Is digital privacy coming to an end?

Marcelo Fernandes
Software Engineer
Wellington, New Zealand
marceelofernandes@gmail.com

I. Introduction

The United Nations declaration of human rights [1] defines and recognises the right to privacy in Article 12. Without doubt, digital databases containing personal information are within the scope of Article 12 and should, accordingly, be managed with high standards of privacy protection. In reality, privacy protection is continuously challenged by new technologies as companies fail to safeguard their data from malicious activities. The financial urge to capitalise on personal data contributes even more to the issue of privacy protection as the success of data-driven businesses becomes a catalyst for commercialisation of consumers' sensitive information. The gathering of personal data seems inevitable, and this scenario poses the question: "How far are we from having a single technology that can, conveniently, expose details of our life, personality, interests, and health condition to *anyone* in the world?".

January 7, 2021

II. 'State of the art' in digital privacy violations

In Mark Zuckerberg's explanation regarding Facebook's business model [2], he states that Facebook is a 'free' digital service that capitalises on user-targeted advertising. In other words, users pay for the service by giving up their privacy. Zuckerberg also claimed that users prefer to see advertisements they are interested in. This claim aligns, to an extent, with a survey from Innovid on personalised ads [3] that found 43% of consumers agreed it was *important* that ads were personalised. However, when interviewees were inquired about the practices that lead to personalised ads, 83% thought it was unethical to track online activity to tailor ad customisation [4], and a mere 24% agreed that tailoring of newsfeeds was ethical. This survey manifests the growing disconnect between the way companies currently capitalise on users' data versus how users expect their data to be used and *sold*.

Moving from Facebook to Apple, in the current version of macOS ("Big Sur" - 2020), users cannot power their devices on and launch any applications without the system recording and transmitting a log with the user's activities [5]. Apart from not being encrypted, this log bypasses the device VPN and reveals, without asking for consent, users' geolocation along with metadata about which application the user was accessing and at which time. This level of surveillance means that, technically, Apple has the resource to know what you enjoy doing on your device at home, which apps you use for work, when you are at home, and when you are at work.

Additionally, both Facebook and Apple were revealed in 2013 [6] as members of the US military PRISM, a spying program that provides access to data within those member companies to the U.S federal police, without warrants. In 2019 alone, Apple supplied personal user data for at least 35,000 requests from the U.S government [7]. Additionally, Apple relinquished its intention to enable end-to-end encryption for iCloud – which would have enhanced users' privacy – after warnings from the FBI expressing their concern about not being able to properly investigate criminal devices [8]. Suffice to say that there is an evident existing threat to digital privacy when U.S government agencies can obtain records of users' messages, geolocation, financial details, and even their stored nudes.

One way to prevent digital privacy violations is by strengthening the law to hold companies accountable for data leaks. This requires careful evaluation as companies will try to divert their lack of security protocols to other matters, such as placing all the blame on hacker activists, as was the case in the Ashley Madison scandal [9, 10]. One of the problems of expecting the government to fix the situation, is that governments are lagging far behind when legislating for new technologies [11]. The U.S government, as an example, is still dealing with laws from the last millennium [12].

III. What the future holds

The current cases of digital privacy violations are already alarming, and the future does not seem to point to a better scenario. Having your email and name exposed by a data leak is an inconvenience. Having your social media profile pictures show up on a Google search is disturbing. Now let's add more information such as marriage status, nationality, date of birth, education, etc. With all this information, we now have a holistic view of your life. Such information can already be fetched if you are a celebrity, a famous public figure, or an important scientist, but how far are we from having a device that we could carry in our pockets capable of recognising strangers and displaying their personal information in real time?

For this device to be successful, it would first need to identify any individual with sufficient accuracy, from whatever information the device has access to. Facial recognition (FR) could be a way to achieve this, but FR alone wouldn't be

sufficient in all cases. If the individual is in a place without adequate illumination, or if they are too far away for a proper camera scan, FR wouldn't work properly. Therefore, in order to uniquely identify someone, the device would need to be able to capture more information. Other recognition techniques can also be implemented in the device to improve the recognition accuracy:

- Voice recognition (pitch, vocabulary, accent, etc.)
- Body Scan (height, weight, skin color, tattoos, etc.)
- Auxiliary gadgets detection (glasses, crutches, wheelchair, hearing aids, etc.)

Using these three techniques, the device might be able to uniquely identify someone, but there is more information that can be captured to reduce ambiguity:

- Geolocation (suburb, city, country, etc.)
- Devices carried that can be identified by wifi / bluetooth, computer vision, etc.

See [13] for a broader list of identifying features.

If this hypothetical device becomes a reality, it would need a central database to service this data. However, this database does not exist yet. Currently, multiple independent organisations (governments included), hold bits and pieces of individuals' personal data. Either these organisations would have to conspire to trade users' personal information, or some entity would need to convince people to handle their information, somehow.

Although it seems unlikely that this central database would become feasible on a global scale, it is plausible that locally concentrated and nation-wide databases could become the trend instead. As an example, China has been a pioneer in biometric data collection [14], whilst also allowing intrusive practices, such as letting companies monitor employees' brain waves for productivity [15]. Not only China, but the U.S has also been criticised for their lack of specific laws to protect citizens' digital privacy [16]. Europe too, has been criticised for their usage of biometric data to contain terrorists at the border [17].

IV. Conclusion

The solution for data privacy violations is a complex and extensive subject, and it was therefore barely touched in this writing. Instead, the focus was placed on the current threats against digital privacy, and how the future is likely to look. Even though the right to privacy is safeguarded by the United Nations, that does not mean it is in the best interest of corporations to also safeguard those rights; especially when their business models depend on it [3]. As more organisations become interested in the data-driven approach, more individuals' information is stored each day. With that, cyber attacks become more harmful and frequent, as the number of resources to exploit goes up. Looking into the future, though the threat of portable devices capable of recognising individuals and sharing their personal information might not become a reality soon, nation-wide databases containing personal data already exist and are already being used unethically by several entities. This scenario calls for awareness, and more people need to be brought into the discussion so that feasible solutions can be proposed.

References

[1] "Universal Declaration of Human Rights", Un.org, 2021. [Online]. Available: https://www.un.org/en/universal-declaration-human-rights/. [Accessed: 07- Jan- 2021].

[2] "Understanding Facebook's Business Model - About Facebook", About Facebook, 2021. [Online]. Available: https://about.fb.com/news/2019/01/understanding-facebooks-business-model/. [Accessed: 07- Jan- 2021].

[3] "Innovid — 2020 Consumer Attitudes on Personalized Ads", Info.innovid.com, 2021. [Online]. Available: https://info.innovid.com/2020-consumer-attitudes. [Accessed: 07- Jan- 2021].

[4] R. LLC, "The Dark Side of Customer Data", RSA.com, 2021. [Online]. Available: https://www.rsa.com/en-us/company/news/the-dark-side-of-customer-data. [Accessed: 07- Jan- 2021].

[5] "Jeffrey Paul: Your Computer Isn't Yours", Sneak.berlin, 2021. [Online]. Available: https://sneak.berlin/20201112/your-computer-isnt-yours/. [Accessed: 07- Jan- 2021].

[6] "NSA Prism program taps in to user data of Apple, Google and others", the Guardian, 2021. [Online]. Available: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. [Accessed: 07- Jan- 2021].

[7] "Privacy - Government Information Requests - Apple (US)", Apple Legal, 2021. [Online]. Available: https://www.apple.com/legal/transparency/us.html. [Accessed: 07- Jan- 2021].

[8] K. O'Flaherty, "Apple Halted iCloud Encryption Plans After FBI Warning—Report", Forbes, 2021. [Online]. Available: https://www.forbes.com/sites/kateoflahertyuk/2020/01/21/apple-halted-icloud-encryption-plans-after-fbi-warningreport/?sh=9ed55533688d. [Accessed: 07- Jan- 2021].

[9] K. Zetter, "Hackers Finally Post Stolen Ashley Madison Data", Wired, 2021. [Online]. Available: https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/. [Accessed: 07- Jan- 2021].

[10] "Ashley Madison Code Shows More Women, and More Bots", Gizmodo, 2021. [Online]. Available: https://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924. [Accessed: 07- Jan- 2021].

[11] "Government can't keep up with technology's growth", Harvard Gazette, 2021. [Online]. Available: https://news.harvard.edu/gazette/story/2019/02/government-cant-keep-up-with-technologys-growth/. [Accessed: 07- Jan- 2021].

[12] "Policymaking must catch up with technology - before it's too late", World Economic Forum, 2021. [Online]. Available: https://www.weforum.org/agenda/2019/11/we-must-bridge-the-gap-between-technology-and-policy-our-future-depends-on-it/. [Accessed: 07- Jan- 2021].

[13] V. Grout, "No More Privacy Any More?", Information, vol. 10, no. 1, p. 19, 2019. Available: 10.3390/info10010019 [Accessed 7 January 2021].

[14] "Biometric data collection by country: What's collected, how is it used?", Comparitech, 2021. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/. [Accessed: 07- Jan- 2021].

[15] "China is monitoring employees' brain waves and emotions — and the technology boosted one company's profits by $315 million", Business Insider, 2021. [Online]. Available: https://www.businessinsider.com/china-emotional-surveillance-technology-2018-4?r=US&IR=T. [Accessed: 07- Jan- 2021].

[16] "Internet Privacy Laws by US State: Does Yours Protect Online Privacy?", Comparitech, 2021. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/. [Accessed: 07- Jan- 2021].

[17] "EU border 'lie detector' system criticised as pseudoscience", the Guardian, 2021. [Online]. Available:

https://www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience. [Accessed: 07- Jan-2021].