ESCALATE

Module 6
Unit 3

Unit 3 – Digital footprints, privacy and surveillance

Module 6: UNINTENDED CONSEQUENCES AND THE ETHICS OF DIGITALISATION

Co-funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission. This presentation reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 3: Digital footprints, privacy and surveillance

1. Effects of transitioning to online/digital teaching and learning
2. GDPR and ethical issues
3. **Digital footprints, privacy and surveillance**

The objectives of this Unit are:

- To illustrate the concepts and uses of digital footprints, cybersecurity, privacy, and surveillance in the HEI context

- To highlight possible issues you may have, and good practice to better inform the management of such issues

Contents

3.1 What are: digital footprints, privacy and surveillance?

3.2 Surveillance and the commercialisation of the surveillance logic

3.3 Pros and cons of surveillance of students, teachers and workers

3.4 Privacy and data protection issues for students, staff and organisations

3.5 Cyber security issues for educational institutions and individuals (staff and students)

3.1 What are: digital footprints?

- Digital Footprint is defined by the UK Government Centre for the Protection of National Infrastructure as " the data that's left behind whenever a person uses a digital service, or someone posts information about that person onto a digital forum, such as a social network." (CPNI, 2016)
- The EU on Citizens' Digital Footprint; "While interacting with digital information systems, citizens create an increasing trail of personal and individual data. These data are recorded and possibly archived somewhere, owned by someone, and potentially used in various ways." (EU online)
- This includes social media, Internet searching, filling out a webform. It can be active (uploading a photo) or passive (such as visiting a website). The increasing use of technology in education means more and more digital footprints are being generated by both staff and students

Source: [3]

Reflection

Question

- What digital footprints have you left today?
- How might they be used by others?

Did you know...

E-Professionalism

Being mindful of digital footprint is also linked to one's e-professionalism

Many professional associations have guidance on using social media, including the General Medical Council

Digital footprint has an effect: jobs, university recruitment, etc.

HEI ideal environments for teaching about the management of one's digital footprint

Good practice

Ways to manage digital footprint

Your digital footprint is present at all times, and will update – learn to be aware and keep on top of any changes

Find out what information is available about you online

Protect your information

Be aware/alert – can you trust this website? How much information does this webform really need? Make sure to keep on top of privacy settings

Recommendations from CPNI (2016); Open University (2020)

ESCALATE

Source: [8]

What is privacy?

- Privacy, despite being used in everyday language, as well as being the subject of discussion in legal, philosophical, and political terms, has no single definition; nor does the concept of privacy conform to a single meaning, or context (Stanford Encyclopaedia of Philosophy, 2018)

- The first entry in the Oxford English Dictionary describes privacy as: “The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.”

- Writing on the developments of newspapers being able to access details about people's personal lives, Warren and Brandeis stated that individuals should have the “right to be let alone” (Warren and Brandeis, 1890)

- Different conceptions of privacy include:
- The right to be left alone
- The right to restrict access to oneself, or information about oneself
- The right to control access about oneself

- Privacy is a fundamental aspect of selfhood and self-development and it is vitally important for autonomy, freedom of speech, and access to information

Source: [6]

UK’s Data Protection Act 2018 (GDPR)

- Data is processed lawfully, fairly and transparently
- Data is collected only for specified and legitimate purposes
- Data collection is limited to what is necessary for those purposes
- Data is kept accurate and up-to-date
- Data is held no longer than necessary
- Data is processed securely and is protected against loss and damage
- The controller is accountable and demonstrates compliance of the legislation
- Information Commissioner’s Office (2020)

Source: [6]

The GDPR Principles

GDPR – 6 Principles of Lawful Processing

Available:GDPR Six Principles of Lawful Processing In 1 minute - 2019 Summary – YouTube

Runtime: 1.30

Source: [X]

Reflection

Question

- Have you been in a situation where an organisation has not handled your or someone else’s data correctly?
- In what ways might an organisation might mishandle data and violate on ethe the data protection principles?

What is surveillance?

- Surveillance: is to watch over
- Surveillance is watching with intent
- It is a huge part of our lives: Part of the “street furniture” (Groombridge, 2002).
- Types of surveillance include surveillance cameras, Internet cookies, customer loyalty cards mobile phone tracking, person-to-person monitoring. It is carried out at state-level, by private companies, and public organisations. A CCTV camera might be used by a municipal council to deter vandalism. A retail business might use CCTV cameras in its brick-and-mortar store to both detect and deter theft.

Source: [2]

Reflection

Question

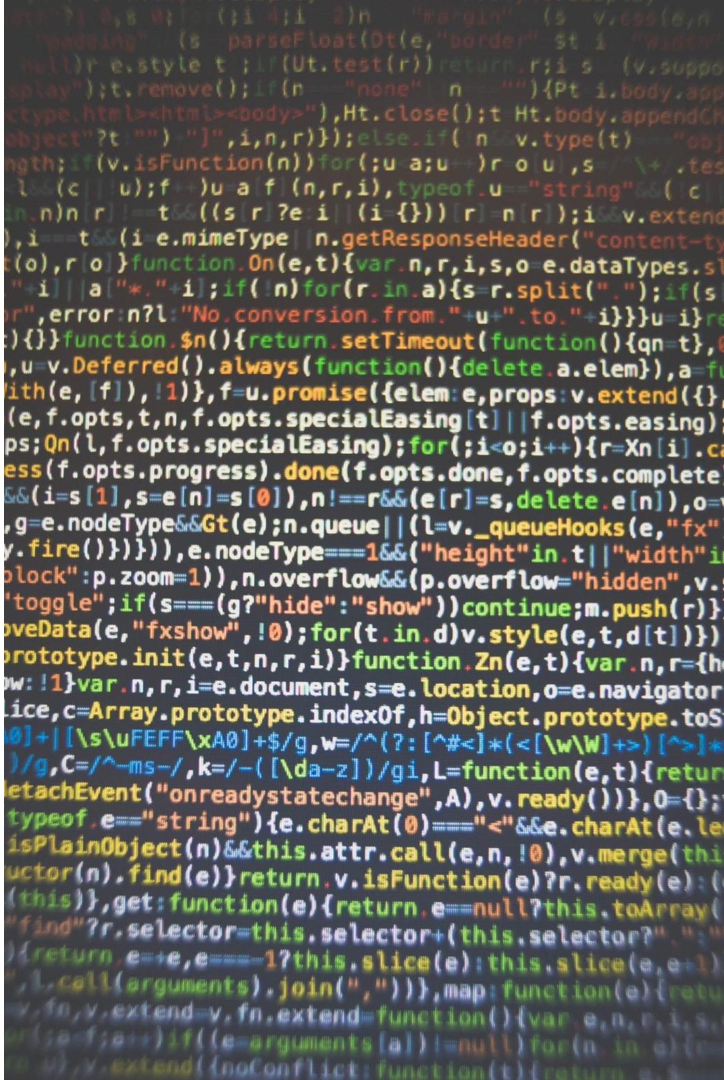
- What types of surveillance have you encountered today?
- What types of surveillance do you encounter at work?

Surveillance: theories

- Panopticon
- Synopticon
- Sousveillance
- Surveillant assemblage
- Often depicted as dystopian (think George Orwell’s ‘1984’) but not always this way.
- Care and control

3.2 Surveillance and commercialization of the surveillance logic

- Analytics software and AI
- Tracking systems in lectures
- Smartcards and app check-ins
- Surveillance cameras
- Radio frequency identification (RFID), trackers
- Internet monitoring



Example

Case Study: app check-in

- The HEI you work at has installed a new system whereby students check-in to lectures using an app.
- Staff can monitor check-ins through the institutions VLE – it also tells them when students go to the library, how long they spend there
- What are the issues with this?

ESCALATE

Source: [10]

3.3 Pros and cons of surveillance of students, teachers and workers

- An early warning system for lack of engagement by students (e.g., not attending classes)
- Can flag misuse
- Protection of students
- Allows students to gain feedback
- increases efficiency
- Gain understanding of how students are using resources

Source: [2]

Pros and cons of surveillance of students, teachers and workers

- Privacy implications
- Chilling effects
- Surveillance creep
- Outsourcing technology and the use and storage of data
- The changing role of staff
- Can be undermined – this is particularly harmful in regards to issues such as COVID-19
- Can be oppressive and lead to stress

Source: [2]

Example

Case Study: MyAnalytics and Cortana

- Software such as MyAnalytics and Cortana analyse work patterns to provide insights into working patterns and email use..
- Have you experienced emails from Cortana or MyAnalytics in Outlook reminding you of meetings or letting you know of tasks you need to finish?
- Were you opted in to the use of this? Did you have a choice?
- Do you find it helpful?

Source: [10]

Surveillance in education

How China Is Using Artificial Intelligence in Classrooms

Available: [How China Is Using Artificial Intelligence in Classrooms | WSJ – YouTube]

Runtime: 5.43

Source: [X]

Did you know…

Privacy at university

Jisc 2018b – (a UK higher, further education and skills sectors' not-for-profit organisation for digital services) found that a high proportion of students trust their HEI with data privacy

Example

Case Study: Student learning

- A new software package has been brought in. It measures:
- student attendance
- what type of books students use at the library
- their progress on assignments.

- It then feeds back this information to the student to let them know how they are progressing and suggests what they can do to increase their performance. It also lets staff know their performance.

- What sort of privacy issues could result when using this technology?

Source: [10]

3.4 Privacy and data protection issues in Higher Education

- Aspects of digital tech (AI, LA) can undermine privacy
- Demonstration of consent
- How necessary the data collection is – the gathering of data can lead to issues of sharing with third parties and using data for commercial means
- Transparency in data collection
- Privacy is important particularly in library settings (codes of conduct) tension with data mining and surveillance

Source: [6]

Good practice

How to Handle Data

Comply with the Principles of the Data Protection Act

Process data lawfully

Be accountable

Be transparent

From Jisc’s Guide to Data Protection (2020)

Source: [8]

3.5 Cyber security issues for educational institutions

What is cyber security

- Definition: How individuals and organisations reduce the risk of cyber attack (UK National Cyber Security Centre, 2020) It is an important aspect of organisations and businesses

- Examples of cyber attack:
- Phishing: an :email purported to be from IT, asking you to reveal the password to your work IT account
- Spear phishing: an email purported to be from your boss (using their correct name) asking for certain information
- Malware: a computer virus hidden on another application, that when installed, stats to destroy data
- Ransomware: a virus installed via an email link has a pop-up box asking for a ransom to unlock computer access

- Phishing is one of the greatest threats to the (UK) higher education sector (National Cyber Security Centre, 2019)

Source: [2]

Did you know...

Cyber attacks in universities

In June 2017, an American university paid $1.9m into a fake bank account after receiving an email invoice claiming to be from their contracted construction company (National Cyber Security Centre, 2019).

Queen’s University in Belfast had to suspend access to a number of systems after an attempted cyber attack early in 2021 (BBC, 2021).

Cyber security issues for educational institutions

- Cyber attacks are a major threat to HEIs as they handle personal and research data, intellectual property and other assets, each of which has significant value to others (National Cyber Security Centre, 2019)
- Can cause lots of damage: research, investment
- COVID-19 research is a current area of threat
- The influx of new technology into HEIs means more information is being made available to third parties who control the software

Source: [6]

EU Cyber Security strategy

- EU’s Cyber Security Strategy (December 2020) http://ec.europa.eu/digital-single-market/en/cybersecurity-strategy

- Covers:
- Security of essential services such as hospitals, energy grids and railways
- Security of ever-increasing number of connected objects in our homes, offices and factories,
- Building collective capabilities to respond to major cyberattacks
- Ensuring international security and stability in cyberspace

- EU response to large-scale cybersecurity incidents and crises (EU, 2017)

Source: [6]

Good practice

Cyber security: People first

Educate and engage with users who will be using digital and online technologies

Create awareness of cyber security risks, and create a positive cyber security environment

Create an AUP that is kept up-to-date, and is such that it emphasises important points, in a clear, easily read and understood way

Update the AUP regular, and highlights its existence to users

Source: [8]

Key takeaways

- The use of surveillance technologies is a complex issues in education, affecting both students and staff: the same technology can be used for both caring and controlling purposes.
- Digital footprints have an important impact on student and staff lives, with information generated online being used by employers and having an effect upon university recruitment. Higher education is an ideal environment for learning about digital footprint management, but the subject is often portrayed in a negative rather than a positive way.
- Cyber security is a major threat to universities. People – both staff and students are the first line of defence against such attacks. Therefore, it is paramount people are well informed of security measures, and a positive culture surrounding cyber security exists.
- Privacy is a fundamental building block of selfhood and democracy, particularly in the context of education. Upholding data protection principles, and being transparent in the use of data is key.

References

BBC News (2021) Queen's University takes 'precautions' after cyber-attack attempt, Available: https://www.bbc.co.uk/news/uk-northern-ireland-56287355
CPNI (2016) My Digital Footprint: A guide to digital footprint discovery and management, Available at: https://www.cpni.gov.uk/security-campaigns/my-digital-footprint
EU (2016) Citizens' digital footprint Available: https://ec.europa.eu/jrc/en/research-topic/citizens-digital-footprint
EU Cyber Security Strategy (2020) http://ec.europa.eu/digital-single-market/en/cybersecurity-strategy
EU (2017) COMMISSION RECOMMENDATION (EU) 2017/1584 Available: https://eur-lex.europa.eu/eli/reco/2017/1584/oj
Foucault, M. (1991) Discipline and Punish: The Birth of the Prison. London: Penguin
Groombridge, N. 2002. Crime control or crime culture TV? Surveillance & Society, 1(1), 30-46.
Haggerty, K. D. and Ericson, R. V. 2000. The surveillant assemblage. The British Journal of Sociology, 51(4), 605-622.
ICO (2020) Information Commissioner’s Office. ICO. 2020. Guide to Data Protection - Principles, Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
Jisc (2018) Digital experience insights survey 2018: findings from students in UK further and higher education, Available: https://www.jisc.ac.uk/rd/projects/student-digital-experience-tracker

References

Jisc (2020) Data Protection, Available: https://www.jisc.ac.uk/guides/data-protection
Lyon, D. (1994) The Electronic Eye: the Rise of Surveillance Society. Minneapolis: University of Minnesota Press.
Mathiesen T. 1997. The Viewer Society: Michel Foucault's Panopticon' Revisited. Theoretical Criminology, 1(2), 215-234.
NCSC (2019) The cyber threat to Universities, Available at: https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities
NCSC (2020) What is Cyber Security? Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
NUS (2018) The Experience of Muslim Students in 2017-18, Available: https://www.nusconnect.org.uk/resources/the-experience-of-muslim-students-in-2017-18
Open University (2020) Being Digital Available: Being digital | Library Services | Open University
Robinson, E., McQuaid, R., Webb, A. and C.W.R. Webster (2021) 'Unintended Consequences of E-Learning: Reflections on the Digital Transformation of Learning in Higher Education', in Larsen, C. et al. (eds) *Transformations of Local and Regional Labour Markets across Europe in Pandemic and Post-Pandemic Times* (Rainer Hampp Verlag, Muenchen

Stanford Encyclopaedia of Philosophy (2018) Privacy, Available: https://plato.stanford.edu/entries/privacy/

Warren, S. and Brandeis, L.. (1890) "The Right to Privacy," Harvard Law Review, 4: 193–220
Webb, A., McQuaid, R. and Webster, C.W.R. (2021) 'Moving learning online and the COVID-19 pandemic: a university response', *World Journal of Science, Technology and Sustainable Development*, 18, 1, 1-19. https://doi.org/10.1108/WJSTSD-11-2020-0090

Authors

Ron McQuaid
Elaine Robinson
Aleksandra Webb
William Webster
University of Stirling, Scotland

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This presentation reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

www.escalate.projects.uvt.ro