TOOL – PERSONAL DATA AND DIGITAL IDENTITY

COMMUNICATION & COLLABORATION > 2.6 MANAGING DIGITAL IDENTITY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
Facilitators	N/A	Level 1	Preparatory guide	Creative Commons (BY-SA)	English, French

This document contains background information for facilitators before they run the workshop with participants. It helps understand how surfing the internet leaves a digital footprint which becomes one’s digital identity.

General Objective	Knowledge acquisition
Preparation time for facilitator	less than 1 hour
Competence area	2 - Communication & collaboration
Name of author	Samantha Giordano
Resource originally created in	French

WORKSHOP DIRECTIONS

1 What is personal data?

The EU's General Data Protection Regulation (GDPR) gives the following definition:

> Personal data are any information which are related to an identified or identifiable natural person.
>
> The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.

However, we should not confuse public personal data that may be visible and potentially sold to a third party (email addresses, purchasing habits…) and private personal data that should be protected at all times (bank account details, social security number…).

2 How are they collected?

Cookies and involuntary traces

Every time you connect to the internet, you leave traces online, often without necessarily wanting to or even realising you are doing so. These traces are numerous and varied: your IP address, your location, your computer's OS, your browser history, and more. But these are also personal information such as your habits, your fashion preferences, your interests, language, health, etc.

All traces contribute to profiling you and creating the most accurate portrait possible of your digital person. The objective is to offer you the most personalised possible online experience, but mostly for the purpose of adapting advertising to your profile. For example, if you search for a new couch, you may at later point see ads popping up for…couches!

These data are collected using what we call cookies. These are small text files containing information about a user's profile and internet use habits: their username for a site or the contents of their shopping basket for example.

Although cookies have often been seen as controversial, they do not have malicious intent – they are neither spyware nor viruses. As you arrive at site, you can easily indicate your preferences regarding cookies. However, for some sites, cookies are necessary – if you want to use these sites, you will need to allow cookies.

For more information, see Wikipedia.

Aside from involuntary traces we leave while using the internet, there are other, similar kinds of data. These are information we might find online concerning ourselves but that we did not post directly. An example of this would be a photo posted by a friend on a social media site, or an article featuring our name.

Voluntary traces

These are data we choose to post online directly. These can be photos, employment information, your website, likes on social media, reviews on retail sites, etc.

These are typically traces visible by others (think of your employer for example). We should therefore beware of what we post, particularly as these types of data are not always easy to erase and/or manage.

3 What are they used for?

Personal data have many uses, some of which are clearer than others. Firstly, they can be used simply to identify you online via your username or email address, to make orders on retail sites for example. But the abundance of such data have developed a highly lucrative online market.

Essentially, data harvesting companies can use what they collect for commercial ends, even selling them to advertisers. These advertisers can use the data to better target ads at users. Most apps that you install will regularly collect your data (log in email, photos, location, etc.). Contrary to what we might think, the sale of personal data is not illegal, in the sense that they are collected according to rules established by the GDPR. For more on this subject, see this video, which explains it quite simply.

Don’t forget…if it’s free, you are the product! Free sites need to be able to finance themselves. Selling personal data is one way to do this.

Other than advertising, personal data that contribute to your online profile are also a means to target propaganda. This can happen in certain cases when political parties propagate certain content adapted to their electorate. Recall the Cambridge Analytica scandal! In this case, the company harvested the data of more than 50 million Facebook users in order to categorise various profiles and target content adapted to these, which ultimately had an effect on the outcomes of the 2016 US presidential election and Brexit campaigns.

4 Personal data and digital identity: what's the difference?

The difference between personal data and digital identity is minimal in the sense that our digital identity comprises our data. Personal data establishes, to varying degrees of accuracy, a snapshot of who we are: what we like, what we do, where we live, who are friends are, what are jobs are, etc. In a way it is similar to an identity card.

There are however, several notable differences between civil identity and digital identity:

- You can choose your online identity. There is no obligation to be held to any administrative reality: you can replace your real name with a username, use a fake address, alter your appearance with image editing software, etc. You can often see examples of these on social media platforms for example.
- You can have several identities. Contrary to our civil identity, on the internet you are able to create unlimited profiles: one for Facebook, another for Instagram, four more on Reddit, etc.
- Your digital identity is progressive. Keep in mind that your taste, opinions, and appearance will evolve over the years. However, the traces that you leave will remain. If you upload a photo of you today, will you still be okay with that being accessible in x years to come?

All visible information that you leave online comprises your personal identity and thus contributes to your ‘e-reputation’. This is the image that others perceive of you. This is why it is necessary to pay attention to what you put online. The image that one person has of you will not necessarily be what you had imagined or intended. This effect is exacerbated by the web whose memory is vast and from which traces are difficult to erase. Think before you post.

5 Why protect them?

First, know that protecting your personal data is not an obligation. However, we recommend you be aware of how you can do it.

Leaving too many visible traces increases the risk of data and/or identity theft. During recent years, scammers have developed many new ways to steal information:

- Phishing: for example, a mail comes from your bank inviting you to log in. This is in reality a fake site built to trick the user into handing over important personal data.
- Pharming: hackers will exploit security issues in certain sites to steal user data. Don’t panic though – this happens relatively rarely.

Your online presence also makes you susceptible to acts of cyberharassment. For example, anyone that has access to our data (images, content, posts) can choose to harm us in various way, for example:

- By stealing our identity. A person can for example create a fake profile on social media using your data.
- By directing hate speech towards you. This can be in the form of threatening messages, insults, hate incitation, etc.

- By revealing personal information. Known as 'doxxing', this consists of revealing personal information such as real name, home address, etc.

6 How do we protect them?

Simple gestures

There are many simple and quick tips to establish in your routine to protect your personal data and by extension your digital identity:

- Change your browser's security settings*
- Change your social media privacy settings*
- Change your mobile app settings, and delete the ones you don't use
- Give the minimum amount of personal information required. Only fill in obligatory fields when creating a profile, for example.
- Search for yourself regularly. The objective here is to be aware of what others may see of you online.
- Create strong passwords and change them regularly
- Think twice before posting content online

Legally

In order to protect our personal data, the European Union enacted the General Data Protection Regulation in May 2018. This applies to all citizens of the EU. It gives citizens more control over the data via various mechanisms such as the requirement to give positive and explicit consent to receive cookies. It also confers the 'right to be forgotten', meaning that anyone has the right to have their personal data be deleted from a given platform. The GDPR comprises many articles detailing citizens' digital rights and the obligations of corporations. See more information here and here.

Here are the main principles:

- Right to access. If an organisation (bank, website, social media platform…) retains information on you, you can ask them to give it you. This means you can control your data, correct it or delete it.
- Right to correction. This follows from the previous. If we notice that some information concerning us is wrong or incomplete, we can ask for it be rectified.
- Right to object. This regards the ability to object at any time to an organisation using our data for a

particular aim. For example, we can ask to no longer receive ads from a particular company.

- Right to be forgotten. This would involve for example asking a search engine to remove or hide information concerning us. Keep in mind however that this does not mean that the content itself is deleted.

To conclude, on the internet as with anywhere else, it is important to respect others and to not discriminate against them. Don't forget that all comments and discussion leave traces! In addition, keep in mind that you cannot distribute photos or videos linked to an individual's private life without that person's consent. This is what we call the right to privacy.

For more on the subject of online rights and particularly regarding sharing and reusing, see Digital Commons #1: Right to Use.

* You can also use a browser like TOR which protects your personal data by default.

7 Glossary of Terms

- **Cookies**: Files containing information on us, collected during our visit to a given website (username, email address…)
- **Cyberharassment**: Form of harassment that takes place online. Can occur via phone, chat, games, social media etc. It can take many forms from mockery to threats to spreading rumours. **If you are the victim or harassment, speak to an adult and don't hesitate to register a complaint!**
- **Defamation**: The action of deliberately damaging someone's reputation. This can be in the form of racism, homophobia, sexism or other.
- **Digital identity**: Traces we knowingly leave online: photos, comments, but all posts of other users in which we are cited. Any information with which we are directly associated.
- **Digital trace**: Saved information regarding a user's identity.
- **History**: Saved in a file or database, this comprises a user's known online activity.
- **Identity theft**: Stealing someone's information for example to buy things or scam others.
- **Image rights**: That pertaining to our right to oppose the distribution of photos, videos, etc. in

which our name appears.

- **Password**: Used to access a personal account. For more security, use a variety of character types, such as upper- and lower-case and special characters such as @, !, ?...
- **Personal data**: All information relative to a person contributing to their identification (name, address, phone number...). Contrary to digital identity, these are data that are not publicly visible and that can be used for commercial ends.
- **Right to be forgotten**: Right of internet users to request that data concerning them be deleted. See here.
- **Phishing**: Technique used by scammers to steal personal information. These people may try to create a fake version of your bank's website and encourage you to log in there, thereby gaining access to your details.
- **Privacy policy**: A kind of contract that explains how a site treats the data supplied by a user.
- **Private life**: Involves any and all activities concerning information on a person's life they may not wish to make public, e.g. on their family, health, etc.
- **Right to be forgotten**: Right of internet users to request that data concerning them be deleted. See here.
- **Social media**: Online platform that facilitates relationships between users. These sites allow users to communicate with friends and groups that share the same interests. The most popular are Facebook, Twitter and Whatsapp.
- **Transparency**: The concept of using simple and clear terms leading to the easy understanding of a policy or rule. It also involves making users aware when there has been a policy change.
- **Virtual life**: The life we create online (for video games, social media, etc.)