STRATEGIES TO PROTECT YOUR PRIVACY

Most apps and digital services that we use daily collect personal information about us. With this data, these companies can create a comprehensive profile of us.

In case this company is hacked or it doesn't strictly adhere to the privacy rules, it is possible that all this personal data is made public at once.

One of the ways to ensure that in the case of a data leak, 'only' a part of your data is made public, you can use alternative applications and services.

In this brainfood, we provide some general tips and tricks you can take into account if you want to make your data more secure against all-comprehensive surveillance by companies or governments and/or all your data being made publicly available by a single data leak.

Knowledge Centre Data & Society (2021). *Strategies to protect your privacy. brAInfood of the Knowledge Centre Data & Society.* Brussels: Knowledge Centre Data & Society.

1. Don't put all your eggs in one basket

Large technology companies often offer an app for every service you can imagine: e-mail, (online) presentation and word processing, (navigation) maps, photo storage ... Often these different **services are connected** so you can easily switch between them and share data. Although this is useful for the user, it is also a way for these companies to diversify the data they collect about you. This way they can make **a more detailed profile of you**.

This always up-to-date profile can be used by companies to **advertise in a more targeted way**. It can also be used as a means to **follow population groups** and **exercise (social) surveillance on citizens**. In various places in the world, companies, whether or not mandatory, share the data they collect with their governments and intelligence services. In addition, if an attacker hacks the company where you have your profile, all the data in your profile can also be made accessible to cyber criminals.

One way to ensure that one company does not have the possibility to set up a total profile of you, is by using a**pps and services from different companies for different functions** (e.g. e-mail via Outlook, cloud storage via Google, ...). In short, to better protect your personal privacy: do not place all your 'data eggs' in one 'company basket'.

2. Be aware of the walled garden.

By offering different services, there's no need anymore to make a separate account with different companies for every service. This way the company can use data from one service to make appropriate recommendations in another service, which can be very practical. For example, the address of an appointment in your agenda can be automatically imported into the navigation software of the same company.

These companies know that this can be a significant added value for the user. They will therefore not make data that they have about you available in an accessible file format, making it more difficult for other companies to integrate that data into their software in the same way. Companies increase your **ease of use** by integrating a wide variety of data and thereby increase the chance that you continue to use the different services of one company. But at the same time they increase the risk that in the case of a **data leak**, all this personal information is made public in one instance.

3. Do your own research.

If you choose to use apps or services from a particular provider, it is worth taking a look at the **company's data and privacy practices**. These documents are often very extensive and contain many legal terms that are not accessible to everyone. They are also often written in such a way to mislead you by invoking a sense of trust.

Another way to do research is by searching for the name of the company or the service followed by terms such as "hacked", "privacy" or "data protection". This way you can find out more about problems or praise about the privacy- and data practices of the company. This is, of course, no waterproof solution. As with everything you read on the internet: **stay critical**.

General tips and tricks:

1. If possible, use apps that are **open-source** instead of apps whose source code is secret. With open-source software, the (source) code is publicly accessible. This gives people (e.g. users, security- and privacy experts) the ability to check the operation of the app. This way you can check whether the app is safe and privacy-friendly or not.
2. Not everything needs to be digital. You can also protect your privacy by keeping certain functionalities **analog.**
3. Provide your own privacy by default: the GDPR mandates processing managers to organize their processes in such a way that the most privacy-friendly options are set from the outset. This is not always the case. However, many applications allow certain data (e.g. the use of location data) not to be processed. If you don't want certain data to be processed, consult the **privacy settings** of the service and, if possible, turn off this data processing.
4. Do not **use the same identity everywhere.** Many apps or services nowadays use 'Log in with your Google/Facebook account', so you can create an account with one click and can log in. By doing so, you give (implicit) permission to exchange your data between the company where you register, and Google/Facebook. This way, both companies can make microtargeted use of your data. If you create an account on the basis of your email address, you can (in many cases to some extent) prevent this.

brAInfood of the
Knowledge Centre
Data & Society