Privacy in an AI world

What is actually at stake when losing our privacy?

Jan Rodríguex Miret

June 20, 2021

Contents

"Privacy is not about hiding our wrongdoings. It's about protecting ourselves from the possible wrongdoings of others."

- Carissa Véliz

1 Introduction

The world is driven by data. Big tech companies are gaining ground in the lists of most profitable companies and their tremendous influence in our societies is starting to rise concern among governments that are struggling to regulate the system. These companies seem to be everywhere already, but their role's weight is still much higher than what we imagine.

The way that these companies are using our data and the power that we are giving to them can have very negative consequences for the present and future world. It is not something new that this data can be exploited, sold, leaked, shared without consent, or misused, as it has happened many multiple times like in the Cambridge Analytica trial.

The reason why this issue has gained attention recently is also that this data-driven world has to deal with the development of new powerful techniques, especially in the field of big data, machine learning, and AI. If privacy alone is a big issue, it is further worrying when combining it with AI and many other ethical concerns that AI raises.

Figure 1 shows this increase of interest using the Google web searches of "Privacy" topic from January 2016 to June 2021. Note that of course, it is impossible to assess the real interest in a topic or a term, but this gives us a rough idea of its tendency. Significantly, there is a peak in May 2018 that corresponds to the GDPR enforcement.

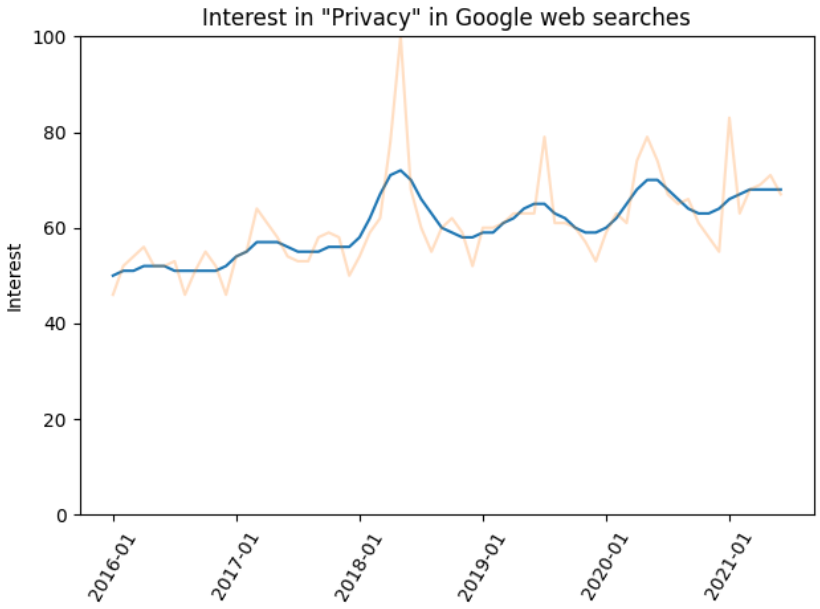

Figure 1: Worldwide monthly interest in the topic "Privacy" in Google web searches from January 2016 to June 2021. Results were smoothed using a gaussian filter with $sigma = 2$ to see clearer patterns (in blue). Source: author, with original data (in faded orange) extracted from Google Trends [https://trends.google.com/trends/explore?date=2016-01-01%202021-06-18&q=%2Fg%2F11fxvbm8wd].

Despite some increasing and recent efforts to shed light on the issue, people are not aware enough of what is actually happening. We cannot afford to not address this prob-

lem with the sufficient importance that it requires. We have to make sure that citizens understand the problem at hand, their responsibilities, and the consequences of not taking care of them.

For this reason, this document aims to clarify what is actually at stake when losing our privacy and what could be done to improve the situation.

First, it tries to contextualize the problem of privacy and AI in Section 2. Then, a deeper explanation on what are companies doing with our data and how they are doing it is introduced in Sections 3 and 4. Next, some regulations and the international interest in the topic is depicted in Section 5. Finally, some advice and a personal conclusion on the topic are presented in Sections 6 and 7.

2 Contextualization of the problem

Artificial Intelligence has suffered many highs and lows since its birth in the mid-twentieth century, where a period of incredible growth and investment precedes a loss of faith in the field and a withdrawal of resources. There have been 3 major cycles throughout history.

The first golden age of AI is usually considered to last from 1956 to 1974, with systems that were based on manually specified rules. These rules had to be defined by an expert through traditional conditional programming which sometimes required to extract meaningful features from the raw data. This approach was sufficient to create some sort of recognizable intelligent behavior in some rather simple tasks in a variety of domains like natural language or machine vision, among others. Many AI systems made use of heuristics to solve computationally unfeasible problems, especially in reasoning and planning. Also, the first and most simple neural network was introduced by Roosenblatt in 1958: the perceptron [6], although its applications were very limited.

These systems were very primitive and rather easy to follow. Engineers and designers had to specify exactly what to look for, meaning that they had complete control over what was going on and the model was predictable. Data was not easily available.

Then, after the first AI winter, came another flourishing period of success and development in the field, from 1980 to 1987. The backpropagation algorithm for efficiently training neural networks was proposed in 1986 by Hinton and Rumelhart [7], though connectionism was still lacking sufficient computational resources to create complex neural networks. Researchers started to gain more interest in using statistical methods to create these AI models, in what is called machine learning.

Machine learning models are built by applying statistics to a data set of samples and trying to distinguish the existent patterns in them. This kind of model, thus, relies on the data that is being used and the specific task that it is trying to solve. Again, features must be extracted in most cases to obtain meaningful results. The complexity of machine learning-based models can be much higher than a simple rule-based one, but still can be quite interpretable in some cases.

Finally, after another AI winter that lasted until 1993, resources invested in AI research just kept growing and growing. Computational power had been increasing at a tremendous pace (Moore's law), enabling new algorithms and techniques to be feasibly performed. In 2012, AlexNet made use of the backpropagation algorithm to train a deep convolutional neural network (CNN) using graphics processing units (GPUs). The model won the ImageNet Large Scale Visual Recognition Challenge and entailed a major improvement over previous techniques. This and many other breakthroughs further arouse the attention of countries and enterprises to invest in the field.

Since then, neural networks have become larger and larger, in what is called deep learning (artificial neural networks with many layers). The natural language model GPT-3 reached an astounding 175 billion parameters in 2020 [4]. Nonetheless, with this increase in model complexity, systems are treated as "black boxes" and are being evaluated end-to-end: giving some input and assessing the quality of the corresponding output but knowing very little about the internal steps.

In the case of deep learning the "black box" problem is more exaggerated compared to traditional simpler techniques. Moreover, it is intrinsic to the nature of artificial neural networks and how they work. The augmenting use of these AI-based systems in many fields and our daily lives is posing an also augmenting threat to society and mistrust towards AI.

Significantly, these systems are very powerful but they need even more data to achieve this high performance. However, data unavailability is no longer a problem with the irruption of the internet as we know it in the 1990s and the smartphone revolution of the mid-late 2000s.

Not just phones and computers broadly, but every application, web page, or smart device (like smart TV or smartwatch) is also generating a tremendous stream of information that can then be processed. These millions and millions of devices will keep expanding with the so-called Internet of Things (IoT) and the aggregation of future intelligent systems (e.g. self-driving cars, traffic lights, etc.).

But with great power comes a great responsibility that is not always fulfilled. And if data equals power, we better make sure it is in good hands.

3 What are companies doing?

So far, we have explained that companies are not behaving well and some of them have been banned for not complying with the law. But what is the real threat? Are these scandals often? These and other questions will be answered in this section.

Companies know more of you than even you do. They are using the data collected and using it to target you and provide you with more relevant advertisements.

That does not seem very scary. In fact, I would argue that it is even desirable. As a male, why do I want to be shown an ad about feminine hygiene? Some company is

investing money in something that is not useful at all. What if instead, I am presented with an ad for the next concert of my favorite artist? That would be of my interest for sure.

The problem is not exactly that. The problem is that we have reached a point where we are no longer in control of the situation, not even them (the companies with large amounts of data). We cannot be sure of how is our data exploited and what are their true purposes.

Companies are not just using data to give us better ads, but to influence us, to make us believe in certain things. Basically, we have become their product.

Most of the services and applications are shifting to be free to use. Think of all the things that you can do with a mobile or computer without having to pay. Do you pay for being guided with Google Maps while on vacation? For being entertained or educated with Youtube videos? For knowing the affairs of your "friends" on social networks? No, it's all free.

Now, think about all that these services and many others can know about you. Up to what degree they know your interests. This is the real business that many companies are feeding from. Even if you pay for a service, like in the case of video-on-demand (VoD) services (e.g. Netflix, HBO) your data is still being exploited to death to keep you engaged.

Thus, many companies are now fighting for your attention. More attention means more data. All their algorithms are aimed at gaining either your attention or your money in the long term. And our society is not aware of that, at least not enough.

4 How are they doing it?

Companies have lots of ways to extract and exploit your data, which depend on the source of it. In fact, even if you are consciously fighting to get rid of this, it's nearly impossible to be completely free of this (and doing so may come at a greater cost).

For normal users, if managing a web browser, be certain that they will be using cookies to track you between sites and share information between them.

There are a lot of cookie types. Some of them enable functionalities to provide a "better" user experience, at the cost of providing them with more of your data and preferences. Similarly, mobile applications use internal variables that are sent and stored to be analyzed. Nowadays, there is not much difference between web and mobile apps, as frameworks are trying to get as much universal as possible to be more broadly adopted.

They can track the time that you have spent on a concrete screen, what you are doing in the app at every moment, and discover many interests and habits of yours (e.g. when you wake up or go to sleep). If they share this information among themselves, they can collaboratively create a profile on you.

Nonetheless, you are not much different from other users. For sufficiently large networks of users, these behaviors can be further aggregated and new patterns and knowledge can be discovered.

As discussed later in Section 5, the companies' own privacy is protecting them to be more controlled, and so we have no guarantees of what is being done with the data. Laws only ensure what kind of data has the right to ask an app and what data could be obtained automatically, but most services cannot be controlled very much as it is complicated to know what is really happening behind the scenes (not available to normal users).

5 Regulations and international interest

Laws, if well made, punish those companies and people that do not behave in what is best for society or what is fair. In this section, an overview and comparison of the regulations existing in three of the most powerful governments (the U.S., China, and the European Union) are presented.

Among the United States, China, and European Union, only the latter has imposed stricter measures to ensure that privacy becomes a reality. The General Data Protection Regulation (GDPR) was accepted in August 2016 and provides a set of laws enforced to ensure data protection and privacy for EU and European Economic Area (EEA) member states [1].

Among many restrictions, GDPR specifies how the data of the residents can be transferred and used outside the EU and EEA, how an organization should inform its users of the data that is being collected and its purposes, how can users reject its consent, and general laws on how to treat data (anonymously where possible), and the bans of not complying to these laws.

Regarding AI, the European Commission reached an agreement to regulate AI systems in an effort to achieve more trustworthy AI systems [3]. This regulation also states the bans to attend for the misuse of these technologies. The document is about AI in general but mentions the need for explainable and interpretable models.

Meanwhile, the U.S. lacks a general privacy or data protection regulation like Europe, but rather has state-wise ones. Some of them are more strict while others are loosely defined or do not have any specific regulation at all. One of the most advanced ones is the Californian Consumer Privacy Act (CCPA) from 2018 [2], which has some similarities to GDPR but is not so strict.

On the other hand, China is on the path of writing its own data protection regulations. Until recently, China has been resistant to it, but the rapid development of the country and the people's awareness of the issue are accelerating the implementation of new laws. However, they will be not as strict as in the EU's GDPR.

In the international panorama, only Europe is trying to enforce stricter laws on privacy and AI uses and responsibilities, while China and U.S. are not that much interested

because of the fight for AI supremacy, the business models implanted, and the benefits of having that information.

As can be seen in Figure 2, China's interest in privacy has increased a lot these recent months. Italy is one of the most interested countries in the topic in Europe: most EU states' interests are even below the U.S. curve (not shown). Note that it is an approximation based on Google web searches, and the fact that it is something relative from within the country does not reflect the real absolute interest, but it is useful to see the tendency of each country. The most prominent peak in Italy's interest coincides with the implementation of GDPR, in May 2018.

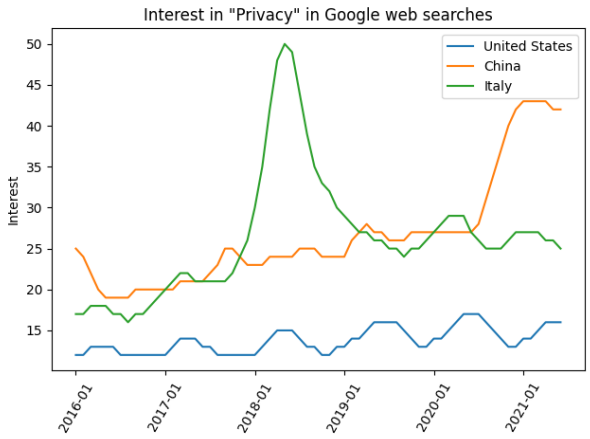

Figure 2: Monthly interest in the topic "Privacy" in Google web searches from January 2016 to June 2021 for U.S. (blue), China (orange), and Italy (green). Results were smoothed using a gaussian filter with $sigma = 2$ to see clearer patterns. Source: author, with original data (in faded orange) extracted from Google Trends [https://trends.google.com/trends/explore?date=2016-01-01%202021-06-20,2016-01-01%202021-06-20,2016-01-01%202021-06-20&geo=US,CN,IT&q=%2Fm%2F06804,%2Fm%2F06804,%2Fm%2F06804].

Despite the regulations and what governments enforce, it is important to emphasize the difference between what is illegal and what is impossible to perform. This is why we cannot just rely on these regulations to be made and take place, but we have to protect also by ourselves, as it is explained in the next section.

6 What should I do?

Once explained what companies are doing with our data and how, and what are some of the current regulations approaches, we can summarize what can we do to not lose the game against privacy and technology.

First of all, we are responsible for our data. As Carissa Véliz wrote: *when you expose your privacy, you put us all at risk*. This is because of the data aggregation and generalization of patterns that can be extracted using machine learning algorithms.

For this reason, I recommend you systematically reject all cookies that are not essential from the web browser. If they don't look for my well-being, it is better to keep your data away from them. Only accept to share more than essential data if you really trust the source and know what is behind it.

Diversifying our applications' parent company would be another great advancement to gain more privacy. Think of it, the tech giants offer lots of services and can aggregate your information on every one of them very easily: Amazon/Twitch/Prime Video, Google/Youtube/Drive/Maps/Android, Facebook/Whatsapp/Instagram, Apple/iOS/Mac, Microsoft/Windows. You may opt for other services even at the expense of fewer functionalities if they are not significant to you.

Since companies are fighting for our attention, it is very much a necessity to disable notifications on our smartphones. We already have enough trouble not getting distracted and using some of these apps that we even have to be prompted from time to time to please use their app. Enable only those that are essential. With that, we will get a much better quality of life and attention to what is really important (what we are currently doing).

Similarly, be careful about where you are signing up and unsubscribe from mail lists that only steal your time. If you reduce the time you give to an application, you are also giving them less information about you. It is especially important to not use your phone the first thing in the morning or the last thing at night, while eating, or whenever you go to the toilet. If not, you will find more difficulties in not getting addicted.

7 Conclusions

In this work, the reasons why privacy matters and why and how we should take back control of it are presented.

Privacy and new AI techniques pose a problem of balance between privacy and functionality. Between responsibility and power. Even if you think that your privacy is not of that much value (which of course it is unless you are a masochist exhibitionist), it's like all of us giving 1€ to the same person. It's only 1€ for you, but the receiver is getting very rich.

Nonetheless, it's time to abandon this irresponsible idea. Privacy is very important, as has been justified throughout the document. Think about what companies or governments can do with our data and how can they influence us if they know everything about us.

One thing worth mentioning is that the interest in Figures 1 and 2 is very bumpy, especially looking at the faded orange curve that represents the original data in (1). I think this resembles how humans think about privacy: it's something not present in our heads until a new big headline occurs in the news. After some concern about it, we eventually forget about it again.

Privacy is similar to other global-scale problems like climate change. They require

human collaboration, and laws to encourage and enforce it, but in the end, it's about every one of us being responsible, taking action on our own part, and calling to action to those who don't.

This becomes especially important when resources and investments to improve AI and data analytic techniques are an incredibly increasing trend. These technologies are the perfect example of a double-edged sword, and it is in our hands to rise awareness and understanding of the problem.

Companies, governments, and whoever has the data has also the power. Maybe to do something aligned with our interests or something that is not. It is possible they do it although (partially) illegal or not ethical. In the end, it is about trust in their responsibility and what they assure in their privacy statements, but it's a trust they don't deserve and that we must keep under control.

Acknowledgements

Thanks to the works of *Privacy is Power* by Carissa Véliz [8] and *21 Lessons for the 21st Century* by Yuval Noah Harari [5], apart from the Universitat Politècnica de Catalunya (UPC) and its professors, for opening my mind on this and other issues.

References

[1] General data protection regulation. https://eur-lex.europa.eu/eli/reg/2016/679/oj, April 2016.

[2] California consumer privacy act. https://www.oag.ca.gov/privacy/ccpa, June 2018.

[3] On artificial intelligence: A european approach to excellence and trust. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, February 2020.

[4] T. B. Brown, B. Mann, N. Ryder, M. Subbiah, J. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan, R. Child, A. Ramesh, D. M. Ziegler, J. Wu, C. Winter, C. Hesse, M. Chen, E. Sigler, M. Litwin, S. Gray, B. Chess, J. Clark, C. Berner, S. McCandlish, A. Radford, I. Sutskever, and D. Amodei. Language models are few-shot learners, 2020.

[5] Y. Harari. *21 Lessons for the 21st Century*. Spiegel & Grau, 2018.

[6] F. Rosenblatt. The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological review*, 65 6:386–408, 1958.

[7] D. E. Rumelhart, G. E. Hinton, and R. J. Williams. Learning representations by back-propagating errors. *Nature*, 323(6088):533–536, Oct 1986.

[8] C. Véliz. *Privacy Is Power*. London, UK: Penguin (Bantam Press), 2020.