2. Internet – Connecting ideas and people

> "Eventually everything connects – people, ideas, objects. The quality of the connections is the key to quality per se."
>
> *Charles Eames, early 20th century designer*

CHECKLIST FACT SHEET 6 – E-MAIL AND COMMUNICATION

Have you created several e-mail accounts and set different passwords for each?

Is the password sufficiently "strong" (more than 8 characters long, with a combination of letters, numbers and symbols)?

Do you clearly label your e-mails with relevant key words in the subject line?

Have you enabled two-factor security on your e-mail accounts (providing an extra security question and/or your mobile phone number)?

CHECKLIST FACT SHEET 7 – CHAT AND MESSAGING MEDIA

Have you included contact details in your website or blog?

Have you taken steps to protect your online privacy?

Have you checked that the content that you are using for your website/blog is in accordance with copyright law?

CHECKLIST FACT SHEET 8 – SOCIAL NETWORKING AND SOCIAL SHARING

Reputation is something we only have one of: do you systematically "think before you post"?

When did you last update your privacy settings on the sites you use?

Democracy depends on the participation of as many citizens as possible in the public debate: have you tried making your voice heard through relevant social network sites?

CHECKLIST FACT SHEET 9 – PRIVACY AND PRIVACY SETTINGS

Is it necessary to post that tagged photo on a social networking site?

Have you read the mobile app agreement to understand what are you sharing: what you own and what "they" own?

When you upload apps, are you sure you know exactly what private information they will access? Is such access really necessary for the app to function?

Do you understand what the European Union's General Data Protection Regulation implies for you?

Fact sheet 9

Privacy and privacy settings

Privacy refers to the degree of control that a person has concerning access to and use of his/her personal information. Most e-mail and Internet users assume that personal information will not be used without permission and that information exchanges are private and secure. The reality, however, is very different.

- Every time you access a website, post content on social media or send an e-mail, you leave information about yourself that could include your physical and computer address, telephone and credit card numbers, consumer pattern data and much more.
- You should also remember that once your data is out there, you may have difficulty retaining control over it and there may be long-term consequences.
- As e-commerce – including online shopping and advertising – becomes a frequently accepted way of doing business, special consideration should be paid to the protection of sensitive data, communications and preferences.
- There should be no lasting or permanently accessible record of the content created by children

on the Internet if it poses challenges to their dignity, security and privacy or renders them vulnerable now or at a later stage in their lives (Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, adopted on 20 February 2008)[1].

Privacy is closely related to security; be sure to read thoroughly Fact sheet 19 on security.

INTERNET PRIVACY

- Internet (or online) privacy is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications and preferences[2].
- Internet privacy is a concern every time a user goes online via computer, tablet, smartphone, gaming console or other Wi-Fi enabled device.
- Internet privacy does not just refer to how you keep your data private online, but also to the accessibility for hackers to retrieve your information.
- The General Data Protection Regulation provides users with more control over their data and affords them more online privacy. The key considerations for the GDPR include:
  - a new definition of user consent – consent can no longer be considered as having been given freely if users have to consent to the processing of more data than is strictly necessary for the provision of that service;
  - better transparency in informing users about how their data is being processed with the use of pictograms/icons and "plain language" – this will allow users to better compare services and choose those with a higher respect for privacy;
  - users' right to data portability, meaning they will be able to retrieve their data in a usable format from the services they use – user control over their data and the principle of data ownership is greatly enhanced with this provision;
  - enhanced protection for children – any child between the age of 13 (minimum) and 16 (maximum) will benefit from extra protection, such as requiring parental authorisation for processing data and protection against data processing for advertising purposes;
  - stronger fees (up to 4% of a company's turnover) in the case of a breach of these rules.
- If a password is hacked, compromised and revealed, the consequences could be very serious, ranging from identity theft to illegal online transactions and more.

Privacy settings

Privacy settings are the controls that allow users to limit who can access your information and how much information can be seen by others.

Privacy settings on most social networks are initially set to a default position; you can usually customise these to your own requirement and should re-check them every time the social network platform advises you that it has implemented upgrades.

Privacy settings should be verified regularly and on all Wi-Fi enabled devices. Remember to check geolocalistion settings too, as the location co-ordinates of you/your device are important aspects of your privacy (see Fact sheet 5 on mobile technology).

Geolocalisation

Geolocation[3] is the identification of the location of an object, such as radar, mobile phone or Internet-connected computer.

Geolocalisation is the process of identifying the location of an object. Geolocation apps report

1. https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75
2. http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy
3. https://en.wikipedia.org/wiki/Geolocation

your location to users and they can also identify the distance to real-world locations in comparison to your location. Geolocation apps have opened up new business models for services and products.

Geolocation can be a threat to your privacy as it pinpoints where you are and the geolocation of a child can also pose a threat to that child's security.

Cookies

A cookie[4] is a text file left on your computer when you visit a website. It cannot harm your computer, but will give access to information about your behaviour and interests. This can provide a more personal surfing atmosphere. For example, when registering with a website, you may be greeted by name upon your return.

It is important to decide how private you want to keep your online behaviour. Since cookies can be used to track usage patterns and contact information, they provide a possibility for encroachment on your privacy. They also facilitate behavioural targeting from advertisers[5].

You can use anti-spyware[6] to help control the data your system is broadcasting and to clean out unwanted cookies.

Today, all websites owned in the EU or targeted towards EU citizens are expected to comply with the Cookie Law (EU Directive 2009/136/EC). This gives individuals the right to refuse the use of cookies that reduce their online privacy.

Data protection

The protection of personal data is regulated by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

You have the right to know what data a business has about you. You should also be able to modify it if it is not accurate and you need to give your consent on how this data is being used.

The best guidelines for protecting your data can be found in the General Data Protection Regulation[7].

Read the disclaimer carefully on all websites and apps where you are asked to provide private information[8]. This is a legal agreement between you and the data controller[9] and should provide details on where and how long your data is stored, and how to have it deleted.

Make sure your machine and e-mail programs are password-protected[10]. When you get a new device or software, or sign up with an Internet service provider, a "default" user and password setting will probably be provided[11]. Make sure you rapidly change such default settings to a more secure password and ID.

It is best to encrypt[12] any sensitive information which is sent over the Internet. Fortunately this is standard for most e-commerce[13] transactions but you should still make sure that a page is secure before transmitting credit card information or bank account numbers.

Different sections of your computer can be secured using passwords. Create passwords for folders containing valuable documents such as confidential projects, research, original designs and so forth.

Right to be forgotten

The right to be forgotten is an important element in any discussion about privacy, as this right allows individuals to "retake" their privacy.

4. https://en.wikipedia.org/wiki/HTTP_cookie
5. https://en.wikipedia.org/wiki/Behavioral_targeting
6. https://en.wikipedia.org/wiki/Spyware
7. http://ec.europe.eu/justice/data-protection/reform/index_en.htm
8. https://en.wikipedia.org/wiki/Disclaimer
9. https://goo.gl/XEkvjh
10. https://en.wikipedia.org/wiki/Password
11. http://www.netlingo.com/right.cfm?term=default
12. http://en.wikipedia.org/wiki/Encryption
13. http://en.wikipedia.org/wiki/Ecommerce

In the European Union, a person can ask a search engine to erase certain results from its index that will not come out when someone looks for his or her name. But there are limits and this measure will always need to be balanced against other people's fundamental rights, such as freedom of expression. In any case, the information will still be accessible in the website where it is located; this will only make it more difficult to find.

To exercise the right to be forgotten and request removal from a search engine, one must complete a form through the search engine's website[14].

But remember, it is better not to post private information in the first place because once it is on Internet it is almost impossible to completely delete.

Importance of talking about privacy in class or at home

The technical and social aspects of privacy and the risks of self-disclosure provide valuable learning themes. Technical aspects may be included in information technology (IT) studies, but should equally form part of a life-skills curriculum.

An important element of education on privacy should be the concept of "profiling" and the linking together of scattered elements of information about a person to deduce a more detailed picture. The important educational implication is that a lot more information can be found about us by "putting two and two together". For example, an "anonymous" social networking profile (hiding behind a pseudonym) may be identified with your real-name by matching photos between the anonymous profile and a full profile on another site.

The idea that privacy is only violated by the disclosure of classic personal information should be examined carefully. New marketing techniques, which discriminate between people based on their behavioural traits (namely, behavioural targeting), may also be considered to be privacy invasive.

Privacy is being increasingly undermined by the rapidity and ease with which children and young people can publish and/or stream digital images on the Internet through web applications and via camera and MMS facilities on mobile phones. A simple rule of thumb: never publish anything you do not want your teachers or parents to see.

Everyone should have the skills necessary to navigate the Internet safely, and that includes knowledge of self-protection, effective communication and responsibility towards others.

There is a natural flow from this theme into the citizenship dimension of any curriculum. The issues raised about online privacy accurately mirror social issues predominant in most cultures today. Exploring the motivations of hackers[15], crackers and privacy activists offers rich possibilities to discuss the value of democratic principles.

ETHICAL CONSIDERATIONS AND RISKS

- Online privacy is one of the most complex ethical and legal topics regarding the Internet.
- Everyone has a right to privacy and needs to be protected from malicious intent.
- Internet privacy risks include phishing (Internet hacking to steal secure user data); pharming (Internet hacking to redirect a legitimate website visitor to a different IP address); spyware (offline application that obtains data without a user's consent); and malware (an application used to illegally damage online and offline users through Trojans, viruses and spyware)[16].
- Sexting, that is the act of sending suggestive and explicit content, images (often selfies) messages, videos, via phone, computer, webcam or other device or writing sexy posts online has serious consequences not only in legal terms but also with respect to reputational risks for the person involved, as messages, images or videos may be posted on social media sites or used in pornographic websites and videos.

14. https://en.wikipedia.org/wiki/Right_to_be_forgotten
15. http://en.wikipedia.org/wiki/Hacker
16. http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy

- We are accountable for all decisions we make about our own and others' rights, for example copyright[17] and intellectual property[18].
- Freedom of speech is a right; however, in practice this is a grey area with no easy answers. What is acceptable and what is not? How does one enforce the rules without encroaching on the rights of the speaker?

HOW TO

Using privacy settings on all of your Wi-Fi enabled equipment with Internet access is one of the best ways to protect your privacy.

Depending on your browser, do a quick search on privacy settings to see how you can:

- block ads and tracking
- block third party cookies
- block websites from accessing your location.

Do not forget to set privacy settings on smartphones, tablets and gaming consoles. The latest cameras have geolocation settings you should check too.

IDEAS FOR CLASSROOM WORK

- Have students do a Google search on their own names. Be sure to look under images and videos as well. Have them create a Google alert on their own names so that they will know when their name has been posted online.
- Create a basic knowledge framework for privacy with your class. Define concepts, both technical and social, and identify prejudices and myths for discussion. Simply setting the questions "What is privacy?" and "Is privacy necessary?" should generate some strong views.
- Search for privacy sites on the Internet and use traceroute[19] programs to locate the physical addresses of these sites to demonstrate the diverse geophysical issues governing legality on the Internet. Explore other issues (cultural, political and historical) that come up from the trace results. For example, choose a remailer[20] site or anonymous proxy service, run a trace, then search for reasons why the services would be located in those countries.
- The Play-Decide role play game on data protection and privacy[21] offers a fun way to explore the implications of privacy law, copyright and freedom of speech, and information across national boundaries or for different age and cultural groups.
- Teach students how to create secure passwords[22].
- Explore and compare user profiles on some of the more popular social networking sites with your students (see Fact sheet 8 on social networking). What private information are users inadvertently disclosing? Draw up a checklist for creating a safe user profile.

GOOD PRACTICE

- Two golden rules:
  - ▶ do not share your personal information with anyone you do not know and trust;
  - ▶ do not use another person's personal information or photo without their consent.

17. http://en.wikipedia.org/wiki/Copyright
18. http://en.wikipedia.org/wiki/Intellectual_property
19. http://en.wikipedia.org/wiki/Traceroute
20. http://en.wikipedia.org/wiki/Remailer
21. http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf
22. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Back up[23] your system, and have a regular backup policy.
- Update security measures on your system and do some research on additional tools at <*http://www.epic.org/privacy/tools.html*> that will support your online preferences.
- Anti-virus[24] and firewall[25] software are an absolute necessity. You might also want to consider other tools such as pop-up blockers[26] and anti-spyware[27]. Be sure to check your system regularly.
- Use "strong passwords"[28] to protect your PC, e-mail and Internet connections. Strong passwords consist of letters, numerals and special characters.
- Before giving out private data, check for the locked padlock symbol that shows up in the toolbar. This is a sign that your transaction is taking place over a secure connection. Before making online transactions, check that the URL includes HTTPS; the S stands for "secure" in the Hypertext Transfer Protocol (HTTP) and authenticates the website and the associated web server, which protects against third-party attacks.
- Avoid online shopping on unreliable websites and avoid exposing personal data on websites with lower security levels.
- Be sure to check your rights; you may be more protected than you think. Users are always the weakest link in privacy and data protection.

FURTHER INFORMATION

- To read more about the Cookie Law and the EU Directive, see: <*http://www.cookielaw.org/the-cookie-law/*>.
- There is a European Commission Fact sheet on the right to be forgotten: <*http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf*>.
- There is also a European Commission Fact sheet on data protection <*http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf*> and other information on related reforms <*http://ec.europe.eu/justice/data-protection/reform/index_en.htm*>.
- The Electronic Privacy Information Center (EPIC) maintains a list of privacy tools and articles: <*http://www.epic.org/privacy/tools.html*>.
- Find out what your PC is telling anyone on the net who cares to look by using BrowserSpy: <*http://gemal.dk/browserspy/*>.
- Concerned about your civil liberties? These discussions on privacy could keep your citizenship class going for a while: Electronic Frontier Foundation at <*http://www.eff.org/*>, Epic.org at < *http://www.epic.org*>, Privacy International at <*http://www.privacyinternational.org/*> and Privacy.net at <*http://www.privacy.net/*>.
- TuCows at <*http://www.tucows.com/*>, is a website which provides access to over 40 000 shareware and freeware programs. It promises fast, local and safe virus and spyware-free downloads.
- Zone Alarm at <*http://www.zonelabs.com/store/content/home.jsp*> is one of the better known firewall programs. It lets you set access controls for different programs which send information out over the Internet.
- CryptoHeaven is an encryption package which offers secure mail, file sharing and chat with symmetrical and asymmetrical encryption: <*http://www.cryptoheaven.com/*>.

23. http://en.wikipedia.org/wiki/Back_up
24. http://en.wikipedia.org/wiki/Antivirus
25. http://en.wikipedia.org/wiki/Firewall_%28networking%29
26. http://en.wikipedia.org/wiki/Pop_up#Add-on_programs_that_block_pop-up_ads
27. http://en.wikipedia.org/wiki/Spyware
28. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Facebook Help Center provides information on privacy settings: *<https://www.facebook.com/help/193677450678703>*.
- Statistics on how children and young people understand online privacy and privacy settings can be found on *<http://web.archive.org/web/20160703155259/https://www.techopedia.com/2/30101/internet/online-privacy/do-millenials-understand-online-privacy>*.
- For statistics on being young in Europe today, see *<http://web.archive.org/web/20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world>*.
- For information on European digital rights, see *<http://www.edri.org>*.
- Relevant Council of Europe documents:
  - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108): *<http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>*.
  - Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet: *<https://wcd.coe.int/ViewDoc.jsp?id=1252427>*.
  - The Council of Europe page contains information about the work of the Council of Europe in the field of of privacy and data protection: *<http://www.coe.int/en/web/internet-users-rights/privacy-and-data-protection>* as well as information about your rights and responsibilities online.