DigiRights - the MOOC for your digital rights.

MENU

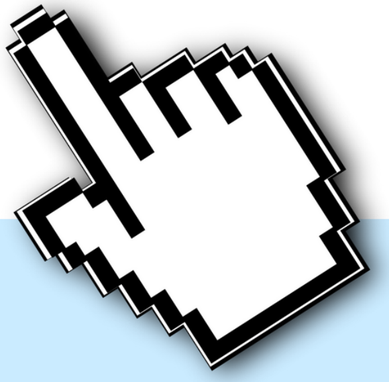
In today's society, the personal information has become one of the most important intangible assets for social platforms, including Facebook, Twitter, etc. These social media companies collect their user's data for both commercial and political purposes. Even though they have the data privacy policies to ask for the permission from the users before collecting user's online data, the process still remains vague. Therefore, most of the users still don't know how their data can be collected and used. This MOOC aims to make the audience:

- Understand how the user's data can be used for different purposes
- Understand how to read the data privacy policy of social media to know how user's data can be used
- Recognize different ways to protect user's data on social platforms

1 INTRODUCTION TO DATA PROTECTION AND THE MAIN SCANDALS RELATED TO IT

The point of the first session of the MOOC is make the audience aware of the importance of protecting their data and what are the derives of the use of personal information for tertiary use. The idea is that the students will realize the political and commercial impacts of their data usage and that after the first class, they will want to do more to protect their information.

Subject A: Cambridge Analytica



Subject B: Data used commercially

Subject A: Cambridge Analytica

Cambridge Analytica is a firm that offers services to corporations and governments for audience targeting. The aim of the company is to analyze a huge amount of consumer data in order to redirect the marketing material of their clients towards potential targets.
Cambridge Analytica was mandated for Donald Trump's campaign in 2016 and the company has been accused to use Facebook data of 30 to 70 millions of users without their consent. A subsidiary of Cambridge Analytica, Global Science Research, created a survey that was spread on Facebook. The data of those who answered but also of all their friends were given to Cambridge Analytica.

1 INTRODUCTION TO DATA PROTECTION AND THE MAIN SCANDALS RELATED TO IT

The point of the first session of the MOOC is make the audience aware of the importance of protecting their data and what are the derives of the use of personal information for tertiary use. The idea is that the students will realize the political and commercial impacts of their data usage and that after the first class, they will want to do more to protect their information.

Subject A: Cambridge Analytica

Subject B: Data used commercially

Subject B: Data used commercially

Facebook has given 61 other businesses the right to access data coming from its users. Among these companies figure Nike, Spotify, UPS, Hinge (a dating website), Amazon and Huawei. The idea behind those partnerships was to include some features of Facebook into the partner's device with, for example, the popular option to "connect with Facebook" to log in. However, it has been revealed lately that some of the partners have had access to privileged data: Netflix and Spotify got access to users' messages and Amazon got names and contact information. Facebook, in return, got more data that it used for the "You may also know..." feature.

Subject B: Data used commercially

Although this is in no way illegal, it is important that the users realize how much their data is spreading, especially since no consent was given for the previous examples.
Facebook is undisputedly the most data-rich platform considering the amount of information that users share through their profiles. However, the social media did not want to stop there: in 2019, Facebook launched the app Facebook Research, which enables the company to collect all the data (coming in and out through the Internet) on the phone of the users. Furthermore, Facebook has paid a monthly allowance of teenagers aged 13 to 15 years-old to access their data and sell it later on.

Subject B: Data used commercially

But it is not only social media that is to blame for the use of private information. In the United States, data from millions of patients of the National Health Service has been sold to big pharmaceutical companies. Companies such as Merck, Bristol-Myers Squibb and Eli Lilly have each paid the State for about 400,000 euros to have access to the data. The Departments of Motor Vehicles (DMV) (to whom you have to give your data in order to get your driver's license) has also been selling data to insurance companies and private investigators.

2

SIMPLE STEPS TO PROTECT YOUR DEVICE SECURITY ON A DAY TO DAY BASIS

The anonymity and lack of transparency that comes with the Web poses a real threat to your fundamental right of data protection and privacy. The first line of defence in data protection is at the individual level. Through this topic, we'll dwell into the basic first steps into keeping your data and devices safe.

A — Privacy Settings

B — Close down accounts you don't use anymore

C — Keep the operating system of your device & applications up to date

D — Be aware of Bluetooth and Open Wifi security

A&B

A:

Privacy Settings

Each social media account & app enable you to know the amount and type of information you are willing to share to not only your “friends” but also to the “public”. The optimal option is to choose the least amount of data sharing.

B:

Close down accounts you don’t use anymore

While Facebook, Instagram and Twitter remain the most used ones, there are many social networks that come and go throughout the years. If you have already signed up for one of them but aren’t using it anymore, close down the online service. They may hold copious amounts of personal data that you may be unwilling to share. When the services disappear, they still hold a right to the information which can then be sold as an asset.

C:

Keep the operating system of your device & applications up to date

Operating system updates have one major role, which is to better the functionality of the device with the recent advances. However, they also also update the device on a security level, which makes it vital to keep updating your operating system.

D:

Be aware of Bluetooth and Open Wifi security

While most home Wi-Fi are encrypted, public wifi is not. You thus encounter a high-risk of third parties to monitor your online activity. You can get protection against this through turning on your firewall and an updated malware protection. Bluetooth technology can also hinder your security & private data. This rule might seem simple, but make sure to always turn your Bluetooth off when not using it. There is al an “undetectable” mode which can be used.

3

HOW TO PROTECT YOUR DATA INFORMATION FROM THIRD PARTIES AND COMPANIES

Switch to other Search Engine Alternatives

Switch to other Browser alternatives

Use an Ad Blocker

Contain Facebook

Use a VPN

Switch to other Search Engine Alternatives

Google is ingrained in our daily digital habits as it is today considered as the best option in terms of search results. However, other search engines such as Bing or DuckDuckGo. DuckDuckGo is an Internet search engine whose primary goal is to protect consumers and individuals private data, while avoiding the “filter bubble” or personalized search results. Compared to Google or other search engines, DuckDuckGo doesn’t profile it’s users and shows all of them the same results. The best part about this alternative is that it enables you to conduct specific searches on other engines as well. You can still use Google, but this will help you minimise the amount of data that you give to one single company.

Switch to other Browser alternatives

Statement by the CEO of Mozilla: “Google is so close to almost complete control of the infrastructure of our online lives that it may not be profitable to continue to fight this. [...] From a social, civic and individual empowerment perspective ceding control of fundamental online infrastructure to a single company is terrible“.

As exemplified in this quote, Google Chrome has a myriad of ways to access our data to the power of Google on the Internet. Their market-leading browser has a monopoly and supporting Google Chrome would further cement that position. It is thus essential to look at other sources such as Firefox, Brave or Opera. Most of these browsers, in opposition to Google Chrome, come with a built-in privacy protection

Use an Ad Blocker

On all browsers (including Chrome), there are plugins that can be installed which will block ads, trackers and malware sites. To supplement them, there are a couple of other privacy plugins that can help in the prevention of unsolicited tracking online. These include Privacy Badger, developed by Electronic Frontier Foundation, a non-profit organization defending digital privacy and innovation.

Contain Facebook

Facebook, WhatsApp and Instagram are a triptych that has become hard to overturn as it is essential element for work & social networking. A few browsers such as Firefox enable you to create “containers” through the use extensions. How do they work? They create an isolated bucket which separates Facebook from all the other browsing you do at the same time. They can be used to isolate any website. This doesn’t mean that Facebook gathers no data, but it implies that they don’t have the ability to tie the date they receive to any other purchasing pattern perceived in yourbrowsing behavior. All the information they collect is thus restricted to their own apps which provides you with a security net against pervasive security threats.

Use a VPN

A VPN has the ability to make your Internet browsing private as it cannot be accessed by anyone who has access to your router. This can particularly be useful if you live in a shared property, with other roommates and have to share your Internet connection. This could be also empower people living in oppressed areas, as it enables them to circumvent the geographic restrictions placed on them.