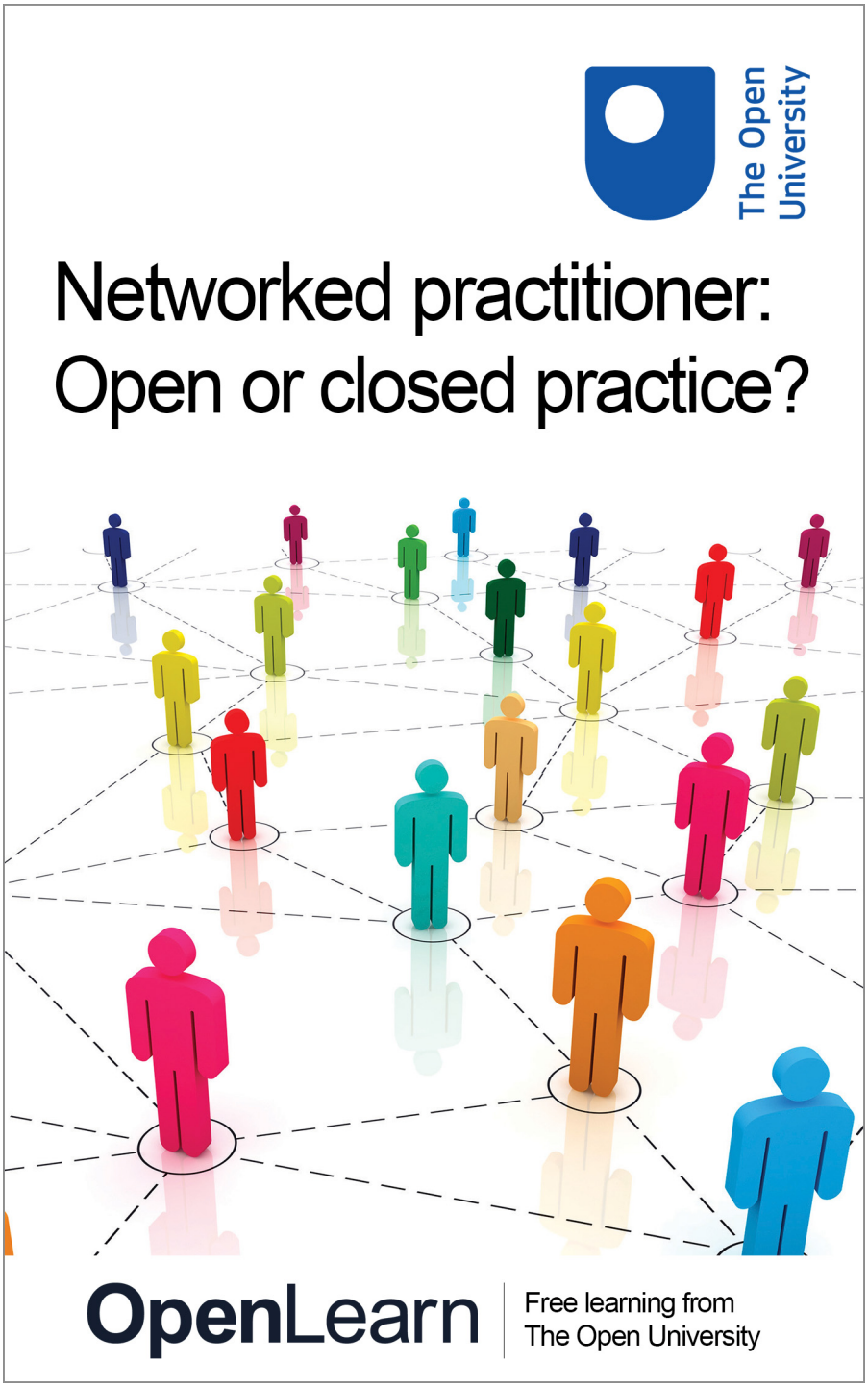
OpenLearn

The Open University

Networked practitioner: open or closed practice?


The Open University
Networked practitioner:
Open or closed practice?
OpenLearn
Free learning from
The Open University

About this free course

This free course is an adapted extract from the Open University course H818 *The networked practitioner* www.open.ac.uk/postgraduate/modules/h818.

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University –

www.open.edu/openlearn/education/educational-technology-and-practice/networked-practitioner-open-or-closed-practice/content-section-0

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Intellectual property

Contents

Introduction 5
Learning Outcomes 6
1 Investigating an open landscape 7
1.1 The variety of ‘open’ 7
2 Benefits of open and closed 10
2.1 Benefits of an open approach 10
2.2 Risks of an open approach 10
2.3 Balancing a more open or a more closed approach 12
2.4 The case for closed: security 13
2.5 Open, closed, usability, security – a fine balancing act 14
3 Being a networked practitioner: privacy, identity and data ownership 15
3.1 Being a networked practitioner: sharing vs privacy 15
3.2 Cookies 16
3.3 What is a digital identity? 17
3.4 How does this translate to open sharing and online issues of privacy and identity? 18
Conclusion 20
Keep on learning 21
References 21
Acknowledgements 23

Introduction

It is difficult to make the daily decisions as a practitioner in the digital world on how open or closed you should be. In this free course, *Networked practitioner: open or closed practice?*, we start a debate to support the decision-making process around openness and the different preferences we each have.

Networked practice online is often connected to decisions about open practice. To network with others requires some exchange of information. To network online, whether for study or for work, often places us in the position of sharing information or conducting activities with people we do not know.

Constraining or anticipating the way information is exchanged is problematic in a digital age. Decisions about online privacy and identity are issues that affect everyone, including students using the internet for learning. In this short course, you will review the idea of openness in networked practice and the links from this into wider areas and broader behaviour.

This OpenLearn course is an adapted extract from the Open University course H818 *The networked practitioner*.

Learning Outcomes

After studying this course, you should be able to:

- explore assumptions about open practices and conduct research to inform personal initial views on openness;
- integrate decisions regarding online privacy and identity into choices to be more open or closed when working online;
- be aware of online networking and how such activity may develop and be visualised.

1 Investigating an open landscape

In this opening section Anne Adams (Senior Lecturer in Learning and Teaching Innovation at The Open University) discusses the benefits and drawbacks of an open versus a closed approach.

Open education is only one ‘flavour’ of openness which may influence your own activity. This section considers how shared, open and networked practice is influenced by other open practices at the boundaries of education.

The meaning associated with the word ‘open’ in education, training and professional practice has shifted. When The Open University was established in the 1960s the term ‘open learning’ emphasised an opening up of education through widening access to formal learning opportunities leading to relatively conventional qualifications (e.g. undergraduate and postgraduate degrees).

More recent uses of the term ‘open education’ refer to relaxation of the requirements constraining registration, assessment, fee-payment, progression and access to educational resources. In Massive Open Online Courses (MOOCs) there may be no fee, no registration process (or a simpler process with less commitment when compared to other forms of education), access to reuse and repurpose the content, optional assessment, and expectations that the majority of learners will not complete the whole course through their own choice.

This shift in opening up education by changing the way in which some courses are offered, resonates with wider shifts in an open landscape surrounding teachers, trainers, students, learners and educational institutions. This openness reflects wider political changes in priorities, particularly in reforming access to research and data where there has been public funding of the underlying work.

1.1 The variety of ‘open’

The word cloud in Figure 1 illustrates some of the terms associated with ‘open’, e.g. education, access, research, source, data, science, publication and massive online courses.

Figure 1 Word cloud illustrating some of the terms associated with 'open'.

There is some obvious common ground between these terms and teaching and learning activity. For example the link between open research and open learning draws together two areas of open academic practice. Open science and open research share common roots and both benefit from the potential to speed up and enrich processes of discovery by utilising crowdsourced data, a practice which can also be applied to open educational resource activity. Crowdsourcing is also associated with emerging open knowledge transfer practices within the workplace (Tapscott and Williams, 2007).

It is not only educational institutions who seek solutions to difficult problems by posting questions to a network of experts. The effectiveness of this model has been well demonstrated through open source programming. The exchange of ideas and analysis across and within sectors can be mediated and transformed in the open environment, particularly when utilising online social tools. The values and norms around copyright and sharing of public-funded work are being revisited from within education and beyond. The potential of open knowledge is becoming more widely recognised and evaluated.

Activity 1

Timing: 1 hour

On the H818 course that forms part of The Open University's Masters in Online and Distance Education we encourage learners to develop a network on Twitter. This can be very useful in both crowdsourcing information (the 'hive mind') and in increasing the reach of your own ideas or research (for example if you need volunteers to undertake an online survey).

- If you have an account on Twitter, perform a search on the hashtag #h818conf – this is the hashtag used for the annual Online Conference of the H818 course *The networked practitioner*. Every student on the course delivers a short online presentation about an aspect of 'Open education' under a subtheme of inclusion, implementation or innovation.
- If you do not have a Twitter account and do not wish to sign up for one, you can perform a similar search using Google – simply enter the terms Twitter and

#h818conf and you should receive the same results as a search within Twitter itself.

- Browse the tweets (these go back as far as the initial conference in February 2014) to get an impression of the variety of topics covered relating to 'open'.
- View the conference programmes on Cloudworks, where you can read the abstracts of any presentations that take your interest. To locate the conference programmes simply go to www.cloudworks.ac.uk and search for 'H818'.

2 Benefits of open and closed

As networked practitioners, we seek to gain openness in scholarship for both teaching and learning. However, to do this in an ethical and effective way requires decisions about when to close access to what information. In this introduction to openness and privacy, you will hear two balanced arguments to explore these questions.

2.1 Benefits of an open approach

Listen to the following audio recording (8 minutes) in which Martin Weller, Professor of Educational Technology at The Open University, talks about the benefits of being open.

Audio content is not available in this format.

Activity 2

Timing: 5 minutes

Martin Weller describes five benefits of openness. Which of the following is **not** one of the benefits he describes?

○ Openness can increase an academic author's income.

This is the correct response. Martin Weller says that publishing openly is unlikely to increase an academic author's income.

○ Openness can help an academic's content increase its reach.

This is an incorrect response. This is one of Martin Weller's five benefits of openness.

○ Openness can assist with increasing an academic's network.

This is an incorrect response. This is one of Martin Weller's five benefits of openness.

○ Openness can aid with reciprocity.

This is an incorrect response. This is one of Martin Weller's five benefits of openness.

2.2 Risks of an open approach

Technology-enhanced learning has the potential to enhance the world of learning across all levels. With OERs (open educational resources) and MOOCs (massive open online courses) there is an increasing number of new forms of distance education. Combined with this is an array of online tools and exciting new activities for formal learning, providing a wealth of possibilities for supporting learning throughout the world.

With the many opportunities come many risks. These risks are not just simple ones that an individual takes or leaves but also risks to organisational systems, processes and its data. So the risks are to you as an individual and for your organisation. System and process risks, such as confidentiality, can dramatically affect users' perceptions of a system's reliability and trustworthiness. It is often unclear whether breaches of confidentiality are malicious or accidental, but they can have serious repercussions for a system and its administrators (Adams and Blandford, 2005). The question of restricted,

closed access can therefore be essential to retain users' trust in an online learning program. Cronin (2016) covers some of the core issues from a practitioner's perspective.

2.3 Balancing a more open or a more closed approach

Figure 2 achieving balance in your approach is critical to success

While we may not want to have a totally closed approach to being a networked practitioner, we need to consider a balanced approach to information sharing. This

requires safeguarding what is important to protect, while not prohibiting valuable access to information that we need and want to be open. This impacts on how we act and our practices as a networked practitioner as well as the systems we use (Adams and Blandford, 2005; Adams and Sasse, 2005).

Although some closed practice, with regard to accessing information and its usage, is essential, it should not impede our original objectives. For example, personal exam results could be openly accessible to everyone as soon as they become available. However, there could be psychological repercussions for students as these are, for many people, very personal and judgmental pieces of information. Students often need to come to terms with their own results and deal with the repercussions, both good and bad, before they inform others. Security systems support that restricted access for privacy purposes. Yet we need to carefully consider what requires closed access and what should be open. Often, as a society, we are too risk averse and we tend to restrict access by default without carefully understanding why. This can have adverse effects on learning systems and practices as security mechanisms, and their poor implementation, have been found to present serious usability problems (Adams and Sasse, 2005; Adams and Blandford, 2005).

2.4 The case for closed: security

There are two principal security issues: authentication and privacy. Whilst authentication can be essential to protect organisations' systems, users often encounter usability problems, such as passwords and pin numbers, which are very labour intensive or simply unworkable. The result is that users either try to circumvent the mechanisms or simply move to other systems to complete their task (Preece, 2000; Whitten and Tygar, 1999). Security mechanisms for distance learning and in virtual learning environments must be designed appropriately to meet students' and teachers' needs to ensure that they effectively protect our information without hindering our ability to undertake the tasks we need to complete.

Users seeking to protect their own privacy encounter further complex usability problems. These usability issues often relate to concepts of ownership (e.g. intellectual property rights, copyright, privacy rights). Many distance learning systems do not provide adequate feedback on these topics, or offer sufficient control over rights (Preece, 2000; Bellotti and Sellen, 1993; Adams and Blandford, 2005).

Although some usability issues only relate to specific online settings, others are more universal.

Assessment and personal progression data is an obvious concern for students and thus authorised access to that data has to be secure. Alternatively, some learners may have concerns about access to their images, while others are completely happy with no restrictions. (It is interesting to note the number of people who turn their camera towards a view or a wall while taking part in video conferencing, while others are completely happy to face the camera. This can be related to the reasons why some students choose distance learning, which can give some anonymity. In an odd way, forcing openness here can curtail an individual's freedom to control how they are perceived by others.)

All of the above would suggest that there should be flexible personal controls on personal information.

2.5 Open, closed, usability, security – a fine balancing act

Figure 3 balance is also impotant in your design process

This discussion has covered some of the arguments around when and why a closed approach should be used to balance an open approach for distance learning and for the networked practitioner. Organisational, and sometimes also personal, security concerns are the strongest argument for closing or restricting access. As we heard from Martin Weller, there are numerous arguments for openness that sit on the other side of the balance. It would be useful to explore Adams and Blandford (2005) and Adams and Sasse (2005) for a more detailed review of the fundamental differences between the culture of security and open online learning that produce clashes between the two approaches. These clashes are often the root cause of usability issues in security mechanisms for online and distance learning users. These two articles also present an account of how future systems can be developed which maintain security and yet are still usable. Gauging this balance between security and usability is a core skill of the networked practitioner.

3 Being a networked practitioner: privacy, identity and data ownership

Networked and open practice requires a degree of trust between participants. This section gives you an overview of the issues and factors affecting decisions about trust and control options. It should offer you some food for thought about privacy, drawing on research into this issue.

Privacy has often been suggested as a basic human requirement. The US Supreme Court ruled that privacy is a more fundamental right than any of those stated in the Bill of Rights (Schoeman, 1992). Over the past 30 years there has been a steady increase in the opinion that computerisation has decreased an individual's privacy (Kumaraguru and Faith Cranor, 2005). At the same time internet sharing of personal information has dramatically increased.

Legislative developments have not cleared up this complexity, but simply reduced it to concepts of ownership. The debate over who owns data has often overshadowed the debate about data usage and what makes it sensitive. Some argue that all data can be sensitive, depending on the context of use, but legislation about data management has often simplistically divided data into two broad types:

1. **Inherently sensitive data (personal information):** for example, racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, data concerning health or sex life
2. **Relatively innocuous data:** for example, consumption habits or household management.

3.1 Being a networked practitioner: sharing vs privacy

As we saw in Section 2, computer system designers and policy makers have a complicated job trying to weigh up the importance of open access to information while maintaining different needs for privacy. The traditional approach to privacy protection, based on political science, takes a procedural, step by step approach rather than reviewing deeper, fundamental issues. The individual (whose privacy requires protecting) is defined as the 'data subject' and the organisation using the data as the 'data user'. There are two issues that are traditionally reviewed by political science with regard to privacy:

1. Limiting access to identifiable data about individuals (the data subject). The need for secrecy for personal information is often noted as one of the common characteristics of privacy
2. Open disclosure of organisational (data user) information usage. Organisational secrecy in information usage is often noted as the root cause of privacy invasion.

Access policies and technical mechanisms, such as access authentication and data encryption, are often seen as ways to limit access to identifiable data. Concepts of

identifiable data or personal information, however, are often based upon simplified assumptions about the data subject and perceptions of privacy invasion risks, such as personal exposures to risk and perceptions or fears of risk.

The personal information approach assumes that the problem is the initial control of releasing information. However, research by Adams (2005) identified that maintaining privacy when sharing relies on an accurate awareness of practices with regard to the receiver of the information, how the information is used and the sensitivity of the information. Perceived sensitivity also relies upon who receives the information and how it is used.

Some privacy experts have sought to review specific sharing behaviours in the light of privacy and trust issues. Joinson and Paine (2006) evaluate the act of self-disclosure; making what was previously unknown about the self, known. Along with issues of control over personal information, they suggest trust and vulnerability are important issues, as well as cost and benefit trade-offs made around the act of sharing.

The personal information perspective approach has directed many activities for protecting online privacy in the digital information sharing and usage, especially those related to marketing. For example, cookies have been used in online systems for several decades and we'll consider these next.

3.2 Cookies

A cookie is a small data file, sent from a website and stored in the computer user's browser. A cookie file is usually automatically installed when an individual first visits a website. The cookie is used to tell a website operator when that person revisits the site. Cookies do not give the website operator any information about that person's identity (e.g. name, address, telephone number), unless the person accessing the site has already given it to the operator.

Theoretically, the only information an organisation can put in their cookie file is the information given to them. Amazon's files probably contain information about what items someone bought, their address, credit card information, and maybe some information about what items they looked at but didn't buy, i.e. any information they have gathered from the user's activity on their website. Amazon does not, therefore, know how old the user is or the colour of their hair, since that information was not given to them.

Web advertising companies use cookies to collect information about computer users, so that they can send them targeted advertisements. They achieve this by having their member sites show advertisements that come from their web domain. Ultimately, the advertisement fools the users' web browser into believing it is the same site, because it is the same organisation providing advertisements. This has been viewed as both beneficial and intrusive. It can provide tailored, relevant information for the user but some people feel that tracking their activities is unacceptable.

Users are able to opt-out of the use of cookies, but it isn't possible to opt-out of IP addressed-based tracking. An Internet Protocol (IP) address is a numerical code attached to each device connected to the internet. This can allow the tracking of devices and device interactions back to countries, cities and organisations depending on how the device is registered.

Activity 3

Timing: 5 minutes

Which of the following is the most effective way to protect your personal information?

○ Encrypting transactions containing sensitive data.

This is one way of protecting some of your personal information, but it is not the most effective of the options given in this question.

○ Never going online at all.

Correct! It would be a drastic measure, but a very effective way to protect your information is never to go online at all. (Note we do not recommend this course of action!) It is also important to note that, even if you never personally access the internet, records and information about you is still likely to appear online through other people and organisations.

○ Opting out of accepting cookies.

This is one way of reducing the personal information that is captured as you use the internet, but it is not the most effective of the options given in this question.

○ Using a Virtual Private Network to disguise your IP address.

This is one way of protecting some of your personal information, but it is not the most effective of the options given in this question.

3.3 What is a digital identity?

Physical, temporal and social psychological contexts can seriously impact on a person's identity, their ability to learn and to re-form their identity. 'I'm at university now so I'm a student, I'm at work now so I'm an employee, I'm home now so I'm a daughter/son/mother/father'. Who we are, is very tightly interwoven with what we have learned (Bernstein and Solomon, 1999; Lave and Wenger, 1991). However, as Lave and Wenger (1991) emphasise, sharing within any domain is more than a formal acquisition of knowledge. It has a strong social element. The concepts of situated sharing highlight how its development relates to the socio-cultural contexts and how this impacts on our identities. Goffman (1969) highlights that our identities are not fixed commodities that can be simply traded up or down.

As individuals, we often inhabit multiple social worlds, and so need to make judgements about the degree of openness we offer within each of them. We have complex identities that we adapt and present for different social situations or communities within which we live. However, as the boundaries between real-life situations and our digital identities blur we need to have a deeper understanding of the impact of merging digital identities to support changes in acceptable sharing (openness) practices that fit with the different sides of our identity (as a student, a colleague, an employee, a daughter/son/mother/father).

The concept of 'communities of practice' emerged from a learning theory developed by Lave and Wenger (1991) called 'legitimate peripheral participation'. Sharing, it could be argued, should be through a process of participation in communities of practice.

Wenger (1999) extends this to a framework in which two basic streams are 'practice' (from collective social norms of practice to accounts of meanings) and 'identity' (from impacts of organisational power and social structures to those of personal subjectivity). Both our

identities and the context of our practice impact upon our perception of openness and acceptable sharing.

3.4 How does this translate to open sharing and online issues of privacy and identity?

Issues of privacy are often countered by arguments for an increase in the freedom of information. Freedom of information was the main driver behind the open access movement. At the extreme end, advocates argued that new technological drives are irrepressible, and privacy safeguards futile. Privacy, it was maintained, can only be secured by concentrating on increasing the freedom of information for everyone and everything. In short, making everything public destroys the problems associated with secrecy.

However, the open access movement has grown to acknowledge some important limits in the complete freedom to access all information. Some national, organisational and personal information does require secrecy to maintain economic advantage and personal freedom of expression free from social scrutiny. Ultimately, open access and online sharing relies on an understanding and respect for what is acceptable to others (netiquette).

Houghton and Joinson (2010) identify the importance of co-owned information and boundaries within which sharing occurs. However, they highlight the difficulty of managing these boundaries and the need for users to be aware of the difficulties. To be aware of difficulties relates strongly to being aware of social norms of behaviour (the netiquette for specific situations online). Schoeman (1992) refers to these as ‘privacy norms’.

In the light of the open access movement, this analysis would suggest that acceptable open sharing can be maintained as long as all parties are aware of the social norms online (netiquette) guiding our sharing behaviours before we share information.

According to the ‘Adams (2001) sharing model’ behaviours can be broken down into three guidance points. Acceptable open sharing is achieved through maintaining accurate awareness of:

1. who we believe we are sharing the information with (information receiver)
2. how the information is going to be used, edited, re-used, and in what context (information usage)
3. how do those sharing the information feel about information sensitivity – attitudes in particular situations may vary depending on 1) who the information receiver is and 2) how the information is likely to be used.

Activity 4

Timing: 1 hour

1. Think of two or three scenarios that you would consider acts of privacy invasion or risks of this occurring (focus on personal information). These may be examples from personal experience, friends or ones which you have heard about in the news.

2. Consider if changing the context changes your perception? For example, if you are paying for a service (e.g. as a registered student) do you expect more than if you obtain that service for free (e.g. as an OER or MOOC user)?

Use the box below to record your thoughts.

Provide your answer...

Conclusion

The tensions between securing the advantages of openness while ensuring that appropriate safeguards have many dimensions – ethical, social, technical and legal. In this free course, *Networked practitioner: open or closed practice?*, you have started to explore these tensions and their implications for online educational environments and networked practice.

Hopefully you found this overview interesting and have made some links to the decisions about open and closed that you make in your work as a networked practitioner. To find out more about Open Educational Resources, you could move on to study the free course Open education, where you can explore several other facets of 'openness' in the educational context, including MOOCs. That free course is adapted from the Open University course H817 *Openness and innovation in elearning*, which is a companion course to H818 within The Open University's Masters in Online and Distance Education.

Keep on learning

Study another free course

There are more than **800 courses on OpenLearn** for you to choose from on a range of subjects.

Find out more about all our free courses.

Take your studies further

Find out more about studying with The Open University by visiting our online prospectus.

If you are new to university study, you may be interested in our Access Courses or Certificates.

What's new from OpenLearn?

Sign up to our newsletter or view a sample.

For reference, full URLs to pages listed above:

OpenLearn – www.open.edu/openlearn/free-courses

Visiting our online prospectus – www.open.ac.uk/courses

Access Courses – www.open.ac.uk/courses/do-it/access

Certificates – www.open.ac.uk/courses/certificates-he

Newsletter – www.open.edu/openlearn/about-openlearn/subscribe-the-openlearn-newsletter

References

Adams, A. (2001) 'Users' Perception of Privacy in Multimedia Communication', PhD thesis, School of Psychology, University College London.

Adams, A. and Blandford, A. (2005) 'Bridging the gap between organizational and user perspectives of security in the clinical domain', *International Journal of Human-Computer Studies*, vol. 63, no. 1–2, pp. 175–202, [Online]. DOI: http://dx.doi.org/10.1016/j.ijhcs.2005.04.022 (Accessed 24 May 2017).

Adams, A. and Sasse, A. (2005) 'The user is not the enemy', in Cranor, L. and Simson, G. (eds) *Security and Usability: Designing secure systems that people can use.* USA: O'Reilly, pp. 610–30.

Adams, A. and Sasse, M.A. (2001) 'Privacy in multimedia communications: protecting users not just data', *IHM-HCI'01*, 10–14 September 2001, Lille, France.

Bellotti, V. and Sellen, A. (1993) 'Design for privacy in ubiquitous computing environments', in de Michelis, G., Simone, C. and Schmidt, K. (eds) *Proceedings of ECSCW'93, the 3rd European Conference on Computer-Supported Co-operative Work*, pp.77–92, Kluwer (Academic Press), Netherlands.

Bernstein, B. and Solomon, J. (1999) 'Pedagogy, identity and the construction of a theory of symbolic control', Basil Bernstein questioned by Joseph Solomon, *British Journal of Sociology of Education*, vol. 20, no. 2.

Cronin, C. (2016) 'Openness and praxis: exploring the use of open educational practices in higher education', [online]. Available at https://www.slideshare.net/cicronin/openness-and-praxis-srhe (Accessed 24 May 2017).

Fiedler, S. and Pata, K. (2009) 'Distributed learning environments and social software: In search for a framework of design', in Hatzipanagos, S. and Warburton, S. (eds.) *Social software & developing community ontologies*, Hershey, PA, USA, IGI Global, pp. 145–58.

Goffman, E. (1969) *The Presentation of Self in Everyday Life*, Penguin Press, London.

Houghton, D.J. and Joinson, A.N. (2010) 'Privacy, social network sites, and social relations', *Journal of Technology in Human Services*, vol. 28, no. 1–2, pp. 74–94.

Ince, D.C., Hatton, L. and Graham-Cumming, J. (2012) 'The case for open computer programs', *Nature*, vol. 482, pp. 485–8.

Joinson, A.N. and Paine, C.B. (2007) 'Self-disclosure, privacy and the Internet', *Oxford handbook of Internet psychology*, pp. 237–52.

Kumaraguru, P. and Cranor, L.F. (2005) 'Privacy indexes: a survey of Westin's studies', Institute for Software Research. Paper 856, http://repository.cmu.edu/isr/856 (Accessed 24 May 2017).

Lave, J. and Wenger, E. (1991) *Situated Learning: Legitimate Peripheral Participation*, Cambridge, Cambridge University Press.

McAndrew, P. and Farrow, R. (2013) The ecology of sharing: synthesizing OER research, in OER 13: Creating a virtuous circle, 26–27 March 2013 [online]. Available at http://oro.open.ac.uk/37755/ (Accessed 24 May 2017).

Pearce, N. (2012) 'Developing students as content scavengers', OpenCourseWare Consortium Global 2012/OER 12 Conference, 16–18 April, Cambridge.

Preece, J. (2000) *Online Communities: Designing Usability and Supporting Sociability*, John Wiley & Sons, Inc.

Schoeman, F. (1992) *Privacy and Social Freedom*, Cambridge, Cambridge University Press.

Tapscott, S. and Williams, D. (2007) *Wikinomics; How Mass Collaboration Changes Everything*, London, Atlantic Books.

Vollmer, T. (2011) 'New federal education fund makes available $2 billion to create OER resources in community colleges' [Web log entry]. Available at:

https://blog.creativecommons.org/2011/01/20/u-s-department-of-labor-and-department-of-education-commit-2-billion-to-create-open-educational-resources-for-community-colleges-and-career-training-cc-by-required-for-grant-outputs/ (Accessed 24 May 2017).

Weller, M. (2010) 'Big and little OER', Open Ed 2010: Seventh Annual Open Education Conference, 2–4 November, Barcelona. Available at: http://oro.open.ac.uk/ 24702/ (Accessed 1 July 2014).

Weller, M. (2011) *The Digital Scholar: How Technology Is Transforming Scholarly Practice*, London, Bloomsbury Academic.

Wenger, E. (1999) *Communities of Practice: Learning, Meaning and Identity*, Cambridge, Cambridge University Press.

Whitten, A. and Tygar, J. (1999) 'Why Johnny can't encrypt: a usability evaluation of PGP 5.0', *Usenix Security*, vol. 1999.

Acknowledgements

This free course was written by Anne Adams, Martin Weller and Chris Pegler.

Images

Don't miss out

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – www.open.edu/openlearn/free-courses.