THE BIG QUIZ: PRIVACY ONLINE

SAFETY > 4.2 PROTECTING PERSONAL DATA AND PRIVACY

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

This workshop in the form of a quiz is an opportunity to review and deepen the knowledge and best practices seen during the workshops dedicated to personal data. It would therefore be more prudent to have done those workshops or at least make sure participants are familiar with that kind of knowledge before conducting this quiz.

General Objective	Knowledge acquisition
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Time needed to complete activity (for learner)	0 - 1 hour
Name of author	Nothing 2hide
Support material needed for training	Bristol board of 5 different colours Pens
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Introduction

This is meant for those who have already taken part in one or several workshops on the theme of personal data and digital identity. Think of it like an oral test but in the form of a quiz. There will be two rounds. The first is series of true or false question. The second comprises four themes: 1) Social Media 2) My Life, My Rights 3) Below the Radar and 4) Smile, You're on Camera. Beforehand, copy the questions on stiff coloured paper. The ideal would be to have five different colours, one for the first round, four for the second (corresponding to various themes). Divide participants into 2 groups.

Note to facilitator: You can also just display the questions using a projector or adapt them as you like.

2 True or False

Ask each group a question by turns until no questions remain. Every group must simply respond true or false. **Facilitation tip**: To increase the pressure, allow just 10 seconds to respond (the opposing team can keep time). You can give come extra detail when giving your response. Every correct response is worth one point. Write down the points at every turn to keep track and maintain the spirit of competition to encourage participants.

Question 1 – Using Tor is illegal False. It was developed for use by the US military – the Marines in particular – to hide their IP addresses and avoid the leaking of mission-sensitive data. Once the military moved on to internal VPN systems which provided even more effective anonymity, Tor was made free and open. It is therefore totally legal to use or download.

Question 2 – Using WhatsApp, your data is protected True – WhatsApp, and so the team at Facebook who runs the service, can not read the messages (which contain personal data).

Question 3 – Using WhatsApp, your metadata is protected False – Facebook has access to metadata. This refers to everything surrounding data itself – in this case that would be elements such as the numbers of the sender and receiver, the time of sending etc.

Question 4 – There are two main ways that hackers break passwords. By dictionary or Arabic characters. False – the two types are by dictionary or by brute force. By dictionary: a hacker has

millions of passwords in several files and a program that will try them one by one until the correct one is found. There are freely downloadable classed by languages, jobs, animals, years etc. By brute force: (this is no longer so frequently used and has been mostly supplanted by phishing) a program is used that will simply try every possible combination of characters.

Question 5 – Apple is more transparent than Android when it comes to collection and sharing personal data. False – Apple collects huge amounts of data. The company is even suspected of having collaborated with others such as Facebook to broaden their scope of collection.

Question 6 – Snapchat can retrieve your temporary messages/images. True – Snapchat harvests and locally stores metadata (data on data). These will allow expired photos to be retrieved. For more information, see this article from the Guardian.

Question 7 – You have the right to object to the automatic processing of your personal data. True: this is a fundamental right in many countries, such as for example in the EU. See recitals 69 and 70 of the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1 In the case the two teams are level in the end, flip a coin to determine the winner. Yes: life is sometimes just luck.

3 Four themes to determine a winner

The four themes are each assigned a Bristol board colour. The team that won the first round can choose the first theme. They answer all questions of this theme. Next, the other team chooses the next theme and so on. For each question, the group can answer directly or ask for the list of responses. If they answer outright, they gain 3 points. If they ask for the list of responses and get the correct answer from there, they gain 1 point. If they answer incorrectly, win nothing. Here are the questions by theme, with response.

Social Media

Question 1 – Am I obliged to give my full name when I create a profile? A – Depends on the site; the conditions for each should be checked separately B – Full name is required C – No we can use a fake name **Answer**: A – Depends on the site. Although many people will use pseudonymes, Facebook for example demand real names. Your account can be suspended if ever it is flagged and you cannot provided your real identity.

Question 2 – **How long does it take to read Facebook's terms and conditions?** A – One day ('way too long') B – 15 minutes ('If I had known, I would have read them' – no need to lie: no one here has read them) C – One hour ('pffft…maybe I could be convinced')

Answer C – One hour : so what are you going to do? Note that the the reading time is similar to that of other social networks. See this workshop roadmap we offer on Instagram terms and conditions.

Question 3 – Can you be fired for something you post on social media? A – No – my social media activity is my private life B – Yes C – Only if I personally attack one of my managers

Answer: B – Yes. Even if your account is personal, your public posts can be read by everyone, including by your employers. Several types of posts can lead to dismissal. Insults to your colleagues can be one of reason but there are many others. For example, an employee of a company makes it clear that they had left on holidays although they had taken sick leave. If their boss saw this they wouldn't appreciate it too much.

Question 4 – You live in Europe. Where is your Facebook data stored? A – In Ireland B – The US C – Cannot be determined

Answer: C – Facebook has data stored all over the world. Although the European headquarters are located in Dublin, we cannot be sure that that's where our data is located. EU law requires that data be stored either in the EU or the US according the the security agreement known as Privacy Shield.

Question 5 – Which of the following is true regarding Instagram? A – Instagram can keep your data, use it and share it with companies connected to its network. This includes your name, email address, school, where you live, your photos, your phone number, your likes and dislikes, where you go, where your friends go, how much you use Instagram, your birthdate, who you talk to as well as your private messages. B – Instagram can delete your posts without telling you why. C – When you delete your Instagram account, the network will retain your data as long as is financially expedient.

Answer: All of the above! See a clear version of Instagram's Terms of Use rewritten 'in plain English' by a lawyer.

Question 6 – What does it when a Facebook account is deactivated? A – In effect it is put to sleep but can be reopened at any time. Data is frozen but stays online. B – The account is frozen. If the user does not reconnect after 30 days, the account is deleted and Facebook deletes the data C – The data linked to the account is being verified after the account was frozen as a result of it having been flagged by another user.

Answer: A – It is put to sleep but can be reopened at any time. Data is frozen but stays online. When a user wishes to completely delete their account, there is a 14 day deadline during which they can return and reconnect before it disappears. Regarding answer C, this regards a suspended account.

Question 7 – When a Facebook account is deleted, how long does it take for the data associated with that account to be deleted? A – 9 days B – 90 days C – 9 months **Answer**: The account will be deleted in 14 days. Facebook leaves you a period of time – if you reconnect within 14 days, the account will not be deleted. However it takes a lot longer for your data to be deleted. According the company, it takes around 90 days to delete everything you published such as photos, status updates and other stored information (such as date of birth).

Question 8 – Instagram now offers users the option to download their data. What can you not find in the downloadable information? (3 points if all 3 are correct; 1 if partially correct) A – All the private message you exchanged B – Every post you liked C – Your search history **Answer**: All. Here is everything contained in your file: published photos and videos, private messages, all posts you have liked, your search history and dates you followed other accounts.

My Life, My Rights

Question 1 – What is the European body that protects online privacy? A – European Data Protection Superviser B – Directorate General of Communication, Content and Technology C – European Council Réponse : A – The European Data Protection Supervisor (EDPS) is the European Union's (EU) independent data protection authority.

Question 2 – You're moving to another country. You need to find a new place to live. As you're doing this, you decide to create a new email address. What should you do? A – Pick something easy to remember as it's just a temporary address. B – Use the password you use for your other address so as to not forget. C – Create a new password.

Answer: C – The longer it is, the longer it would take a hacker to break it. It is therefore recommended to make it complex but in a way that is easy for you to remember. See the workshop 'Creating Strong, Unique Passwords'.

Question 3 – What do we call the information – the personal data – we leave on the internet? A – Digital identity B – Social identity C – Elderberry imprint

Answer: A – Digital identity. Digital identity is the totality of online information concerning ourselves. It is therefore an identity comprised of data. As in real life (or 'IRL'), virtual identity is a mix of what you

want to show, what you want to hide, what you don't know is there, and what others perceive of you (such as when you think your neighbour is always annoyed although they are actually friendly but just don't happen to be constantly smiling!)

Question 4 – What can you do if Google displays a search result concerning you that you don't like? A – Nothing, nothing can be done against Google B – Complain (and be lose your case on trial) C – Ask Google to delist the page

Answer: C – You can ask Google to delist, but not to delete, the page concerning you. Google could not actually delete it – they do not have the power to do so. If they accept your request, the page will no longer appear in their search results linked to your name. Understand however that the page still exists – it will always be possible to retrieve it with other key words for example. This is a right that exists mainly in the European Union. This means that someone who searches your name outside the EU could still see the otherwise delisted result.

Question 5 – What do we call the right to demand that an organisation supply information concerning us? A – Right of Curiosity B – Right of Mastery C – Right of Access **Answer**: C – Right of Access. More information here. **Question 6 – Okay you get it now. You're creating different passwords for each of your accounts. But you don't trust your memory. Which of the following should you do?** A – Write them all down in a notebook: the name of the each site and the password associated with it for easy retrieval. B – Use a password generator then connect all my accounts C – Use a password manager

Answer: If you insist on writing things down, only write the start of the password to help you remember! Otherwise, if someone finds what you're written, you're in trouble! The password generator can be a good solution, but not if you stay connected. Rather we recommend the password generator! These are tools that allow the encrypted storing of all passwords in one place. They then take the forms of simple browser extensions.

Question 7 – What do we call unwanted email, often containing ads, which we should not open? A – Marbage (contraction of mail and garbage) B – Sponsored content C – Spam

Answer C – Spam. While a lot of spam mails are just ads, some are contain scams that try to steal your data and more broadly (when a virus makes it on to your device) all your content.

Question 8 – If you want to modify your data on a site, you should ask the host. How long do they have to respond? A – You don't have the right to ask for modifications. This is the magic of the internet. B – One week C – One month

Answer C – For all requests for the modification of your data, the deadline for the organisation concerned is one month. Once this deadline passes, you can take it up with your national government body. See here for an example from the UK.

Smile, You're on Camera

Question 1 – You appear on Google Street View. Can you do something? A – No, you was in the wrong place at the wrong time B – Yes you can ask to removed from the image only if it reflects negatively on you (for example you are walking with your forbidden lover) C – You can ask to be blurred out. In this case, click on 'send feedback' on the bottom right of the image. Google will now have 2 months to respond.

Answer: C – You can ask Google to blur the part of the image in which you appear. In this case, click "Report a problem" at the bottom right of the image. If after two months, Google has not reacted, you can file a complaint with the data privacy regulatory body in your country.

Question 2 – What can I do to ensure Google is not aware of where you are? A – Deactivate your location on your smartphone B – Deactivate the position on your smartphone as well as your location history C – Deactivate the position on your smartphone, delete your location history then for every application you download, every site you check and everything you search for on your phone, you have to refuse access to your location **Answer**: None. C is still not good enough. Google can still subtly approximate your location through other means, such as for example when you use the weather app.

Question 3 – How long is security camera footage typically kept? A – One month (except in the case of a ongoing legal case) B – One year (except in case of ongoing legal case) C – Indefinitely

Answer: A – Security camera footage is kept for a maximum of one month. In the case of an ongoing legal case some footage can be extracted and kept but only for this reason.

Question 4 – Do security agencies have the right to listen to your phone calls? A – Yes B – No C – Under certain conditions

Answer: C – Security agencies can listen to the conversations of criminal suspects through requesting of or permission from a judge. Without going through a judge, this is called a security breach. See the laws in your local country and adapt the details based on those.

Question 5 – On Skype, who, aside from users involved in a conversation, can access that conversation's contents? A – Google. It's always Google B – Facebook, the owner of Skype C – Microsoft, the owner of Skype Skype allows encrypted conversations between users however these are

not completely encrypted by default. Microsoft has ways to encode and decrypt and can technically gain access to the content of your conversation. To have a really confidential conversation on Skype, select the 'Private Conversation' option.

Question 6 – In which case can your employer use a GPS system to track your work vehicle? A – Finding the vehicle in case of theft B – During working hours C – Checking whether the driver is respecting speed limits

Answer: A and B, usually. See details for the case of the UK and the EU here.

Question 7 – What does a cookie do? A – Studies and targets the behaviours of potential online buyers B – Please us as snacks (chocolate chip – my favourite!) C – Blocking viruses

Answer: A – Cookies are small text files that websites are able to leave on your computer via your browser. Historically, they were created during the 1990's to improve the experience of internet users and to address issues on the earliest retail sites which, in the event of any connection interruption, would empty their customers' baskets. The idea was to deposit a file on the user's computer which was sent and read by the retail site at the moment of reconnection so that it recognises the visitor. This could for example allow a site to remember you and show you the most recent articles you read.

Question 8 – There are several ways to protect ourselves from targeted online advertising. Give an example of a tool (3 points for all 3 correct; if no answers are suggested, you can list the answers and participants will have to name the one that is not correct for 1 point). A –PrivacyBadger B – uBlock C –VPN

Answer – C. A VPN is not for blocking cookies.

Question 9 – Does a shopping centre have the right to track your phone to analyse how you visit its stores? A – No you're actually joking we in fact live in a free country! B – They can: the shopping centre is private property and we should accept their conditions when we enter C – Yes but they're not allowed to know your identity and your consent must be clear

Answer: C – Yes, but there are conditions. The data emitted by the phone must be deleted once the user leaves the store. The data collected must not be allowed to reveal the identity of the user – for this, clear written consent of the user is necessary. See here for more information.

Under the Radar

Question 1 – What does TOR stand for? A – Triggered on Rage B –The Onion Router C – Tower of Regret **Answer**: C – The Onion Router.

Question 2 – What does this onion signify? A – The layers of protection of an onion B – The developers who created Tor loved fried onions so they honoured this passion in the image. C – A symbol of power in antiquity, the onion represents now the network that will take over the internet. **Answer**: A – The layers of protection

Question 3 – On protonmail (encyrpted email provider), everything is encoded except one thing. What is it? A – Attachments B – Subject line C – Email addresses **Answer**: B – Subject Line. We hope you're avoid putting compromising information in the subject line then!

Question 4 – Encrypted mails are assured between Protonmail users. There is a way for Protonmail users to send encrypted mails with users of other email providers. What is it? A – Click on the lock in the inbox and attribute a password to your recipient so the mail can be encrypted B – Click on the S (for security) in the window and attribute a password to the recipient so that the mail can be encrypted. C – Trick question. No way to do it. Let's all become Protonmail users and live happily.

Answer: A – Note that the 'S' is actually included in emails to indicate that there is a layer of encryption.

Question 5 – When your communications are totally unencrypted, we say that they are: A – Out of the bag B – Plain text C – Light web data

Answer: B – Plain text. When you use a mobile network (therefore texts and calls sent/made directly from your phone) your conversations are plain text. When you use 3G/4G, it depends on the apps used.

Question 6 – What is the safest app today for encrypted communication? A – Telegram B – Snapchat C – Signal

Answer: C – Signal! For further information, see the workshop tool: 'Communicating with Signal'

Question 7 – What can you not do with Signal? A – Create a group conversation B – Send temporary messages that delete after reading C – Receive temporary messages that delete after reading

Answer: none. Anything is possible. Signal is as easy to use and has the same functionality as any non-encrypted app like Telegram.

Question 8 – What is the option called on Messenger that allows a complete encrypted converstaion end-to-end? A – Secret conversation B – Dark conversation C – Long Live Freedom

Answer: A – Secret Conversation. We still recommend using Signal however. Now you just have to

count the points!

4 Going further

To put into practice all this knowledge on personal data, ask participants to try an online role-playing game at home. Here is one example: https://datadealer.com/