/article/2183540/big-brother-huawei-watches-philippine-city-does-china-too

35. Getty, “Chinese facial recognition tech installed in nations vulnerable to abuse,” Oct. 16, 2019. [Online]. Available: https://www.cbsnews.com/news/china-huawei-face-recognition-cameras-serbia-other-countries-questionable-human-rights-2019-10-16/

36. C. Rollet, “Ecuador's all-seeing eye is made in China,” Aug. 9,2018. [Online]. Available: https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/

37. A. Cohen, “Will ‘Stalking Apps’ be stopped?,” Feb. 13,2013. [Online]. Available: http://ideas.time.com/2013/02/04/will-stalking-apps-be-stopped/

38. G. Noubir, Feb. 6,2018. [Online]. Available: https://theconversation.com/your-mobile-phone-can-give-away-your-location-even-if-you-tell-it-not-to-65443

39. E. Rosenberg, “Report: FBI spent $3 million on drones,” Sep. 27,2013. [Online]. Available: https://www.usnews.com/news/newsgram/articles/2013/09/27/report-fbi-spent-3-million-on-drones

40. F. Bajak, “Researcher: Data on 267 million Facebook users exposed,” Dec. 19,2019. [Online]. Available: https://apnews.com/bdf02dbe7bf266b025b6f1b0ae5860fd

41. Y. Carrière-Swallow and V. Haksar, “The economics of data,” Sep. 23,2019. [Online]. Available: https://blogs.imf.org/2019/09/23/the-economics-of-data/

42. J. Brill, “Remarks: Big data, big issues,” Mar. 2,2012. [Online]. Available: http://www.ftc.gov/public-statements/2012/03/big-data-big-issues

43. D. Manos, “Patients sue Walgreens for making money on their data,” Mar. 18,2011. [Online]. Available: http://www.healthcareitnews.com/news/patients-sue-walgreens-making-money-their-data

44. N. Kshetri, “Big Data's Impact on Privacy, Security and Consumer Welfare,” *Telecommun. Policy*, vol. 38, pp. 1134–1145, 2014.

45. N. Kshetri, “ICTs, strategic asymmetry and national security,” *J. Int. Manage.*, vol. 11, no. 4, pp. 563–580, 2005.