CS978 – Legal, Ethical and Professional Issues for the Information Society

Week 1 – The information society

Introduction

If you are part of what has been dubbed the *Google Generation,* it might be difficult to imagine a world before information was the main driving force of the world economy. Yet the emergence of the Internet, and preceding this, the **information society**, are relatively new influences in human history.

What is the Information Society?

We are now in a phase of history that has been dubbed the **post-industrial society** (Bell,1973). Bell characterised this world as one that is increasingly moving from a reliance on the production of tangible goods to a reliance on the production and management of information. Another prominent writer on the information society was Yoneji Masuda who argued that the dominant forces in the emerging society would be those that support the production of information (1980). Masuda means that what will drive society will be the formation and management of the infrastructure that supports the information society. For example, the industrial revolution was supported by canals, roads and railway lines, and we can compare this to the telecommunications and computing revolutions that have supported the growth of the networked society. Just as it was impossible to move tangible goods such as coal, cotton, or steel without the appropriate infrastructure, it is impossible to transport many information products without broadband Internet access.

As early as 1962 in a report on the emergence of knowledge production in the USA, Machlup defined what he felt were the information industries:

- Education
- Media
- Information machines (Computers and ICTs)
- Information services (Software and online services)
- Other service activities (not for profit and research & development) (Machlup, 1962)

Almost five decades on we can see that what were essentially emerging industries in the time of Machlup are now the cornerstones of our economies. Only twenty years ago the average Internet citizen had a modem that delivered speeds of 56k, and to this user the downloading of multimedia such as music and films was slow and impractical. Nowadays speeds of 100 times those of ten years ago are commonplace, with companies now currently advertising broadband speeds in excess of 500MB a second.

Governments and the Information Society

The relationship of governments with information and the various organizations, departments and other bodies connected with information creation, storage and dissemination is a complex one, made more so by rapid changes in information and communication technologies. This simply adds to the problem: legislation and policy are constantly trying to 'catch up' with developments and the ways in which people use those developments. In some instances, there is a perceived role for government (depending on the political ideology of the country concerned); in other cases, it will be regarded as a problem for the information industries themselves to control in some way, often by establishing a code of practice enforced by an industry-representative body.

Consider, for example, the way in which social networking sites such as YouTube and Facebook have been used to post offensive and potentially defamatory material about schoolteachers or to show bullying incidents at school. Teachers' trades unions in the UK have called at times for legislation to ban such postings, and at other times for the sites' providers to remove the material (Goff, 2007). The problem, as always, is how to prevent abuse of the technologies without adversely affecting the desirable uses. Social networking sites clearly meet a need among some sections of the population: how do we encourage that without also encouraging abuse? It we allow users to access such sites in response to acknowledged demand, are there ways in which we can ensure that defamatory or offensive material is not viewed or uploaded? If we do that, are we then guilty of censoring the users? It is often seen as a better, and a more justifiable use of resources, simply to block access to such sites, as is done in some public and school libraries. In doing, so we raise fundamental questions regarding freedom of access to information, and freedom of expression.

Information Policy and Strategy

The constant need of government and its agencies to catch up with technological developments and uses has tended to mean a piecemeal, reactive approach to policy and legislation, despite the recognition in the 1980s that the development of the information society and the 'information superhighway' demanded a long-term and far-seeing (as far as possible) policy. Few nations, therefore, have a *single* information policy, but rather a collection of (sometimes contradictory) policies on specific aspects. For example, governments in the developed countries want to stimulate e-commerce because of its efficiency and effectiveness, its potential to reduce overheads, and so on. However, the commercial organizations involved, while also recognizing the benefits of e-commerce, are concerned about the confidentiality of transactions, protection of customer data (where they have legal obligations as well), for example, and so wish to employ strong encryption techniques for this purpose. Governments, however, are worried that strong encryption could be used to hide criminal or terrorist activities and so are less favourably disposed towards it. This tangle of issues and concerns is made worse by the number of actors which information policy formulation requires. We can list the following organizations and groups and their interests or involvement in one or more features of information policy (this is probably not a complete list of the interests of the various actors: you are invited to consider what others might be relevant):

-*government*: economic development and an informed citizenry, while abuses of the technology are prevented; precise approaches will depend on ideology (freedom of information vs. censorship or control of content)

-*political parties*: ideological approaches to specific issues

-*the civil service*: responsibility for ensuring implementation of policy, but with its own vested interests (e.g. over freedom of information)

-*the private sector*: encouragement of industry, research, use of e-commerce, marketing, etc.

-*pressure groups*: ability to use the technologies to promote interests

-*professional associations*: regulation of professionals involved, maintenance of relevant standards

-*international bodies*: international regulation and policies, development of international standards

-*regulatory agencies*: monitoring and control, implementation of standards

This list gives an indication of the numerous factors which have to be taken into account and which go some way to explaining the sometimes contradictory nature of information policies. One way to remove some of the complexity and, more importantly, the contradictions would be to consider the key issues in information policy which impinge both on the development of information resources at a national level and their exploitation and then involve government departments and so on as required. For example, in addition to involvement as appropriate in the technical infrastructure (e.g., the promotion of technical standards to ensure reliability and compatibility), governments need to address the following issues:

-*freedom to publish information materials* (i.e., what is and is not permitted?)

-*protection of information and information rights* (copyright and intellectual property, piracy, hacking, e-mail scams, data protection, rights of access balanced by rights to privacy)

-*market development, including investment and export* (e.g., pricing of information for basic provision or revenue generation for value-added services)

-*availability of skilled people to exploit and develop information resources* (educational and training programmes to meet society's needs)

Responses to these by the relevant bodies will, as we have suggested, depend on the ideological slant of the government of the day, and are thus liable to change with a change in government. Governments may also change their stance on a particular issue in the light of public opinion or the working out of the legislation in practice. In the UK, for example, Members of Parliament tried to amend the Freedom of Information Act because it could be used to reveal details of their expenses claims, memberships of other bodies and so on, claiming that the legislation might not protect private correspondence with constituents (Hencke and Mulholland, 2007). Legislation can also, of course, be affected by major unforeseen developments, of which one of the most recent affecting Europe and North America has been the so-called 'war on terror'. Since 2001 this has led various governments to introduce new legislation in a number of areas that impinge on information policy.

The legislative response

We can identify a set of legal and/or moral issues on which governments have legislated or created standards which, it is suggested, have implications for information policy and consequently for information and computing professionals in their daily working lives. These include:

• *content* (what is and is not permitted)
• *privacy* (is it a fundamental right? When might it be overridden by the state?)
• *cyber-crime* (using the internet to commit 'old' crimes and the rise of new ones)
• *monitoring use of e-resources* (when does this become an infringement on privacy, and when is it justified?)
• *protecting intellectual property* (how do we do this on the web?)
• *freedom of information* (just how 'free' should it be?)
• *human rights to privacy, to information* (when can these be set aside and by what demands?)
• *cyber-terrorism* (how can we identify the ways in which terrorists are using the internet?)
• *health and safety* (are our computer terminals safe for staff and users?)

The detail of legislation on these issues will differ from country to country (a further complicating factor in the establishment of the 'global village' or of a consensus on the use of the internet and web). Compare, for example, attitudes to content in the USA, where it has constitutional *protection* under the First Amendment, with the German constitutional *prohibition* of content relating to Nazism and Holocaust denial. Look at the way in which China prohibits its citizens from accessing online information relating to the events in Tiananmen Square in 1989. In the UK in the 2010s riots in English cities saw calls from senior members of the current government to ban the use of social media and Blackberry Messenger services, as these were seen to be mechanism for organising the riots. Some of these issues (such as cyber-terrorism) are new, a direct result of the development of online resources, but in some cases (e.g., the protection of intellectual property) they have existed in relation to printed media for a very long time: the question has become one of whether we simply extend the existing legislation to include the new medium of the internet or develop new laws. Intellectual property rights protection is an example of ensuring that existing legislation, modified where required, is adequate to the task. 'Phishing trips', in which users are tricked into providing personal information such as bank account details and passwords to websites masquerading as legitimate ones, are new crimes and require new legislation (though some might argue that laws on prevention of fraud could cover such activities).

Below are listed some ethical and legal concerns related to the information society, and how their legal provisions might impact on you as information and computing professionals (the relevant UK legislation is added in brackets:

-*intellectual property rights*: (Copyright, Designs and Patents Act 1988)

-*privacy of personal information*: (Data Protection Act 1998; Human Rights Act 2000; Investigatory Powers Act 2016)

-*improper use of computer systems*: using computers to hack into systems or to plan criminal or terrorist activities; (Computer Misuse Act 1990; Anti-Terrorism, Crime and Security Act 2001).

-*local and national government activities and those of publicly funded bodies*: provision of information in various formats; access to information; advice on access to information (Freedom of Information Act 2000; Human Rights Act 2000)

We will discuss a large number of these Acts and consider the ethical implications of them in future lectures.

The Digital Divide
Of immense importance to consider is what has been dubbed the digital divide. Feather gives this topic a large treatment in his peerless work on the information society (2013). In considering the digital divide, it is important not only to consider it in a global context but also a local context. Focusing on the global issues firstly, and although the economies of the west are at the moment in somewhat of a bleak period, much of the growth of the late 1990s and early 2000s was related to the possibilities afforded by the information society. Loans and other financial services have increasingly been offered by banks and financial institutions able to operate outside of their own country of foundation, and indeed this was one of the key factors in the UK banking crisis, as the retrenchment of the foreign banks in the wake of the economic downturn led to significant gaps in lending availability in the UK. This boom (and subsequent bust!) was possible because of the increasing sophistication of ICTs and tools for undertaking e-commerce and e-banking, leading to a global marketplace in financial services. Without an ICT infrastructure and the skills in their populace, developing countries have major challenges in benefitting from such economic advantages. On an even more basic level, developing countries also miss out on the social and educational benefits the information society brings.

Even in the so-called developed world, the digital divide is a sociological problem of great note. It is crucial as information professionals that we seek to play our part in addressing the issue of digital exclusion. Chapters four and five of Feather (2013) deal with the economic and political issues related to the digital divide.

Crucial issues to ponder

In the weeks to come of this class it is important that you not only become familiar with the laws that govern the information society, but also what impact those laws have on individuals, and on wider society. As future professionals in information and computing science, you must also consider the ethical issues related to the laws governing information creation, dissemination, storage and use, and your own role in both administering the laws, and your responsibility to do so ethically.

References

Bell, Daniel. (1973) *The coming of post-industrial society.* New York: Basic Books

Feather, John. (2013) *The Information Society: a study of continuity and change*. 6th edition. London: Facet Publishing.

Goff, H. (2007) Websites Urged to Act on Bullies http://news.bbc.co.uk/1/hi/education/6539989.stm

Hencke, D. and Mulholland, H. (2007) Lack of Lords Sponsor Wrecks Plan to Exempt MPs from FoI Act, *The Guardian*, 14 June.

Kellerman, A. (2000) Phases in the rise of the information society. *The Journal of Policy, Regulation & Strategy for Telecommunications & Media.* 2 (6) pp.*537-541.* Available from: http://www.emeraldinsight.com/10.1108/14636690010801708

Machlup, Fritz (1962) *The production and distribution of knowledge in the United States.* Princeton, NJ: Princeton University Press.

Masuda, Y (1980) *The Information Society as Post-Industrial Society*. Washington DC: World Future Society.