MIRROR MIRROR, WHAT DO YOU KNOW ABOUT ME?

COMMUNICATION & COLLABORATION > 2.6 MANAGING DIGITAL IDENTITY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
All, Job seekers, Low literacy citizens, School drop outs	Adults, Elderly citizens, Teenagers	Level 2	Activity sheet	Creative Commons (BY-SA)	English, French

Using online tools (Yasni, Webmi) or simply by doing basic research on Google, this activity allows the educator to raise awareness of good online practice in order to secure and control the information available about ourselves online.

General Objective	Awareness building
Preparation time for facilitator	less than 1 hour
Competence area	2 - Communication & collaboration
Time needed to complete activity (for learner)	0 - 1 hour
Name of author	Marion Piecuck
Support material needed for training	Computers-and/or tablets-Internet connection
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Introduction

This workshop considers notions of personal identity and personal data protection. Through a role-playing game, participants will be led to search for a large amount of information online, which will help them consider behaviours to adapt while using the internet to improve the safety of their identity.

Facilitation tips: It is recommended to test the tools and sites in advance of the workshop, verifying **your own information**: the group members **will likely try entering your name**. **Ensure that you have protected what you need to protect in advance – for this, use the advice given in part 3**. You may also need to check information concerning participants to be sure that nothing serious will be 'discovered' if for example a participant 'stalks' another during the activity. Pay attention to the effect this activity has on the group while this activity is going. Don't leave it go on for longer than 20 minutes. In order to be on point, refer to 'Personal Data: Keeping Track'.

2 What is personal identity?

We recommend that you start with a short discussion. Start by asking how they would define identity. Note the answers on a whiteboard/flipchart (this will allow them to visualise the main points of the discussion). Answers will likely be things like name, age, personal experience etc. You can introduce the idea of the shifting nature of identity: it is not something fixed.

We are not the same person as we were yesterday, and we will not be the same tomorrow, depending on our experiences. Ask: *do you think your identity stays the same for your whole life*? If needed, give examples (an experience may stir your interest in something you were never interested in before, a meeting or a conversation can change a point of view you had that had previously been seemingly fixed). Refer to the multifarious nature that identity can have: we may perceive someone differently than someone else will perceive that person. Identity is made up of fractured perceptions. All of our identities, personal, social and cultural, have a digital identity depending on the traces we leave online. That is your '**digital persona**'. Ask participants what kinds of information they leave on which sites. Note their responses on the board. The answers will be as follows:

- Types of information: comments, photos, likes, etc.

- Types of sites: Facebook, Instagram, YouTube, forums, blogs, retail sites, etc.

This information is indeed public data (related to 'publication'), as opposed to private personal information (information we give when we make an online purchase, for example). Make an example of a particular Facebook account, what music and films the account holder likes, what they are interested in, their friends, etc. (**The account holder should have given their permission/use a profile of a public personality, Mark Zuckerberg for example**).

What is the difference between personal data and digital identity? Personal data are personal information you give when you sign up to a social media platform, or when you make a purchase online, for example. These are data that are not visible to everyone but which are used for commercial purposes, to facilitate targeted advertising, for example. Digital identity is all the traces you leave knowingly: photos, comments but also others' posts in which you are tagged, all information to which you can be associated personally or via a third party. Your digital identity is everything that can be seen about you online by other users.

3 How others perceive us

Ask for a volunteer to showcase their Facebook profile (or Twitter, or Instagram, according to the participants' ages and use habits). Don't show it at first, only ask if, according to them, their profile corresponds to their IRL ('in real life') identity. Ask participants if the image of themselves they present via their social media presence reflects their actual personality. Without revealing everything, they can answer briefly.

Now move to others' perceptions! Open the volunteer's profile. Go through it together using a projector. The others will watch and write what they perceive. Guide them if needed. What are this person's interests — what they do in their free time? What do you notice about their personality? Who are their friends and family? These are just some elements to explore! When everyone finishes taking notes, discuss the results. Everyone, in turn, should read out and make an argument for what they wrote. Allow the volunteer to react to each impression. If you have time, repeat the process with other accounts (Instagram or Twitter for example). Compare these to get a sense of whether the person presents themselves in the same way, gives the same information and the same impressions across the different platforms. This kind of consideration can lead to rich debate!

4 Stalking workshop

This requires a computer and internet connection per participant. Each person will evaluate their digital identity by searching on the following: • Google • Webmii http://webmii.com/?language=fr. Not particularly distinct from Google but the site is well-designed.

• Yasni http://www.yasni.fr/. Not particularly attractive but on which we sometimes find surprising results.

• Google images

• You can also share this link which details how participants can download their Facebook data: https://www.facebook.com/help/1701730696756992/?helpref=hc_fnav Leave group members time to go over what they find and ask them to list different types of information they will need to search for. Write them on whiteboard/flipchart so they are readily available during the activity:

• Data shared voluntarily (0 point) • Data once shared voluntarily but are now a source of shame or no longer correspond to our identity or how we present ourselves (2 points)

• Data shared voluntarily but which has been reused in another context by an individual or website (3 points)

• Data shared by which should not be accessible publicly (private data that is now public) (4 points)

• Data shared by a third party with the the user's consent (1 point)

• Data shared by a third party without the user's consent (2 points) • Data shared by third party in an instance expressly unwanted by the user (4 points)

This activity should last maximum 20 minutes; if it's not finished, not to worry. Each player will start with 50 points, from which they will subtract the numbers corresponding to the types of information as outlined in the list above. Do not subtract points for the same information found more than once via different sources. After, the group should compare their scores. Participants will quickly realise certain things themselves, for example, that accounts in their name, using their Instagram details have been recreated ex nihilo. This indicates a reuse of public data and shows why it is important to pay attention to our accounts' privacy settings. We will focus on this in the third part of the workshop. Another example: likes on social media (Facebook, YouTube, etc.) are public data. You consented to this by signing up. Don't think of it like private data becoming public, but rather something you posted but

hope that people won't come across.

There are three types of traces, of which two concern issues of digital identity:

- **Voluntary traces: what we say about ourselves**
- **Inherited traces: what others say about us**
- **Involuntary traces: what systems retain about us**

It is therefore useful to pay attention to how the mirror of the internet reflects us and our public data. But this digital identity becomes more difficult to apprehend (and thus to control) the longer it has to evolve, not necessarily based on our identity itself but more on how computer memory and IT tools reflect us over time. This is more or less random and controllable to some extent. It depends, amongst other things, on how search engines operate and the way they archive data. In other words, influencing or controlling how our information is used is a complex and difficult issue.

Facilitation tips: You can give a personal example here which will create a link between you and your audience and encourage them to share discoveries they may have found surprising. When you searched for yourself on Google or Webmii, for example, you came across a comment that you left on Craigslist on a listing for a tent for sale, asking if it would be suitable for you and your romantic partner camping in a winter environment. No one outside Craigslist needed to know that. This example will serve to get across that everyone leaves traces.

5 Variant

You can also facilitate the activity as a role-playing game: Here is a 'catastrophic scenario': the government decides to categorise citizens based on their digital identities. Participants will use Webmii, Yasni, Google (Images), Facebook and other platforms to determine whether their citizenship is in danger. The idea is not to fall into line, but once again, to learn how complicated it can be to influence and even control our personal identity. This will be based on a new scoring system, which differs slightly from the one used previously.

Participants are going to use a marking scheme different from the one previously described: **'What category will you fall under?'**

• Data shared voluntarily (+ 2 points)

• Data once shared voluntarily but are now a source of shame or no longer correspond to our identity or how we present ourselves (- 2 points)

• Data shared voluntarily but which has been reused in another context by an individual or website (- 3 points)

• Data shared by which should not be accessible publicly (private data that is now public) (- 4 points)

• Data shared by a third party with the the user's consent (+ 1 point)

• Data shared by a third party without the user's consent (- 2 points)

• Data shared by third party in an instance expressly unwanted by the user (- 4 points)

The objective for the facilitator here is encourage debate regarding information that circulates about us online without our consent, or at least without our knowledge. Remind the group that in some places, this has categorisation scheme has already been implemented, such as in China.

6 How can we control our data?

Anticipation

- Change the settings on our account to strengthen privacy (see annex)
- Keep different aspects of your digital identity separate

It is important to be aware that we have several digital identities online, belonging to different communities: professional, private (family, friends), artistic/hobby/pastime (e.g. for an artist who manages a blog on modern art or who paints) In this way, you can use **pseudonyms** (for a Facebook account for example, or to join a forum on Indian folk pop). Therefore, a link will be difficult to make between the administrator of VashundaraDasOfficalFanclub and Fred Hobson if a professional colleague searches for the latter.

Maintenance

- Verify regularly by repeating the previous activity and by checking different sites
- Contact the sites that host information you no longer want to appear and ask them to delete it (you will sometimes need to insist that they are obliged!) In the context of EU law, see the GDPR and the right to be forgotten.

All sites need to make their privacy policies transparent (see Google's in annex, for example). Finally, have a general discussion to conclude. What have they understood? What have they retained? Emphasise the key ideas again. The objective is that you have developed participants' awareness of the subject.

Facilitation tips : The idea is to move users from characterising themselves as 'victims' offering up their data to informed agents conscious of their activity online and feeling more in control of their data.

7 Going further

Resources for the facilitator to better understand the idea of digital identity:

- https://en.wikipedia.org/wiki/Digital_identity
- https://www.sciencedirect.com/topics/computer-science/digital-identity
- https://www.researchgate.net/publication/266146567_Digital_identity_and_Teachers_Role_in_the_21st_Ce

Further educational material

- https://www.commonsense.org/education/digital-citizenship/topic/digital-footprint-and-identity

More information on securing our information on Facebook:

- https://mediasmarts.ca/lessonplan/privacy-and-internet-life-lesson-plan-intermediate-classrooms

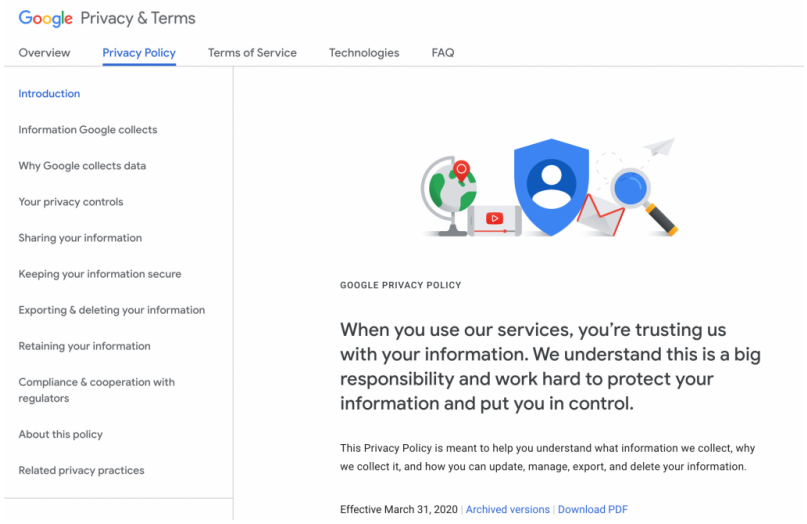
Activity on digital identity (for 11-14 year olds)

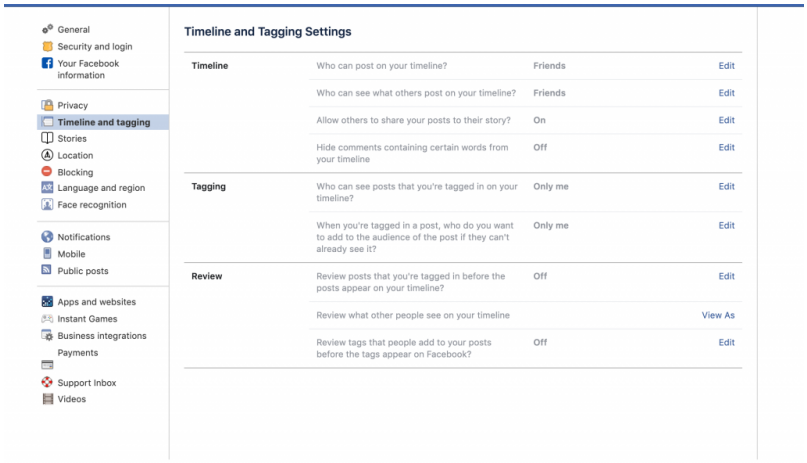
- https://mediasmarts.ca/teacher-resources/your-online-resume

Prominent non-profit organisation defending digital privacy

- https://www.eff.org/

8 Annexes


Google Privacy & Terms
Overview
Privacy Policy
Terms of Service
Technologies
FAQ
Introduction
Information Google collects
Why Google collects data
Your privacy controls
Sharing your information
Keeping your information secure
Exporting & deleting your information
Retaining your information
Compliance & cooperation with regulators
About this policy
Related privacy practices
GOOGLE PRIVACY POLICY
When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.
This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.
Effective March 31, 2020 | Archived versions | Download PDF


General
Security and login
Your Facebook information
Privacy
Timeline and tagging
Stories
Location
Blocking
Language and region
Face recognition
Notifications
Mobile
Public posts
Apps and websites
Instant Games
Business integrations
Payments
Support Inbox
Videos
Timeline and Tagging Settings
Timeline
Who can post on your timeline? Friends Edit
Who can see what others post on your timeline? Friends Edit
Allow others to share your posts to their story? On Edit
Hide comments containing certain words from your timeline Off Edit
Tagging
Who can see posts that you're tagged in on your timeline? Only me Edit
When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it? Only me Edit
Review
Review posts that you're tagged in before the posts appear on your timeline? Off Edit
Review what other people see on your timeline View As
Review tags that people add to your posts before the tags appear on Facebook? Off Edit