CS 978 – Legal, Ethical, and Professional Issues for the Information Society

CS 800 – Health Information Governance

Privacy

Introduction

This week we will set up the key issues for our discussion of UK data protection legislation next week with a consideration of the concept of privacy, and the issues that are at the forefront in the practice of information and computing professionals.

Perhaps the most famous definition of privacy was uttered by Supreme Court Justice Louis Brandeis in the case Olmstead v. U.S., 277 U.S. 438 (1928) where he defined privacy as "The right to be left alone—the most comprehensive of rights, and the right most valued by a free people." In more modern times, privacy has been interpreted as a right that we all should be entitled to expect to be defended. For instance, Article 12 of the *UDHR* states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Therefore, privacy is defined as a right that we all should be able to expect to be defended in law. However, the right of the individual to privacy is becoming an ever-increasing concern in the information society, as information about us can easily be exchanged between parties at the click of a mouse, across countries and continents. It is also extremely difficult to know when and if this occurs, and this poses major problems for any legislative body seeking to curb such excesses.

Defining privacy

Privacy differs from confidentiality and security; privacy is the overriding concept which involves the right to be left alone and the autonomy to determine with whom we share details of our personal lives or personal information. Confidentiality is a narrower concept. Violation of confidentiality undermines privacy but privacy can be achieved without confidentiality in that you can choose not to share your information in the first place and thereby not entrust others to keep it confidential. Security is necessary to maintain confidentiality and therefore privacy, as stored

data needs to be kept securely and be accessible to only those who need it for the purposes for which it was provided.

Of course, as we will see, privacy has also to be balanced against other values. As with other rights, there are trade-offs and competing rights and interests which need to be respected. Economic interests may cause consumers to trade privacy for convenience such as occurs in credit card shopping. Efficient government requires personal information for taxation, health care, and the like. Privacy can also conflict with publicly accepted principles of law enforcement and public safety, as it is not desirable for the work of criminals or terrorists to remain private if they break laws and threaten wider society.

It could be argued that privacy is beginning to become a potentially old-fashioned concept. The increasing desire of our governments and the businesses we use to know more about us is impinging more on our day-to-day lives. Registering for many web-based services sees us having to tick boxes to unsubscribe from mailings or to ensure we do not have our data passed on to "selected third parties." Individuals and organisations increasingly have to spend money on spam and junk mail filters to attempt to ensure that their email inbox is not stuffed with inappropriate emails offering dubious services. Providing such security measures is at the very least an inconvenience, and at the worst offers the potential for personal information to be abused or misused.

Further defining privacy

Privacy is the "right to be free from unwarranted intrusion and to keep certain matters from public view" (Law, 2015). As such, privacy is also an important element in the autonomy of the individual. Much of what makes us human comes from out interactions with others within a private sphere where we assume no one is observing. Privacy thus relates to what we say, do, and perhaps even feel. If we are not able to trust that we are in a private space, then we may not be completely autonomous, we may hold back crucial elements of ourselves. As Griffin has observed: "frank communication… needs the shield of privacy; it needs the restraint of peeping Toms and eavesdroppers, of phone taps and bugging devices in one's house, of tampering with one's mail or seizure of one's correspondence" (Griffin, 2008, p.225). Without a right to privacy, then, we are not able to be fully ourselves. Wacks also emphasises this point in considering the issue of electronic monitoring of employees: "the slide towards electronic supervision may fundamentally alter our relationships and our identity. In such a world, employees are arguably less likely to execute their duties effectively. If that occurs, the snooping employer will, in the end, secure the precise opposite of what he hopes to achieve" (Wacks, 2010, p.4-5). In summary, "knowledge that our activities are, or even may be, monitored undermines our psychological and emotional autonomy" (Wacks, 2010, p.4).

Equally, freedom of expression is also about autonomy and self-development. Barendt argues that “restrictions on what we are allowed to say and write, or…to hear and read, inhibit our personality and its growth” (Barendt, 2006, p.13). Achieving our potential as human beings is fundamentally about being able to seek out our own path, through access to knowledge that informs our worldview and way forward. Under this justification we can also see links between some other fundamental human rights such as the “rights to freedom of religion, thought and conscience” (Barendt, 2006, p.13).

Undoubtedly privacy can pose significant challenges to security. If an individual is seeking to commit a crime or a terrorist act, then arguably privacy affords him more opportunity to do so. The dichotomy is the heart of the tension between a right to privacy and protecting the legitimate interests of others, and the state.

What is important for us to understand in this context is that privacy is a right *qualified* by other interests. What we mean by this is that other rights may take priority over it. This is an absolutely rational notion, since unrestricted privacy could entail individuals undertaking activities that potentially damage the interests of others or society in general. It does, however, reveal that there is a tension between what a person might expect regarding privacy and what may be deemed to be encroaching on the rights of others in doing so. Whether we recognise it or not, the intricacies of this qualification lie at the heart of the controversies we face in our professional practice. Wacks identifies seven *shortcomings* of privacy that are important to consider:

1. Privacy is often perceived as an old-fashioned value: “an air of injured gentility”
2. It may conceal genuine oppression, especially of women by men, carried out in the private realm of the home.
3. It may weaken the detection and apprehension of criminals
4. It may hamper the free flow of information, impeding transparency and candour
5. It may obstruct business efficiency and increase cost due to the necessity to adhere to standards in the collection of personal information
6. From a communitarian viewpoint, privacy is individualistic and trumps community values
7. Withholding unflattering personal information constitutes a form of deception (Wacks, 2010, p.35-37).

The European Convention on Human Rights (ECHR) states both the right to privacy, and the limits that can be placed on it. Article 8 states that: “*Everyone has the right to respect for private and family life, his home and his correspondence.”* Section 8 (2) of the ECHR covers the limits that are allowed to be placed on the right to privacy specified in 8(1): *“There shall be no interference by a public authority with the exercise of this right except such as is in*

accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In reality, what does this mean? Firstly, that any restrictions placed on the right to privacy by states must be *lawful*. There must be a legal basis for the intrusion, and it must be justified by existing legislation. Framed as they are we can see here a set of restrictions that advocate invasions of privacy only in terms designed to protect what are deemed to be the legitimate interests of others, whether in the body politic or in their own right.

Towards the protection of data

Data protection began to concern society in the late 1960s and early 1970s when the dawn of new technologies made it possible for organisations to electronically store information on individuals. There are other issues related to why the protection of data and the right of a person to decide what happens to their own personal data have become high profile issues. As mentioned above, the ease at which the personal data of individuals can be passed around has increased. We are increasingly seeing cases in the news where data on laptop computers, discs, or memory sticks has gone missing or been found by someone who had no right to access it. Such cases raise major concerns for citizens and highlight even in countries with robust data protection legislation how the carelessness of human beings can bring the issue negatively to public prominence. In addition, both the increasing use of customer profiling in a business context, and the tracking of customers in online environments to offer them more tuned services to their needs, despite being on the face of it a positive use of data, are also subject to abuse.

Therefore, the growth in the amount of information being gathered on individuals and the creation of large databases, not least by government, combined with the ability to link information across such databases, have brought the issue of data protection to the attention of the public. Growth in database marketing and the activities of credit reference agencies which utilise such large databases have also led to increased public awareness about how much personal information is held in electronic form and the negative consequences which can ensue should such information be found to be inaccurate. There is also growing concern over civil liberties and personal privacy especially in respect of personal data contained in, for example, medical, financial and employment records. We will discuss these issues in more detail next week when we address the UK legislation related to data protection.

The cookie context

A primary concern for EU legislators relates to the ubiquity of cookies, the small files that download to a person's computer when they browse a website in order to track activity and allow

the user a more enhanced experience. As much as cookies are essential for ecommerce solutions, they pose significant privacy concerns, as they store user activity while they are using websites, but can also track behaviour across the web. In an analogue world this would be the equivalent of a customer walking into Marks and Spencer's, using their credit card to buy an item, and then being followed around other stores afterwards by someone who is making notes on their purchases. This is clearly an invasion of privacy and goes against the spirit of data protection in the EU.

EU Directive 2009/136/EC of the European Parliament and of the Council has laid down the parameters of cookie use across the EU, and compels member countries to address its provisions within their own national legislation. The key element that relates to cookies within the Directive states that the placing of cookies on a browser's computer is "only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC." The emphasis then is that a user must *opt-in* to receiving a cookie, and in doing so they must have been given access to information as to what that cookie will store about them, and why. In this context we are dealing with the concept of *informed consent*, which has a history in EU Directives on data protection (Borghi et al, 2013, p.109). In other words, users "must understand the facts and implications of an action to be able to make informed choices, ensuring that they are effectively able to choose freely and voluntarily" (Borghi et al, 2013, p.120).

This links to the important point that the "cookie directive", as it is commonly known, builds on pre-existing EU Directives related to data privacy, and thus forms the next link in a chain. *Directive 95/46/EC*, is the backbone of data protection legislation throughout Europe, and is an important component in privacy law, and *Directive 2009/136/EC* itself was an update to *Directive 2002/58/EC* which first dealt with the issue of cookies amongst other issues related to electronic privacy and transmission of data. Thus within the EU we can see a natural evolution of data protection law that now encompasses the threats to privacy posed by cookies and the tracking of user behaviour in the online space. A robust data protection legislative framework incorporating challenges to online privacy can be seen as EU legislators moving with the times and addressing the significant issues presented by new technologies.

The citizen factor

We can trace, then, a clear EU focus on online privacy and actions to legislate to protect the rights of citizens. The elephant in the room, however, is the behaviour of citizens themselves when using online services.

One of the common paradigms of the modern era is the notion of customisation of services to users. In an online environment the use of cookies for a user could well be a good trade-off with

regards their privacy, if the experience they receive from the website is more tailored to them. However, this tailoring comes at a cost, the loss of part of their privacy. This is perfectly fine if the informed consent concept we discussed earlier is a part of the process; however, research on the awareness of cookies amongst the population suggests this is far from the case. The Information Commissioner cites a report conducted in the UK for the Department for Culture, Media and Sport that raised some significant issues:

- 41% of respondents were unaware of different types of cookies
- Only 13% indicated they fully understood how cookies work
- 37% had heard of cookies, but did not understand how they work
- 37% did not know how to manage cookies on their computer

We can see then a significant problem with regards the actual issue that is being legislated against. If people do not understand the nature of what they are being protected against, how can the legislation be effective?

We must also consider here the concept of *engineered consent*, which in contrast to informed consent is built around consent being given because the user essentially has no choice, if they wish to receive the service provided. As Borghi et al state, "if data subjects have to give more information than is strictly necessary to buy goods or access services, then it is likely that they will consent to whatever broad uses of their data to obtain the goods or services" (Borghi et al, 2013, p.120). If the user *not* accepting cookies on their computer means the service they will receive will be of lesser quality, they may trade off in their mind consent for the service versus their privacy. Such a process has arguably coercive elements to it that we must be wary of. Similar scenarios apply with social media and email accounts: is not having them a worse scenario for a citizen than actually having them?

Conclusions

We can see that privacy has been defined as a fundamental human right both by the United Nations, the EU, and by many national governments. Despite the shortcomings of the concept, and the potential dangers it presents, privacy matters to us as human beings: "privacy stakes out a sphere for creativity, psychological wellbeing, our ability to love, forge social relationships, promote trust, intimacy, and friendship" (Wacks, 2010, p.34).

How privacy is afforded in countries can vary, but one of the most fundamental approaches lies in the provision of data protection legislation which offers individuals rights in law as to what can be done with their personal data.

We will explore how this has been addressed in the UK next week.

For an excellent critical discussion of the philosophical approached to privacy, please read:

Nissenbaum, HF 2009, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Redwood City. (Highly recommended Part II: chapters 4 thru 6)

This is an eBook, and the link is available on MyPlace.

References

Barendt, E. (2005) *Freedom of Speech*. 2nd edition. Oxford: Oxford University Press.

Borghi M, Ferretti F and Karapapa S. (2013), 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK' *International Journal of Law and Information Technology* 21

Griffin, J. (2008) *On Human Rights*. Oxford: Oxford University Press.

Information Commissioner, (2012) *Guidance on the rules on use of cookies and similar technologies*.

Law, J. (2015) *Oxford Dictionary of Law*. Oxford: Oxford University Press.

OHCR (2005) *Universal Declaration of Human Rights*. Available from: www.un.org/en/documents/udhr/ [Last accessed: 30th September 2016]

Wacks, Raymond. (2010) *Privacy: A Very Short Introduction (Very Short Introductions)* Oxford University Press.

Further Reading

ADAMS, Andrew A. and McCRINDLE, Rachel J. (2008) *Pandora's Box: social and professional issues of the information age*. Chichester: John Wiley and Sons. **Chapter Seven**.

PEDLEY, Paul. (2012) *Essential Law for Information Professionals*. 2nd edition. London: Facet Publishing. **Chapter Seven**.

DMcM/09-2018