Conceptual Issues in Cyberspace

MIT3107/3207/M207

Gary Stringer

Creative Media and Information Technology

University of Exeter, UK

Conceptual Issues in Cyberspace: MIT3107/3207/M207

Gary Stringer

Abstract

Module Purpose. This CMIT module can be taken for 15 or 20 credits, at level 3 or level M. It examines the role of the Internet in today's society, and discusses the problems the information society is bringing about.

Legal Notice

Table of Contents

Preface

As the Internet grows, it begins to have an impact not just on the way we use our computers, but on the way we live our lives too. The effects of mass communication are already apparent in the way we inhabit the “global village”, but these are just the beginnings of a massive social and cultural change. We are moving towards an information society.

This module looks at how the Internet has already changed the world for almost everone in it. It examines the benefits, problems, and moral dilemmas that the Internet has presented, and looks to a future where the Internet will be even more ubiquitous and influential.

GBS

Chapter 1. Education and Research

One of the earliest visions of networked, hyperlinked information was based around the concept of a library, designed for education and research (Bush 1945). This rôle has been in the forefront of the development of the Internet for most of its history, only recently being superceded by commerce as its major driving force. So how can the Internet help us learn?

Higher Education

- self-directed learning
- content delivery - web-based notes and lectures
- content negotiation - online seminars, tutorials and feedback

In higher education, the emphasis for learning is providing self-motivated students the means for self-directed learning, as well as providing learning content in the form of lectures or notes. The Internet can facilitate each of these areas, both for face-to-face learners and over long distances.

Delivering learning content effectively

- Online course notes allow easy access to course content
- “Taking notes” becomes “making annotations”

The process of learning, whether online or in a traditional, face-to-face environment, involves two basic operations. The first, *content delivery*, concerns the effective dissemination of knowledge, in the form of lecture notes, reading materials and other information. The content may be verbal (lectures), textual (books, handouts, web pages) or multimedia (audio cassettes, CDs, DVDs, podcasts, streamed media), but is primarily a one-way transfer of knowledge from the tutor to the student.

Content delivery is often now achieved by electronic means. The Open University pioneered the use of audio cassettes and broadcast television to transmit knowledge, but it and many other institutions are now moving to web-based delivery, providing notes, audio clips and streamed video across the Internet. This allows easy and flexible access to the materials, when and where the student wishes, encouraging self-paced learning.

Computer-based notes can also help with note-taking. Adding annotations to existing copy, or being able to copy and paste sections of the notes or quotes from the text allows more accurate annotation. Where multiple online materials are available, methods of *knowledge assembly* (assembling ideas and facts from a variety of sources) can create a broad picture of a subject, a key skill in learning.

Negotiating content online

- Feedback is necessary to ensure effective learning
- Student-to-tutor email, mailing lists and web forums
- Chat rooms, Instant messengers, Facebook
- Videoconferencing?

In additon to delivering the knowledge, there needs to be some *content negotiation* as part of the learning process. This involves the student using the knowledge gained in controlled situations, such as seminars, feedback exercises and tutorials. The important part of this process is that the student modifies their view of the information gained with the help of the tutor (or their peers). This tweaking of knowledge is important to both develop and affirm that the the topic has been properly understood.

In computer mediated learning, there are several ways in which this content negotiation can be achieved. Most simply, exercises may be completed online, either being submitted to the tutor to be hand marked, or in some cases being marked by computer, the latter often giving immediate feedback.

For more complex learning tasks, a human element is more vital. Seminars and tutor groups can be facilitated using chat rooms, MUDs/MOOs, Instant Messenger applications, or ideally, videoconferencing.

A case study in this last method can be seen in the ReLaTe project [http://pallas.ex.ac.uk/pallas/relate/] (rather old, but still relevant).

Self-directed learning tools

- e.g. Blackboard, WebCT and Moodle
- Designed for distance-learners
- Commonly used to facilitate all types of learning
- Research needs to be done to evaluate effectiveness

As Internet technologies have developed, most have been adapted in some way for educational use, with varying degrees of success. The most obvious use is content delivery over the web, but with more interactive technologies there are more interesting possibilities.

There are now a number of learning environments which allow greater interaction with the content, giving a degree of content negotiation even for virtual participants. The University uses WebCT as its *Virtual Learning Environment* (or VLE), but others are widely used including Blackboard, Moodle and Bodington.

The main advantages of using VLEs rather than traditional content delivery mechanisms are the level of monitoring of student progress (typically, the tutor can track each student as they view the material and gather statistics about access times and durations), and the possibilities for testing and feedback, which again can be monitored easily.

VLEs are evolving still, and there is still some debate as to their effectiveness. Some theorists believe that the VLE is only suited to certain types of tasks, and many feel that the design of current VLEs needs significant improvement before we reach the optimum for effective learning across a wide range of students. Often, the user interface can be restrictive towards some learners, limiting their effectiveness in the learning process.

Resource-based Learning

- Learning through examining evidence - online or off
- Limited by what is available
- Could the Internet be the ultimate library of all knowledge?
- How can we judge the authority, reliability and accuracy of information?

To some extent, higher education has always placed a high value on learning resources such as books, journals and even audio and video. However, the expansion of the web has made available a library beyond the dreams of any University librarian, having both broad coverage and detailed depth. However, it is not without it's problems, and judging the usefulness or authority of a resource found on the Internet can be a difficult process, especially for the novice.

Digitising resources for preservation

- preserves rare or delicate resources in digital format
- provides wider, more flexible access to key resources
- needs a rigorous approach to give accurate preservation

As the demand for online resources grows, we need to think about how this information is stored and delivered. Storing data in formats that are inappropriate may limit its usefulness or accessibility. Formats that only work on one platform (one type of computer, eg PC or Macintosh) may prevent many people from seeing that data. Similarly, many current formats are proprietary, working only with one software developer's products, and with little documentation on how they are structured available in the public domain, which means that in future years the data may be irretreivable without resorting to preserving the exact software and hardware combination needed to run the original application. Many formats can only store certain types of data, and will lose information if used for other purposes. There are many pitfalls to preserving data and making it accessible to all users.

One way around these pitfalls is to use a standards-based format for archiving data. Markup languages such as HTML are defined extensively and precisely in their own standards documents (for HTML, these are produced by the World Wide Web Consortium, the W3C [http://www.w3.org/]). Some of these languages are produced for a specific task, to archive a specific document type; an example is the Text Encoding Initiative (TEI) [http://www.tei-c.org/] which provides markup tags specifically for preserving humanities texts, such as manuscripts, novels, plays and poetry. These languages often preserve the minutest details of the original, such as notes on the typography and binding, on any handwritten notes in a manuscript, or on any damage to the original copy.

Here the intention is to preserve and disseminate a detailed description of the document original, so that anyone around the world can study that document without travelling to the document's physical location, and perhaps more importantly, without handling what may be a valuable and fragile original (Hollingham 2004).

There are growing archives of material on the net. For example, Project Gutenberg [http://www.gutenberg.org/] contains simple text files of a huge range of novels and other books. A more standardised and rigorous project is the Oxford Text Archive [http://ota.ahds.ac.uk/], a preservation project using TEI, XML and other SGML languages.

Preservation by Digital Surrogate

- increases access to otherwise inaccessible resources
- prevents damage to fragile originals from continual handling

With some resources, the best way to produce a digital copy is to photograph the manuscript, and allow the web-reader to page through the graphics so produced. Examples of this type of *digital edition* include Caxton's edition of Chaucer's Canterbury Tales. Here, the significance of the manuscript is as much the look of the pages as the textual content, as this was one of the first printed books in English.

Producing this edition of a very valuable and fragile manuscript allows many more people to access it, both from the scholarly community and from the wider public.

Photography alone does not, however, produce a searchable version of texts, so further efforts must be made to transcribe the contents into an accessible and searchable form. Common formats for this include TEI, a form of XML markup specifically designed to capture original features of manuscripts and printed material.

Providing public access to public works

- culturally significant material can be made publicly available
- may be restricted to out-of-copyright material

This access is particularly important for publicly-owned works, where there is a significant investment on the part of the state to preserve or restore a work. A great deal of research funding is tied now to creating accessible resources of items held in otherwise inacessible libraries and archives.

There are still problems with *resource discovery* - often, these digital resources are held on institutional servers and are not widely publicised. There are a few relatively comprehensive catalogues around, such as the AHDS Cross-Collection Search [http://ahds.ac.uk/collections/index.htm] and the Intute [http://www.intute.ac.uk/] catalogue.

There are, of course, often problems with copyright for many resources, and this leads to a strong bias in available resources to those that are out of copyright. Often, the most accurate texts or up to date research is ignored, because only an original that is decades old is available for digitisation.

Creating electronic documents

- Writing compatible documents
  - use open formats written in an open metalanguage
  - use encoding standards (e.g. TEI, HTML/XHTML, DocBook)

There are also other markup languages designed for creating documents rather than preserving printed copy. The notes you are reading were created originally in a home-grown SGML-based markup language, and converted to web or printed form. Once a suitable standard document type became available, they were easily converted, and are now created in a modern, standardised, XML-based markup language, called DocBook [http://www.docbook.org/].

SGML, Standard Generalized Markup Language, is what's known as a *metalanguage* , it's used to define other markup languages. Both TEI and HTML are defined using SGML, as are many other types of document. Because the language (whether HTML, TEI or any other) is defined using a common metalanguage, and is defined precisely and completely by the metalanguage, it's much easier to write software to edit and convert documents in that language.

Unfortunately, SGML is rather unwieldy; it's difficult to learn and has a bewildering array of features unnecessary for most applications. A “cut-down” version, called *XML* or Extensible Markup Language, is now becoming widely used--even in products such as Microsoft Office. XML is also making an appearance on the web, initally with the “XML-isation” of HTML into *XHTML*, and eventually with fully-fledged XML documents being made available.

The important idea here is the standardisation of documents and document definitions. Without standards, the web falls apart, since the clients used to access the data must speak the same language as the servers that store them. An example of this is HTML, where the

incompatibilities caused by browser designers building in “enhanced features” occasionally means that pages created for one browser cannot be viewed with others.

The social life of documents

- Standardisation can give information a better social life
  - easy to search and extract information (data mining)
  - easy to convert to new formats, house styles, corporate identities
- Metadata can help documents find friends...

Use of standards also allows documents a greater “social life” -- they are accepted and converted in more situations than a single proprietary-format document could be (Seely Brown and Duguid 1996, 2000). Search engines could not operate if documents did not adhere to the HTML standard (however loosely), as they just wouldn't know how to read the documents. And standard additions to the HTML language such as *Dublin Core* or *RDF* allow search engines to “data mine” your documents more effectively. These additions add *metadata* (i.e. data about the document) which can be used by search engines and indexers to categorise the information that the document contains.

Search and retrieval of information is now such an important issue that many businesses and organisations are storing all of their internal documents as SGML or XML to aid searches, to allow easy conversions, to prevent information being inaccessible when software is upgraded, and above all to create logically structured and easily written material from the start. Documents that are *born digital* and written in a standard format are easier to convert to each new corporate style, as the presentation can be overlaid onto the document when needed.

As we move deeper into the information age, managing information will become critical. We are producing more information than we have ever done before, and the important question for researchers is not “How do I find information?” but “How do I filter out all the unneeded information?”

Other Research Perspectives

- Web began as a research application
- Originally designed to freely share information
- Commerce models have imposed new expectations on web
- New potential with Grid Computing, etc.

The Internet was created as a research network, enabling scientists to share their latest research expediently and allowing swift responses to proposals and drafts of articles and

papers. The World Wide Web was conceived to extend this, providing a simple universal language with which to present ideas and link them together (Berners-Lee 1999). Now that the Web has grown beyond all recognition, moving towards a more commerce-driven model, that spirit of sharing may be being lost.

One up-and-coming group of technologies which has restored this co-operative ethos is *Grid Computing*, which has elements of data and processor sharing, and encompasses synchroous communication technologies including videoconferencing. For more details, see the Grid Support Service [http://www.grid-support.ac.uk/] and the Access Grid Support Centre [http://www.agsc.ja.net/].

Has the Internet helped or hindered research?

- Information overload or access to unprecedented amount of data?
- Better research, or more research of poorer quality?
- Is it possible to increase resource quality and quantity?

The Internet provides more information at the push of a button than has ever been available before. Has this revolutionised research, or has it merely caused information overload? The wide range of information available, and the variable reliability of what's actually there, has caused concern.

Collaboration is important to effective research, and the Internet has to some extent revolutionised the way joint research projects are conducted. Email allows results and draft reports to be communicated quickly and easily. Audio- and video-conferencing can also be used to hold meetings and discussions.

How are technologies affecting scholarship?

- Text analysis and authorship studies
- Broader comparison of results
- Immediate access to new research
- The Web as the subject of study?

The textual database has created a new relationship between scholar and text; the scholar can discover relationships and gather statistics without “knowing” the text as would have

been the traditional method. In the past, relationships within and between texts could only be discerned through continual reading and rereading of texts and the recall of previously read texts. Now, with fast search and retrieval capabilities of database management systems, links between texts can be discovered without even reading them through.

The Internet adds another dimension to this new relationship. The availability of texts online increases the scholar's scope and allows more diverse relationships to be discovered. The scholar has access to a wider range of texts from a variety of sources, not just from libraries that are geographically accessible to them. Often, rare and difficult to find texts are made available, some so rare that most scholars would have no chance to experience or consult them otherwise.

And in a sense, the World Wide Web is an increasingly more extensive textual database, of language material both academic and colloquial. This forms a resource particularly valuable to linguists and cultural investigators, but can also provide material in many other disciplines, especially in showing how our society is influenced by factors under study.

The Internet in Schools

- should Internet skills be part of the core curriculum?
- how can the Internet be used effectively in existing subjects?
- can schools keep up to date with rapidly advancing technology?
- does the Internet distract or enhance teaching of core subjects?
- how do we make the Internet safe for children to use?

The Internet is seen as a mixed blessing by many schools. On the one hand, it provides access to almost limitless resources, but on the other, it stores much that may be considered undesirable or dangerous for children to view.

How will schools use the Internet to enhance their teaching?

- Computers *will* become ubiquitous in the classroom
- They *will* be Internet-connected
- They will usually be used to support all learning types and subjects

Many schools are already connected to the Internet, and within a few years, most UK schools should have access to the resources of the web. In the US, it's now common to have a PC in each classroom, available for students to use for researching projects.

Internet resources are already widely used to supplement traditional learning resources, and this use will grow as we develop more effective methods for safe access, and as web resources grow in quality and quantity.

Will schools be able to keep up with rapidly advancing technology?

- Is technology essential where budgets are already stretched?
- Is it more important than other core areas (text books, sports equipment, etc.)?
- Teacher training is needed to stay up to date

Financial and human resources are a constant problem for schools, and technology can make excessive demands on both. Running a computer network, monitoring Internet connections and maintaining levels of security take considerable time, and usually need a full-time system administrator. Teachers, in many cases already overworked, are required to learn new skills. And, of course, the technology rapidly goes out of date, so that the shiny new computer lab installed two years ago now looks outdated and in need of more investment.

Is the Internet just a distraction from the teaching of core skills?

- Should education concentrate on core skills more than ICT?
- Is ICT now a core skill?
- Learning about technology can be a fun activity

It is often claimed that the Internet, and computers in general, are taught to the detriment of core skills such as reading and writing, that computers distract us from getting the basic bedrock of education correct. It's perhaps too early to tell whether this is the case, though many small-scale studies have taken place already. These mostly indicate that using computers can significantly improve career prospects later in life, and can provide an interest to students who are struggling with more traditional core learning tasks.

Should Internet “research” be encouraged?

- The copy/paste culture
- Plagiarism detection methods
- Google and its effect on our memory
- Towards intelligent knowledge assembly

Should we limit access to certain areas of the web?

- The Internet is a dangerous place -should we restrict children's access to it?
  - Locally mirrored “safe sites” copied to school network
  - “Walled gardens” restrict access to known “safe sites”
  - Content filtering used to block “unsafe sites” or content
- Discuss the problems inherent in these approaches

The National Grid for Learning [http://www.ngfl.gov.uk/] has some guidelines [http://safety.ngfl.gov.uk/] for the “safe use of computers and the Internet”. There are several ways of limiting access to parts of the Internet. Firstly, we can use a *local mirror* to provide access to a very limited subset of the 'net: a copy of the required website is made on a local computer, and access is restricted to this computer. Secondly, we can use what have come to be known as “ *walled gardens* ”, where access is restricted only to certain websites, which have been vetted for appropriate content. Thirdly, we can use a *content filter*, often incorporated into a *firewall*, to analyse incoming information for inappropriate words and phrases, blocking them or their site of origin if necessary. None of these ideas are totally acceptable; the first two limit the student's freedom to follow up hyperlinks external to the selected material, and the last often filters much that is inoffensive or innocent.

See also the BBC's guidance [http://www.bbc.co.uk/schools/help/safety.shtml] on Internet safety in schools.

Chapter 2. The Virtual Marketplace

For some introductory reading on the types of online business and some of the issues surrounding them, see [4]. A more comprehensive treatment of the practical aspects of e-commerce can be found in [59], especially Chapter 9. For a full synthesis through the window of economic theory, see [29], and for a wider look at the social and legal issues surrounding e-commerce, look at [7].

Trends in the Digital Economy

- What happens when an economy goes digital?
- How have businesses adapted to the new economy?
- What new business possibilities have arisen online?
- What about non-monetary economies?
- What problems have emerged from digital economies?

Information becomes a commodity

- Commodities are entities that have intrinsic value.
- Information often has this property, especially when in digital form.
- In particular, personal and customer information has high value.

Information exchange is vital

- In the business-to-business realm, good data exchange is essential
- May involve stock availability, document exchange, financial data
- Money transfers often completely virtual

Markets become global

- The concept of business “space” replaces physical “place”
- Everyone in virtual space has access to the global virtual market
- Niche markets become viable as their reach extends globally

In what has become known as the “Long Tail” [2], many businesses are now able to specialise to a degree previously unknown and uneconomic; the Internet provides access to a market so wide that any interest, no matter how unusual, is marketable to.

Disintermediation and cybermediaries

- Internet allows direct dialogue with manufacturers
- Traditional intermediaries must therefore evolve

- Cybermediaries enable small businesses to access large markets

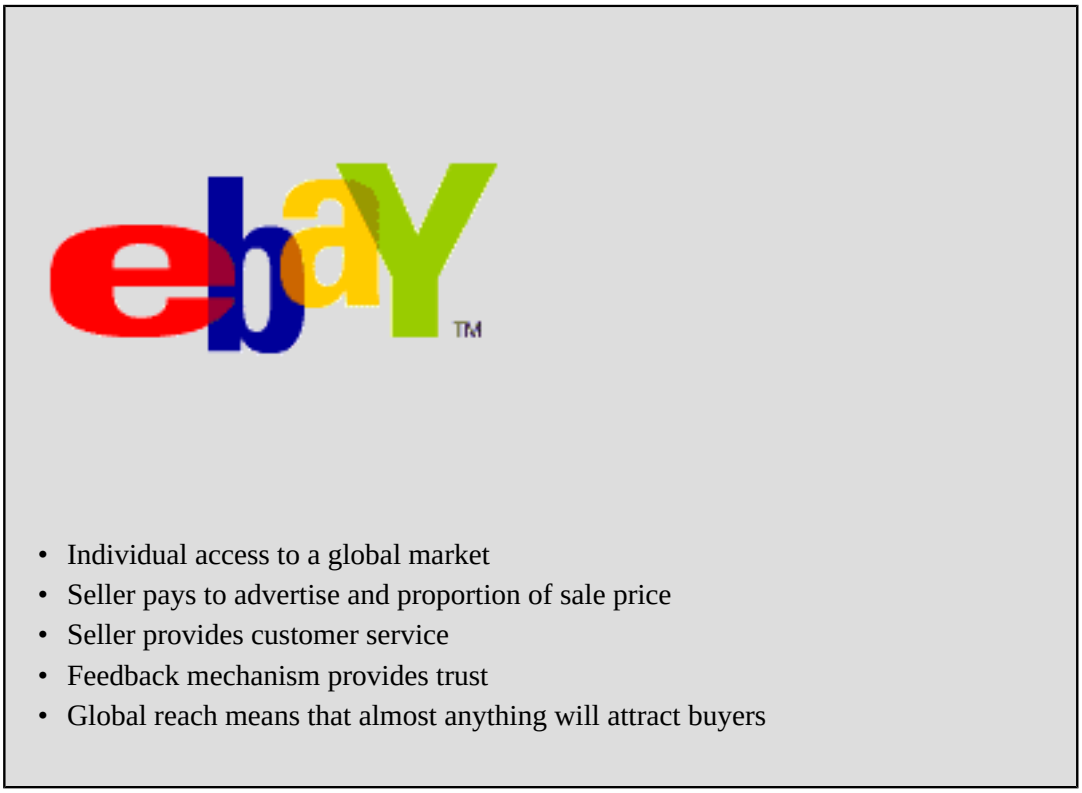
As information exchange to and from their customers becomes more vital to the design and production process, manufacturers are taking advantage of this contact to remove the intermediaries such as traditional retailers and other middlemen, and are able to deal with their consumers directly. This *disintermediation* process gives them a significant cost advantage over more traditional models involving wholesale and retail sectors.

As this begins to happen, the intemediaries must evolve to offer some “added value” over the manufacturer, in order to keep competing in the virtual marketplace. One common strategy here involves the “one-stop” store offering a large range of goods from many manufacturers, adding value through convenience (e.g. dabs.com, tesco.com).

Another, the service-based model, adds information, consumer reviews, forums and improved customer service keep the interest of the customer (e.g. amazon.com, expansys.co.uk).

And most interestingly, there is the trust-based model, where the manufacturers/sellers are able to sell through a trusted intermediary (often known as a *cybermediary*), giving the customer confidence in an otherwise unknown brand (e.g. Amazon Marketplace, abebooks.co.uk).

Ebay - the Ultimate Cybermediary?



One of the most important successes in Internet business in recent years is eBay, the online auction site. The idea behind eBay is that it acts as a global auction house, allowing you to sell your goods to a very wide audience for relatively little cost.

The eBay business model gives the company a measure of immunity from the problems that many online businesses face. eBay acts as a *cybermediary*, which provides a medium through which others transact, isolating the company from problems such as providing customer service for individual transactions, and dealing with poor payers. In effect, they act merely as an advertiser and mediator for each transaction.

Perhaps the most revolutionary part of eBay's business model is the highly transparent system of reputation generated by buyers and sellers giving feedback on transactions. In a global marketplace, it's difficult to know who is trustworthy, so the feedback system gives a measure of virtual trust. Although the system isn't perfect, it is difficult enough to subvert, and policed well enough by eBay itself, that most transactions are safe and reliable.

In some ways, the feedback system emulates the reputation of a traditional business which, by word of mouth in a geographical locality, can generate trust within a neighbourhood.

Whilst eBay began aiming its auctions at low-value items, its biggest market is now in more substantial transactions, notably motor cars. It has also encouraged growth in business-

to-consumer markets, inviting large companies to offer goods and services through its marketplace.

For a look at bidder behaviour on eBay, see [67].

Evolution of E-commerce

A typical “traditional” retail business will go through a number of stages in the process of entering the e-commerce market:

Initial resistance

- many companies resisted the coming of e-commerce for as long as possible
- lack of secure transaction methods deterred early adoption

Reluctant first steps

- Static web information (e.g. catalogues or advertising brochures)
- Email enquiries
- Email ordering (note security risks)

The first step was usually to place catalogues or other information on the web, usually converted from paper-based materials. This was seen as a form of advertising, but failed as it was too static.

The next step was to allow ordering by email--primitive but useful, though not without its problems. Sending private information (such as credit card details) via email is always risky, as it is an unsecured medium.

Buying and selling online

- providing an online ordering system
- processing orders automatically
- allowing customers to check orders and accounts online

Enhancing the online shopping experience

- providing dynamic information about stock availability
- allowing customers to publicly review products and services
- using browsing and purchasing statistics to make recommendations

This phase is often referred to as the “Web 2.0” phase, where the consumer is less a passive buyer and more an active player in a shopping game - providing feedback and reviews that are used to create a rich shopping environment.

This has been most successful with large online stores such as Amazon, where the volume of customers for each product means that there is a greater likelihood of someone writing a review. Of course, there's also the kudos of providing the best reviews, which almost becomes a gift culture (the section called “Something for Nothing? Gift Economies”./>

Buying and selling information-based products

- fully digital -- the buyer downloads the item without the need for any physical delivery
- the buyer purchases the right to download and use the information -- buying a license rather than a product.
- payment is usually also fully digital
- no physical product means no delivery, no delay, no production overheads, etc.
- examples: software, music, eBooks, etc.

Virtual Products and New Economies

- Virtual “products” mean low per-item costs
- Examples include music, software, services, access to information, virtual entertainment, etc.
- Online gambling has proved particularly successful
- Copyright problems, led to DRM technologies to restrict use

iTunes and the Virtual Product

- DRM restrictions - a compromise
- Major media companies signed up
- Captive marketplace of iPod buyers
- Bundled with *de facto* standard media player software

There were several false-starts by companies trying to sell digital music online. Most famously, Napster fell foul of the Recording Industry Association of America, and was closed down overnight, even though its business model was sound.

It needed a company with some weight and authority to take the lead and overcome the paranoia of the music copyright holders before virtual music really took off. Apple were able to bundle a new application with their Quicktime software which would manage music files and ensure that copyright was not breached; this application (a form of *Digital Rights Management* software) was enough to make the venture successful.

Apple's iTunes service allows you to download tunes at a fixed price, and play them an unlimited number of times. You are restricted, however, in how many times you can copy that tune from device to device, which to some extent enforces copyright. It was this compromise that the big media companies needed in order to feel comfortable with Apple distributing their songs.

There are other forms of DRM technology, which will be discussed in Chapter 4, *Legal Issues 1*.

Web Advertising

- Highly profitable sector for e-commerce
- Popular websites can command high prices for advertising space
- Google's “cost-per-click” model
- Viral marketing

Internet technologies have enabled new methods of advertising to dominate the Web. Google's *AdSense*, for example, uses context from the page hosting the ad, coupled with information from previously clicked ads, to place relevant advertising to the page's tartget audience. Their revenue model is also innovative, only generating a charge when a user clicks-through to the advertiser, ensuring that charges are based on how attractive and relevant the advert is, rather than how popular the page might be.

Technologies such as social networks and media sites can also be employed in more subtle forms of advertising. Viral campaigns ([61]) encourage people to pass adverts or links to advertising media around, forming a “buzz” around the object, and generating greater exposure to the advert. A recent example of this is *Cadbury's* “Gorilla” campaign, which used various social networks to spread the ad and generate discussion.

Viral marketing is often difficult for companies to control - once a viral ad is “out there”, then it may be replicated, modified or subverted into something less favourable to the company. In extreme cases, *culture jamming* may occur, where media advertising a brand or product is deliberately modified to work against the original intent of the advert.

Viral techniques can also be coupled with guerilla strategies, where the subject of the advertising is not disclosed until there is sufficient marketing “buzz”. Guerilla techniques are often risky for the company involved, as they may just as easily create a backlash against the company . Subverted media artefacts can be extremely persistent on the internet!

Something for Nothing? Gift Economies

- Contribution to abundant free resources on the net
- Gifts of work, information, expertise or programming
- Given to the “community” in exchange for use of the resources

One of the most unusual aspects of the web is the amount of free information that exists on it. Often this material is valuable in terms of its reliability and expertise level, and often is it freely given to the Internet community. This has led theorists to analyse what has become known as *Gift Economies* on the Internet.

The most well known example of this is Wikipedia [http://www.wikipedia.org/], a freely available, user-contributed encyclopedia. Here, the information contained in the encylcopedia is created by interested individuals, then mediated by any number of moderators, all of whom have equal access to change any part of the entry. This seems like a recipe for anarchy, but most often produces a considered consensus of knowledge which has the reliability of the collective moderators, many of whom may be experts in the field under discussion.

Another example of a gift economy is more technical - the GNU/Linux operating system. A replacement for Microsoft Windows, this software is again written by its users, and is provided free to anyone who wishes to install it. With GNU/Linux, the motivation for contributing is often the prestige of taking part, and having your name and your programming code embedded in the final product. Linux is on the edge of the commercial and FLOSS (Free/Libre Open Source Software) ways of creating software - some commercial companies offer support for Linux, or repackage it with 'value-added' features for sale, though the core software must always remain free and open. A good example of FLOSS development is the Debian flavour of GNU/Linux [`http://www.debian.org/`].

There have been many studies of the organisation and motivation of these gift economies, see for example, [5]. A key commentator is Eric Raymond, whose paper entitled *The Cathedral and the Bazaar* (Raymond, 1998) has sparked much discussion.

Problems arising from the Virtual Marketplace

Taxation across Borders

- Internet has no real concept of nations and borders
- Difficult to track international transactions
- Where is the point of taxation?

The problem of jurisdiction on the Internet crops up in many discussions - it does not respect national boundaries, and has little sense of “place” in many ways. Taxation is a “place-based” entity; you are taxed based on where you live, work and shop. In the early days of the web, this was seen as a considerable paradox.

However, it does seems that many of the fears expressed (mainly by governments facing lost revenues) were unfounded. The processes involved in e-commerce mostly have to take place in real locations with real companies and real money changing hands. On the whole, governments have quickly adapted their existing taxation policies to encompass the new markets.

One problem that does recur is the possibility of locating businesses in low-taxation countries, with obvious benefits. When virtual products, such as digital music, software or even online casinos are involved, the location of the company is immaterial, and can be chosen to provide the best financial advantage.

This highlights the question of “at which location should tax be applied?” Goods despatched from Jersey, for example, will have no sales tax added, but may be subject to import duty; the point of taxation moves from the company to the point of entry to the UK, which is much harder to manage, and the tax less likely to be applied. Where virtual products are sold, the point of taxation is even harder to determine. Some have argued for border controls on the ISP's points of entry into the UK, but as most commercial data is encrypted, this would not help.

Further reading

For further reading, see the First Monday section on Economics [http://www.firstmonday.org/subjects/economics.html], and especially the recent special issue no.3 [http://www.firstmonday.org/issues/special10_12], on “Internet Banking, E-Money and Internet Gift Economies”

Two topics relating to e-commerce are discussed in later lectures. The problems of copyright, patents and intellectual property are discussed in Chapter 4, *Legal Issues 1*. Aspects of secure data transfer, protection of private information, etc., are discussed in Chapter 5, *Legal Issues 2*.

Discussion

- Do you use review sites or shops with reviews? How important are they in your decision to buy?
- Have you written reviews? What were your reasons for doing so?
- Do you feel that the iTunes DRM limitiations are a reasonable compromise?
- Is the buying of music as a “product” coming to an end, with the rise of streaming services such as Spotify?

Chapter 3. The Information Society

There is little doubt now that the advent of the Internet has caused significant change in our society. Some theorists feel that we are undergoing a culture-shift as pronounced as the Industrial Revolution, with similar consequences for the way we live and work.

Social theory and the Internet

- Is the internet a catalyst for social or cultural revolution?
- Will cyberspace change the way society works?
- Will it affect the way we interact within society?

Before we look at some of the individual areas where cyberspace has begun to change our society, we will need to examine how the social theorists have analysed the impact of computers and computer-mediated communication technologies. Our society is constantly being observed and deconstructed by these theorists, and many have concluded that we are undergoing a major cultural revolution from a primarily industrial society towards a more information-centred one.

There is still much debate as to the magnitude of this revolution. Some see it as an evolutionary stage in our progressing society, just the next step in a long chain of advances. Some, however, consider our move to the information society as a radically new form of existence, which is quite unlike any other form of society. Cyberspace, the enabling technology for the information society, has the power to transform it in the same way that steam power and mechanisation transformed society in the Industrial revolution (Graham 1999).

Post-industrial Societies

Daniel Bell (1919-)

- Daniel Bell's post-industrial or information society
  - move from manufacturing to service-oriented industries
  - predominance of science and technology industries
  - power moves towards technocratic elites

The first comprehensive critique of the changes brought about by the computerisation of society was proposed by Daniel Bell, in his book, *The Coming of Post-Industrial Society* (1973). Here, he suggested that we are moving into a new phase of society, where the primary industries are service-based, the most marked growth being in information analysis and processing. At a time when the computer was still restricted to large company or government installations, he foresaw that information transfer would be central to this new order, and hence predicted the need for the Internet.

The reasoning behind this came from the decline in traditional manufacturing and raw materials processing; mining, steelmaking and motor manufacturing were all giving way to banking, retailing and fast-food.

Bell sees this as a symptom of a change towards a more scientifically led society, that places knowledge as the instrument of power. Industries that advance this knowledge or redistribute it are held in high regard. Perhaps the most obvious example of this in today's society is Google [http://www.google.com/], which has now become one of the most well-known brands across the globe.

Though Bell had little evidence for the trends he was predicting at the time, subsequent events have to some extent confirmed his analysis, and other theories which have built upon his work have shown it to be useful.

Network Societies and Flows

Manuel Castells (1942-)

- Manuel Castells' Network Society
  - informational mode of development
  - flows of information/power and network enterprises
  - timeless (accelerated) time and distanceless space
  - breakdown of collective identities (nations, ethnic groups) - the cultural turn

Taking Bell's ideas further, the sociologist Manuel Castells has detailed a view of the information society (which he calls the “Network Society”) from statistics and trends gathered from around the world. His trilogy, *The Information Age*, outlines several themes.

Most importantly, Castells agrees with other theorists that the centre of the new society is the industry of gathering, processing and interpreting information. He suggest that this *informational mode of development*, the advancement of society through knowledge and information, is next evolutionary step for society.

He also looks at how power is invested in information, and how the flow of information creates many of the poser structures on which today's society is based.

The informational society has other implications, such as the breakdown of our conventional notions of time and space, and the gradual disappearance of collective identity,as we all become part of the global society.

Work in the Information Society

- Information industries mean greater education requirements
- Technology used to augment the traditional workplace
- Knowledge workers need no physical workplace

The economies of the Western world seem to be moving from industry to information. Rather than buying and selling products, the currency is information, in the form of customer data (emails, addresses, buying preferences), intellectual and creative property (patents, ideas, digital images, etc.) and other data. The skills required for the workforce of this economy are knowledge-based, in such areas as education, training, computer literacy, programming skills, legal skills and so on.

These skills are not tied to physical location and their productivity can be transmitted across the world, so that companies can now operate easily in a global market, without reference to their local conditions.

Examples of this knowledge-based globalisation are abundant. The current trend for relocating call-centres into India is only the latest part of the industry to make a move towards a global workforce; the legal industry has for some years outsourced the writing of many legal documents to places where there are well-educated employees with fewer expectations on employment conditions or pay, such as India.

(Castells 1996, ch.2), (Castells 2001, ch.3)

Remote working

- teleworking used to create more flexible working patterns
- teleworking used to provide more employment opportunities
- Reduces travel needs, and hence reduces pollution and congestion
- Reduces social aspects of work - interaction with colleagues, etc.?
- Working communities - real and virtual

The mass availability of computing and communication equipment has often led to comments about the changing nature of work, and in particular the move from the traditional workplace into the home. Though there has been a steady trend, the extent of home-working and telecommuting has not been as great as was expected. There may be many reasons for this, such as the reluctance to give up the social aspects of work; the benefits associated with using a different environment for work to that for other activities, and the difficulties associated with the technologies themselves.

In the nineties, teleworking was promoted as a viable alternative to going in to the office, despite the inadequacy of the technologies. During that time, it never really took off, because it never allowed the teleworker to feel part of the community of the office, and was always unreliable and difficult to set up and use.

However, now that the technology has caught up, and we have usable videoconferencing and text-based discussion, it's a more popular tool. Teleworking as the primary way of working has not become as popular as many predicted, but teleworking as a way of creating flexibility

in your work patterns certainly has. Many teleworkers do so only for a few days per week, physically going in to the office for the rest of their time.

Hotdesking has become a popular idea here, where an office has generic desk areas where anyone can work rather than specific allocated areas for each employee. Logging in to the computer often provides a customisable desktop which gives the worker a feeling of “place” since they cannot personalise the office space in other ways.

Teleworking often allows those who could not normally work easily in an office environment an opportunity to contribute and hold down a job; single parents, the disabled and those living in physically remote areas can all benefit.

As with all technologies, the aim should be to enhance communication and develop community. There is a fine balance between allowing employees the flexibility of teleworking, and ending up with a socially unsatisfying virtual community where everyone hides behind their email.

For further reading, see Dyson (1997, ch.3), Castells (2001, pp.231-235), and Mitchell (1995).

Work, Surveillance and Privacy

- Electronic communication is easy to monitor and record
- Surveillance is now part of our culture

One of the implications of the widespread use of computer-mediated communication technologies is the ease by which this use can be monitored and filtered (Lessig 1999, p.149).

The “Surveillance Society” is now an accepted norm; we walk past hundreds of CCTV cameras each week. It's an easy matter to implement a very high level of surveillance with email and web traffic. In fact, it's already specified (and even required) by our legislature (see the RIP Act in the section called “Problems with Strong Cryptography”)

Equality and Human Rights

- Internet as an equalising factor
- access to information a human right?
- Internet as a tool for dissidents & propaganda

The Internet is often cited as a divisive factor in society; that those having access are increasingly advantaged over those having no access. Is this the case? Should we have a right to access the digital domain? Why is access important?

As our government places more of its information and advice online, it will become essential that all have access to this. Initiatives have been launched in the past to address the imbalance between those who have access and those who do not (for example, the Improvement and Development Agency's e-Government paper [http://www.idea.gov.uk/idk/core/page.do?pageId=1074872]). Access is particularly problematic for ethnic minorities (language issues) and the disabled (accessibility problems).

Independent evaluations of the accessibility of local and national government web sites show serious failures. In one study, the comparison against the WAI's Web Content Accessibility Guidelines showed:

- 60% of the sites evaluated did not reach minimum accessibility levels.
- 35% were either just below minimum accessibility levels or achieved minimal accessibility but still had serious problems.
- Only 5% achieved the UK Government’s guideline of WAI Priority 1 Accessibility Level whilst displaying signs of working towards Priority Level 2.

The Digital Divide

- Information-rich and information-poor
- Western companies swamping growing third-world markets
- Expensive internet access in third-world countries is often only reliable means of communication

Access to information and communication technologies becomes very important when we move into an information society. Those that have access are able to compete and sell their knowledge services on a global market. Those who have no access are disadvantaged against the global players. This separation is often termed the *digital divide*.

This disparity does not confine itself to the traditional division between the “first world” and the “third world”, indeed it can be seen in almost any society, including the UK. Here, the government has created several initiatives in the recent past, to encourage disadvantaged communities to connect to online services, through the use of Internet connections in schools and libraries, and through subsidising computers and braodband connections to poorer communities.

However, the globalisation of markets is enabling more powerful companies from the information-richer nations to flood the burgeoning knowledge-based markets in poorer countries with cheap (often subsidised) knowledge goods such as software.

There are some areas that are fighting back; the use of free open-source software and recycled computers can enable the financially or socially disadvantaged to compete on a more level playing field in the knowledge market, and projects such as One Laptop Per Child [http://laptop.media.mit.edu/faq.html] are enabling this to happen.

For recent studies, see Cendrós Guasch & Ugas (2007), Fuchs & Horak (2008)

Open Societies, Open Governments

- Access to processes of government
- Freedom of Information Act (2000)
- Transparency only for those who can understand?

Transparency in government is a common theme, for journalists and politicians, and can significantly reduce corruption and malpractice - the threat of all discussions and communications being accessible (to law enforcers, to ombudsmen and even to the public) can certainly concentrate the minds of those in power. There is, though, always the danger that if too transparent and open, alternative routes of communication will be found.

There are also difficulties associated with the complexity of politics. To those who do not understand how the machinery of government works, the information available to them can see both daunting and extremely opaque.

Internet Subversion

- Enabling the publishing of subversive texts under oppressive governments
- Allowing dissidents and oppressed minorities the freedom to communicate
- Publishing freedom - a double-edged sword?

The Internet has often been used to promote personal opinion across a global audience, and this can be used to promote human rights and freedom, by disseminating information about oppressive governments and rights abuses.

Organisations such as the Digital Freedom Network [http://www.dfn.org/] and Privaterra [http://www.privaterra.org/] [website currently undergoing maintenance] provide information promoting human rights and highlighting abuses. Sites such as Index on Censorship Online [http://www.indexonline.org/] and Amnesty International [http://www.amnesty.org/] show the work of non-governmental organisations (NGOs) working in this area, in a way that is accessible to many who are subjects of abuse.

Often, though, more informal means of disseminating information are used by those caught in oppression or abuse. During the invasion of Iraq, the view from inside the country written by the “Iraqi blogger” was carried by much of the world's media; the Zapatistas of southern Mexico have used the freedom of the web to highlight their cause, and the anonymity of email to organise their rebellion (Froehling 1999).

More recently, the darker side of the freedom to publish in cyberspace has been highlighted, in the case of animal rights activists in the United States publishing the names and addresses of those involved in UK research labs, together with incitements to harm or injure.

Freedom of speech is hotly debated in cyberspace, and is an issue that will always prove contentious as governments try to find ways to moderate the web without curbing this freedom.

New Interactive Media

- Web publishing and citizen journalists
  - Blogs (article and photo journalism)
  - Podcasts (audio and video)
  - Video-on-demand (e.g. Google video)
- Media awareness and public participation

Recent developments such as blogs and wikis have made a real impact on political life. To some, political blogs are just a quick way of spreading rumour; to others they get much needed information about the political process out to the masses.

Public participation in the political process may also be enhanced, such as with the online availability of petitions (http://petitions.pm.gov.uk/) and other less official forums (e.g. GoPetition [http://www.gopetition.co.uk/petitions/change-the-london-2012-logo.html] collected 50,000 signatures to change the London 2012 logo).

And the availability of news media, often “as it happens”, fuels our demands to have greater and faster access. News aggregators, such as newsnow.co.uk [http://www.newsnow.co.uk] and Google News [http://news.google.co.uk/] let us to assimilate more news stories from differing perspectives, allowing more effective *knowledge assembly* of a rounded, balanced viewpoint.

As mobile technology advances, delivery of media becomes more pervasive as the condensing of news and views into podcasts and video downloads allows them to be downloaded wherever you might be.

Singularity Theory and Inhumanism

Vernor Vinge (1944-)

- Internet anarchy?
- Internet as a global consciousness?
- Convergence to an ultimate point of evolution?
- Escape from physical reality?

What is the ultimate destination of these trends in society? There is no doubt that technological advancement is accelerating, and that the information society is having an effect on our perceptions of space and time, as well as the ways we interact socially and professionally.

Some predict that the Internet will create a state of global anarchy (Graham 1999), though it's not always clear whether they perceive this to be a good or a bad outcome. Others see the technological acceleration as culminating in a *technological singularity*, where Artificial Intelligence creates a conscious, non-human being, and beyond which we cannot predict or imagine our future (Vinge 1993).

In particular, Ray Kurzweil (an inventor of digital music and speech synthesizers) has extended Moore's Law, which observes that computing power doubles roughly every two years, to other technologies and linked it with his own “Law of Accelerating Returns” (2000). This predicts that the rate of technological change will continue increasing, producing such massive and rapid change that it produces a significant change in the evolution of humankind. His estimate of this event is around the year 2045.

In a similar vein, Jean Francois Lyotard has suggested that the ultimate goal of technological advances is to free our minds from the constraints of the physical body, at which point the human consciousness is able to evolve freely, and can escape the ultimate destruction of the earth (1991).

As you may imagine, these themes are well represented in Science Fiction as well as Futures studies, with prominent authors such as William Gibson (esp. *Neuromancer* 1984, and *Mona*

Lisa Overdrive 1988), Neal Stephenson and Vernor Vinge all predicting a future with at least partial escape from the body.

Discussion

- Is the internet as significant as, say, the Industrial Revolution, or Gutenberg's invention of movable type?
- Should access to the internet be a high priority in developing nations?
- Will the accelerating rate of progress initiate some major shift in evolution?

Chapter 4. Legal Issues 1

Intellectual Property

- What is intellectual property?
  - Patents, copyright and trade marks
- What rights do we have to own intellectual property?

The Internet has allowed ideas and information to be freely and easily communicated on an unprecedented level. The ethos of this sharing was entirely cooperative, being primarily to disseminate results among a scientific community, and did not allow for the ownership of information. As the Internet has matured, it has had to come to terms with such restrictions as copyright, patents and libel laws, though these laws and restrictions have had difficulty in keeping up with the technology.

Patents and the Digital World

- patents for processes and products, but not ideas?
  - some *very* silly patents!
  - can software be patented?
- differentiate patents from copyright ownership

Patent law is undergoing changes in an attempt to adapt it to the new digital world. In the process, many poor decisions have been made and many bad patents have been granted.

In Europe (and in the UK), there is a fairly clear definition of what is patentable:

Patentable inventions

1. European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

2. The following in particular shall not be regarded as inventions within the meaning of paragraph 1:

   a. discoveries, scientific theories and mathematical methods;

   b. aesthetic creations;

   c. schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers;

d. presentations of information.

3. Paragraph 2 shall exclude the patentability of the subject-matter or activities referred to therein only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such.

—EUROPEAN PATENT CONVENTION: PART II - SUBSTANTIVE PATENT LAW, Chapter I, Article 52 [http://www.epo.org/patents/law/legal-texts/html/epc/2000/e/ar52.html]

Whilst this is (fairly) clear, there have been exceptions made to rule 2(c) on the basis of software being part of a manufacturing process. The large software corporations continue to lobby for software patents.

In the US, there is a more complicated situation, with patents being granted or denied on a variety of criteria. For an overview of the current situation in the US, read the Patent Law Primer [http://www.jurisdiction.com/patprim.htm]. For the latest patent and policy news (again US biased), there's a website [http://www.oreillynet.com/policy/] run by the O'Reilly publishing group, who have interests in the Open Source ethos.

Should we allow the patenting of information and ideas? What about computer programs, or even programming algorithms and techniques? See Ludlow (1996) and Grosche (2006)for more details.

Some benchmark cases

- the Unisys GIF/LZW algorithm
- US case of amazon.com v. Barnes & Noble regarding 1-click ordering
- BT claiming patent for hypertext links (the “Hidden Page” patent)
- Microsoft applying to patent XML? Or at least their document definitions.

Unisys [http://www.unisys.com/about__unisys/lzw] GIF/LZW algorithm.

- Compression algorithm patent that was violated in many web-graphics, and by most image-editing software
- .png format developed directly in response by the open source community
- Patent has now expired in most countries.
- For a historical overview of the case, see the League for Programming Freedom [http://lpf.ai.mit.edu/index.html]'s page on the Unisys/CompuServe GIF Controversy [http://lpf.ai.mit.edu/Patents/Gif/Gif.html].

amazon.com v. Barnes & Noble.

- Amazon claims patent on 1-click ordering system (1999)
- Injunction granted preventing wide use of 1-click technique, but later repealed
- Dispute settled out of court (2002)
- Amazon successfully defends patent in court against IPXL Holdings (2004)
- Enthusiast shows prior art, forcing Amazon to narrow patent (2007)

BT's Hidden Page Patent.

- Proof of “prior art” needed to undermine BT's case
- See for example, Michelle Delio's (2002) report (Move Over, BT: He Invented Links [http://www.wired.com/news/culture/0,1284,50398,00.html]) in Wired News.
- Should such a fundamental and simple technology be patentable

Perhaps the problem here is that it is easy to “dress up” a very simple idea or process as a highly technical programming technique, which can often get past the Patent Office scrutineers.

Domain Name Piracy or “Cybersquatting”

- Who owns which domain name?
- Should anyone have the right to own a particular name?
- Should there be a free market in domain names?
- Application of trademark law - "passing off"

In recent years, the system of allocation of names on the Internet has given rise to a new form of profiteering. Before many of the larger corporations became aware of the need for a corporate website, opportunists would register their name as an Internet domain name, then wait for the company to stir, realise that it needed the name, and then offer the name for sale for a large sum. Many of these opportunists did take significant amounts of money, though the practice was always considered dubious. Several court cases were filed against them, but the results were variable, almost always being settled behind closed doors, well before a judgement was reached.

However, in one case[i], a company that had registered the names of a number of UK businesses as domain names was forced to relinquish those names, as their use could be regarded as “passing-off”, i.e. the use of a trademarked name to imply that a website has a connection to the trademark's owner. This is a direct violation of the Trade Marks Act 1994, which covers use of any registered trade mark in any context. In this case, the company had speculatively registered names such as marksandspencer.com, sainsburys.com and britishtelecom.com,

[i]Marks and Spencer plc and others v. One in a Million Ltd., Court of Appeal, 23 July 1998.

and initially offered the names for sale to the companies concerned, but with the implication that they would be sold to the highest bidder if each company refused to buy outright. It was this intention that forced the judgement against the speculators.

Today, most cases are settled out of court, and usually within the mechanisms for dispute resolution provided by the registrar (in the UK, this is Nominet.UK [http://www.nominet.org.uk], who maintain an index of UK case law [http://www.nominet.org.uk/disputes/caselaw/index/] relating to this).

The practice of registering domain names which are underused but still attract some traffic is called *Domain Parking*. This is common within Internet Service Providers, who register potentially useful domains and offer them for sale, but in the meantime add revenue-generating material to the site, to offset the cost of registration.

It's also common now to find registrations of domains created through common typographical errors on well-known domains, which is sometimes known as *Typosquatting* (Edelman 2008). For example, a typosquatter may register the '`bcc.co.uk`' domain name, and place advertising or other revenue generating material on that domain, in the hope of users typing '`bcc`' instead of '`bbc`' in their browser's address bar.

Copyright Law

- How does copyright work?
- How does it apply to online content?
- How has copyright law evolved in the digital world?

Copyright on the Web

- Who owns the information on your web page?
- Hyperlinking encourages the use of other people's material on your pages
- How can you protect your information and software?

Copyright law exists primarily to protect your investment of research, analysis or creativity as a producer of media and ideas. Anything that you yourself create can be claimed as copyright. So when you create a web page, all that you write as original material is yours, and can't be used by others without your permission.

However, creating web resources often involves reusing other people's original works, and there the boundaries become blurred. How much rewriting must you do to claim it as your own work? What if you incorporate graphics, HTML code or scripts from other's sites?

The hyperlink positively encourages the author to link to other people's material. HTML also makes it possible to seamlessly incorporate outside material into web pages. Is this appropriate?

And of course, the web is an open, accessible medium where it's easy to copy and paste material without thinking about copyright - so how do authors protect their creations?

Hyperlinking and Reuse of Information

- Simple links to other's websites are generally acceptable
- Deep linking can be problematic
  - Links to information contained in another's website which bypass their homepage and thus possibly the identity of the copyright owner.
- Framing
  - Using information from other website by placing it within a frame displaying your identity
- Test case: Shetland Times[ii]
- General rule: acknowledge your sources and don't pretend that material is your own.

In the test case mentioned here, a website owner was found to be reusing the news reports of another site, presenting them as articles that he had written himself. This is considered by the UK courts as 'passing off', as presenting information not owned by you as your own work.

Other legislation and cases that apply here include the Copyright and Rights in Databases Regulations (1997), which safeguards the effort invested in data gathering and encoding for large-scale databases, particularly those made available to the public. It prohibits the reuse of significant amounts of information contained in the database by a third party without permission or acknowledgement. This was recently tested in the case of the British Horseracing Board vs. William Hill.

The Public Domain and Finite Copyright

> “Art is making something out of nothing and selling it.”
>
> —Frank Zappa

Copyright is, at present, of finite duration. If you claim copyright on a work, then you have a number of years to exploit that work in whatever way you see fit.

The duration varies according to the type of media and the role of the copyright holder, so for a performer releasing a hit record, the copyright expires 50 years after the year of the performance. But for an author writing a book, the copyright lasts 70 years after the author dies. For a full table and necessary explanations and clarifications, see Cornish (2007).

Whilst in the short and medium term, copyright is seen to be a necessary incentive to creativity, long-term or even perpetual copyright can threaten the survival of culturally significant works which are no longer financially viable. It's a fine balance between making money from works and preserving them for the longer term, as recognised by the British Library (2006). In the digital world, copyright enforcement technologies will significantly complicate this balance.

The Concept of the Commons

- common culture, heritage and information
- the copyright-free resources we all share access to
- new works deliberately placed into the commons

Traditionally, the concept of a “commons” relates to land use, and we often think of common land as having shared ownership. In fact, land, facilities or objects deemed to be part of the commons are owned by everyone and no-one.

Think of the street outside your house. Most likely, it is maintained by the local council, who take money from you to do so. However, they don't own the land in the normal sense, though they have responsibilities towards it. Everyone has equal access to it, and can use it almost as if it were their own.

In intellectual property terms, the equivalent is the creative work that has fallen (or been placed) into the public domain. No-one can claim ownership of it, and hence cannot charge royalties for its use. Everyone should have equal access and equal right to use the work.

Eldred vs. Ashcroft

Eric Eldred (1943-)

- What should be placed into the commons?
- How long should copyright last?

In the early nineties, Eric Eldred was a hobbyist who scanned works of literature and placed them onto his website, so that anyone could access them. He took works which had passed out of copyright, and made them available for free in a new format. However, as he accumulated a larger and larger collection of works, he began to hit a problem. More recent works, which

were nearing their release from copyright, were suddenly put out of reach of this cultural service, through the extension of the copyright term. And this happened repeatedly.

Eldred began to question why this was happening, and why some works never seemed to be released from the restrictions of copyright (Lessig 2004, Ch.13). He argued that this extension, brought about by the 1998 Sonny Bono Copyright Term Extension Act (CTEA), and if perpetuated would lead to indefinite copyright for certain works, and thus was unconstitutional (violating the first amendment).

The US Supreme Court upheld the CTEA, but only after a massive lobbying effort on both sides, by libraries and libertarian groups on one side, and by the music and film industry on the other.

Practical Considerations

- Why has the Internet precipitated these problems?

The Digital Copy

- Traditional media has often had inherent deterrents to copying:
  - cost
  - imperfect copying methods
  - inconvenience
- Digital data often has no such barriers
  - it can be easy to make a perfect copy of information

The limitations of traditional media have meant that passing off a copy as an original has been difficult to achieve and easy to detect if done on a large scale, though generally copies have become acceptable in quality for personal use. This has led to a concept of “fair use”, which permits making personal backups etc., of traditional products. Certain copyrighted material is subject to fair use when quoted, criticised or parodied, though much material (especially new media) is not covered, though most of us have developed our own idea of fair use, as applied to the text, music and video we use.

With digital media, we need to re-examine the fair use idea, and there have been several attempts to formalise it in the courts, with little success. Many copyright holders still consider any copy to be an illegal one, and some refuse to publish works digitally because of this.

These problems are similar to those inherent in protecting the copyright of software, which has never been satisfactorily solved.

Peer to Peer File Sharing

- Distributed, often decentralised, many publishers
  - each participant becomes a distributor on a network
  - equivalent to “home taping” but on a global scale
- P2P also widely used to distribute legal software and media
  - E.g. Channel 4's 4OD and BBC's iPlayer services
  - F/LOSS software distribution also uses P2P to alleviate load on servers

Peer-to-peer filesharing has often been the scapegoat that has taken the blame of all the troubles of the media industry, as they have tried to come to terms with the changes that digital media are necessitating.

The key characteristic of a true peer-to-peer system is the lack of a central server or directory for clients to attach to. Instead, data is downloaded from nearby peers who are hosting the data, with each 'client' acting as a peer within this network, making available material to be downloaded themselves. So, rather than all clients downloading a file from a single location, the file could come from many possible sources, usually consisting of thosw who have downloaded the file previously. As a file download gains in popularity, so the number of peers offering the file increases. The advantage is that there is no longer a need for a high-bandwidth server to make popular files available.

The decentralised nature has other effects. Firstly, it means that it is harder to find files, hence the rise of directory sites such as Ananova and The Pirate Bay. Secondly, it makes it harder to shut down the service, as there is no single entity to prosecute. It is still possible to detect individual peers that are offering illegal content, but these must be pursued individually.

A Current Case: Music Publishing

- Problem: Music piracy/sharing
  - MP3 format - high quality, fast download
  - More convenient than tapes & CDs
  - Easily distributed
- Peer to peer sharing mechanisms/software
  - decentralised, therefore difficult to sue
  - personal, cooperative and participatory
- Video piracy/sharing is also gaining popularity using DivX & Matroska formats (for example)

In an attempt to curb the illegal distribution of music and video, some companies have introduced copy-protection on CDs and DVDs. The CD protection has been particularly

problematic, as it relies on the user not being able to read the disk in a purely digital form. It works by introducing errors which are normally corrected by most audio CD players, but which cause the digital copy to break or skip in computer CD players, which don't have error correction mechanisms.

Of course, the protection was quickly broken by hackers reverse-engineering the error correction mechanism, by using more sophisticated CD players, or in one case, by obliterating a section of the disk using a marker pen... within hours of a CD being released, there are usually digital copies on the net.

In fact, there is a subculture on the Internet now which competes to produce the earliest digital copies of the latest films and music, generated by taking hidden video cameras into premiere showings, leaking material from the record companies themselves, and so on.

Companies such as Microsoft have a difficult position; they want to tap into the popularity of digital media and encourage its use, but in such a way that the powerful media companies do not object to.

Some Suggested Solutions

- Password protection
- Digital signatures
- Encrypted downloads
- Digital Rights Management
- Micropayments
- Media tax
- Streamed services

Password protection. A password is sent independently of the download, which is then needed to use the media or software. Ineffective, since passwords can easily be exchanged with the copied file.

Digital signatures. ensuring authenticity of both supplier and consumer, can be used to prevent unauthorised playing or copying;

Encrypted downloads. attempts to copy-protect the media, preventing use without authorisation;

Digital Rights Management. encompasses all these ideas, usually integrated into a digital media player;

Micropayments. A very small charge (perhaps less than 1p) is made for each view or play, but accumulates to significant amounts if sufficiently popular. The key to this is the ease of making the payment.

Media tax. In some countries, a more rudimentary solution has been tried, which tries to add a surcharge on blank media used for copying, the revenue from which is used to compensate copyright holders. In most cases, this has been quickly abandoned, not least because the compensation mechanism is usually too complex to work well. In addition, there is a sense that this approach legitimatises the copying process - if the downloader is paying the copy-tax, then the act of downloading will seem “less illegal” in some way. Many European countries still use this method for “fair-use” copies for personal use only.

Streamed services. Music is streamed directly to the user's device in real time, so no files are saved and (in theory) the stream cannot be captured or replayed without contacting the server. Services may be funded by subscription, a topslice of an ISP charge, or through advertising. For example, spotify.com [http://www.spotify.com/] uses either subscription or advertising-funded models.

Code, Copyright and Law

- restricting authorised use by means of software
- what happens if software restricts beyond “fair use”?
- If successful, this code effectively becomes the law (Lessig 1999)

Some commentators are concerned about the implementations of DRM technology that are available, and in particular regarding the way they limit certain actions on the product which would normally be considered “fair use”. In fact, argues Lawrence Lessig [*Code and Other Laws of Cyberspace* , 1999], the implementations of “fair use” embedded into these products effectively become the law, since they cannot be circumvented without contravening other laws (such as the US Digital Millennium Copyright Act).

Some conclusions

Are we consumers, users or owners of media? Some advocates argue that we should move away from the traditional idea of the consumer of media, since the ability to make perfect copies means that nothing is physically lost when media is given away. They also argue that fair use should mean that if we buy media, we should have the right to back up that media, and to copy it for use on any or all devices we own.

Businesses are keen to re-sell us our previous media purchase in new formats (e.g. vinyl, cassette, CD, mp3, SA-CD, DVD-Audio, etc., etc.).

Is copying damaging the music industry? Of course, the music publishers see each digital copy as taking away revenue from their legitimate business. But according to various studies, this is a shaky conclusion; media sales have remained roughly static (even in a time of general market depression in the US), and when interviewed, those sharing media often use it as a 'try-before-you-buy' idea, and buy as much media as before, but make more informed choices about what they buy.

What does the popularity of media sharing tell us? Perhaps the sharing technologies have shown us that we consider the price of music and video to be too high, or not good enough value. The media companies need to reevaluate the way they create revenue, perhaps switching more to 'value-added' products and more 'collectible' packaging, which would make us feel as though we have bought something valuable to us.

Discussion

- Should software be patentable?
- Should copyright be forever? Does the commons provide a safer future for media that is important to us and our culture?
- Which digital media solution will win?

Chapter 5. Legal Issues 2

Privacy and Personal Data

- Why do we need security?
- What are the basic tools for security?
- How does the law deal with privacy & security?

Introductory reading

Bruce Sterling's short story *Maneki Neko* (from *A Good Old-Fashioned Future*, 1998) is about a world where there is little privacy for anyone, which has both good and bad consequences. There's also a vivid picture of a world of total surveillance in William Gibson's (1988) novel *Mona Lisa Overdrive*.

I'd also recommend that you dip into *Database Nation* (Garfinkel 2000), which exposes the types of fraud and accidental data release that are perpetrated by individuals, businesses and governments.

The need for security

We don't send a letter without sealing the envelope, so why do we send email without securing its contents?

The Internet could be described as an information channel, where data of every kind flows. Some of this data will be valuable or sensitive in some ways, and hence needs to be protected as it flows through the Internet's computers. So for example, it would be foolish of us to send credit card information unprotected over the Internet, or to be able to view our medical records over an unprotected link.

There are many ways to protect this data, mostly involving the use of cryptography, in one form or another, though the most important tools are an understanding of the vulnerabilities and the application of common sense. Remember that plain email and web traffic is readable at any point on its journey; all that is required is a *packet sniffer* - software that decodes the protocols on the network (internet, intranet, whatever).

Identity theft is one of the fastest growing crimes in the UK. Personal information, whether retrieved from rubbish bins, overheard on a mobile phone or taken from insecure transactions

from the internet, is proving to be difficult to detect and prevent, largely because people aren't aware how important their personal data is.

Three areas of Internet security

- Physical
  - Protecting access to your computer hardware
- Data
  - Protecting access to your information
- Software
  - Ensuring that local/remote software is trustworthy

Physical security. protecting your computer. Do you allow others to use your computer? Do you allow your computer to memorise passwords to sensitive information?

Data security. protecting the data during storage and transfer. Are you sending information in plain text (e.g. standard email)? Are you using a secure web connection (is SSL enabled)? Are you checking your computer regularly for viruses?

Server & software security. trusting the third party. What is the company's information privacy policy? Are you sure the server belongs to who you think? Is the application you just downloaded sending information about you to its vendor?

Three aspects of data protection

- Privacy
  - Keeping your information private
- Integrity
  - Knowing that the information has not been changed
- Authenticity
  - Knowing who sent the information

Privacy. Ensuring that your data is visible only to those you have permitted. Uses encryption to safeguard data, protecting it from being seen by unauthorised parties.

Integrity. Ensuring that data has not been modified *en route*. Uses encryption to enclose data in a digital envelope, to indicate that the data has not been tampered with.

Authenticity. Ensuring that the sender of data is verifiable. Uses encryption to assure the recipient of the sender's identity through the use of *digital signatures*.

Cryptography

- encoding messages or data using a code or cipher
- provides protection if message is intercepted
- examples include secure web servers using SSL

Prevention is usually better than cure: encoding a message containing sensitive information reduces the chance that if that message is intercepted, someone will be able to view the information it contains.

Example: Secure Web Servers. As an example, a basic level of security and privacy is provided by most of the commonly used browser through the use of secure servers, using a protocol called SSL (Secure Sockets Layer). This encodes the data traffic between the browser and the webserver, so that eavesdroppers cannot read the contents of the pages being downloaded.

- Sensitive data (e.g. credit-card details) is encrypted by the brower before sending.
- Often used by commercial sites, but usually limited to a small group of pages per site, due to overheads involved in maintenance and encryption computations.
- Look for the key or padlock symbol in Internet Explorer and Firefox...

Remember that this only protects the actual information transfer; data can still be vulnerable at either end of the encrypted transfer.

Types of Encryption 1: Symmetric

- Uses the same key to encrypt and decrypt
- Easy to understand and implement
- Requires *key exchange* by some trusted method

Examples:

- Simple cyphers (e.g. a=1, b=2, etc.)
- DES (Data Encryption Standard) - uses 56-bit keys

Types of Encryption 2: Asymmetric

- Different keys to encrypt and decrypt (*key pair*)
- One key is published (the *public key*)
- Other key is kept secret (the *private key*)
- Avoids problems with *key exchange*

Examples:

- RSA - Patented, US Government-supported system
- PGP - “Pretty Good Privacy” - *de facto* standard

To understand public key cryptography, imagine the public key as a padlock, and the private key as the padlock's key. Padlocks can generally be easily locked by anyone, but need a key to unlock them. To encrypt a message, the recipient sends out or publishes their padlock, which the sender snaps shut onto the box containing the message (ie encrypts it). The box can then be sent to the recipient, who is able to unlock it with their key. The fundamental advantage that this process has over simple symmetric encryption is that the private key never leaves the recipient, thus solving any problems with key distribution or exchange.

Public Key Encryption/Decryption:

The process of sending an encrypted message is simple:

1. I create a *key-pair* and publish the public key to a public *key-server*
2. You download my public key from the key-server, and use it to encrypt a message
3. You send this encrypted message (the *ciphertext*) to me
4. I use my private key to decrypt the message

As my private key is secret, only I can read the message

Note that you only need to create the key-pair once, which then effectively becomes your “identity” when published to the key servers. Your private key is additionally protected by a *passphrase*, which you should take great care not to forget; the nature of PGP systems means that if forgotten, the passphrase is not recoverable, and hence the key-pair is useless--leaving any encrypted data completely unreadable.

Digital Signatures:

If the encryption/decryption procedure is reversed, the key-pair can be used to identify and verify the sender of a message.

1. I use my private key to sign a message
2. Anyone can check my signature against my public key
3. Message must be from me, as only I know private key

Digital signature may be combined with encryption, to give secure and authenticated data exchange.

Further reading...

The Code Book (Singh 1999) has more detail on public key cryptography.

Problems with Strong Cryptography

> "...encryption is one of very few powerful technologies that do not seem to have a destructive downside.... About the worst it can do is protect criminals from detection or keep shady electronic transactions secret." Esther Dyson, *Release 2.0* (1997)

Dyson perhaps underestimates the fears that governments have regarding strong cyptography, namely that criminals will be able to communicate freely and securely without fear of eavesdropping.

In the US, cryptographic software was regarded as "munitions" and its export was restricted -- until recently, limited in strength without special licence; though now exportable to "trusted countries" only (i.e. not Libya, Iraq, etc.). In Europe, the debate still ongoing, but the EU is likely to sign up to similar multinational restriction agreements.

In UK, the new Regulation of Investigatory Powers (RIP) Act recently passed into law, giving policing authorities new powers to demand decryption keys, and the right to intercept any electronic communication; it may be used to force ISPs to keep records of their customers' accesses and communications.

Many consider the RIP Act to be one of the most invasive laws ever passed by a democratic government. The section on surrendering decryption keys, for example, places severe penalties on those refusing to reveal their key, whatever the reason - potentially even if it is just forgotten. This highlights the concern that many governments have over the use of strong cryptography.

Key Strength

- measure of "unbreakability"
- 128-bit and 256-bit are most commonly used today
- some governments restrict use according to keystrength

The *key strength* of an encryption technology is an indication of how securely it protects data, and hence how much you can trust its protection. In considering any encryption software, the key strength it uses will be a major factor affecting its overall usefulness. It is measured by the length of the key used to encrypt the data:

- 40-bit - “export strength” - breakable within a few minutes given the best available hardware
- 56-bit - US proposed “strong export” - breakable in about twenty hours
- 128-bit - US “domestic strength” - breakable in about a thousand years
- 256-bit or more - unbreakable? At least, not in a feasible time with current levels of computing power.

After the lifting of the export restrictions, most browsers now use high-strength technologies (at least 128-bit), though if you are using an older computer, you may have a browser that uses weaker security. Check your browser's capabilities by going to a secure server and examining the page properties.

For some assymetric encryption methods, longer key lengths are needed to provide equivalent strength, so for RSA encryption, a 3072-bit key is equivalent to a 128-bit symmetric key.[i]

For more statistics on cracking these encryption methods, and a chance to participate, see `http://www.distributed.net/`, a project which harnesses your computer's idle time to test the strength of encryption methods. in .

Key Escrow

A popular (with governments, that is) solution to the problem is to allow strong cryptography on condition that the private keys are stored in a secure repository, accessible only to police and government, and thus allowing surveillance.

There is strong opposition to this idea, on the grounds that the repository (at a “trusted third party”) may be hacked, compromising everyone's security, or that the system may be abused in other ways.

See also Denning & Barlow in Ludlow (1996) on the “Clipper Chip debate” - an encryption chip which allowed a “back-door” for surveillance. The arguments are similar.

There are also more general problems with the use of cryptography in everyday life. Mobile phones depend on cyptographic algorithms to prevent people listening in - in fact, the DECT system was recently cracked [ii], potentially allowing the wireless interception of household calls. Similarly, a weak algorithm in a hardware locking system used widely in cars, garage doors, and other remote entry systems, could potentially allow the development of a 'universal key' for those devices[iii].

[i] See [42] for a full discussion.
[ii] As reported in slashdot [http://it.slashdot.org/article.pl?sid=08%2F12%2F30%2F133222&from=rss], 30 Dec 2008.
[iii] Eisenbarth et al. (2008) "Physical Cryptanalysis of KeeLoq Code Hopping Applications". ePrint [http://eprint.iacr.org/2008/058]

Computer Crime and Legislation

Where the Internet is concerned, legislation is often the weakest form of protection. Since international boundaries are relatively meaningless, there are difficulties in defining the jurisdiction of courts.

Computer Misuse

The Computer Misuse Act 1990 was designed to deter hackers -- see Ayres (1999).

There are several types of offence covered by this act, including:

- **Hacking.** -- breaking into computer systems without authorisation
- **Cracking.** -- breaking or removing copy-protection on software
- **Phreaking.** -- exploring communications (esp. telephone) networks to gain free access, calls or information

But with all computer misuse, the general rule is that prevention is better than cure--secure computer systems, passwords and cryptography provide a better solution than after-the-event laws and punishments, which should be considered only as a last resort.

Note

The term “hacker” can also mean just someone who programs in a particular way, or who just enjoys tinkering with computers; in some circles I'd describe myself as a hacker, though I don't attempt to break into computer systems (except my own!). Many hackers (in the legitimate sense) have campaigned for the term “cracker” to be used universally for anyone involved in illegitimate activity involving computers. I list the terms as above since that's how the Computer Misuse Act defined them.

Hacking: types of attack

- viruses - most common form of attack
- denial of service attacks
- trojans (or trojan horses)
- brute-force and social engineering password attacks
- port scanning and spoofing
- phishing
- ransomware

Viruses

- Easily transferred in emails or downloaded files
- May damage data on infected computer
- May allow privileged access to host
- May flood the network with spurious data

Staying safe...

Use a virus checker, and make sure you update it regularly.

Keep your system files and applications up to date (e.g. with Windows/Office Update).

Phishing

This is a method of luring an unsuspecting user into giving out their username and password for a secure web resource, usually a bank or credit card account. Ebay and PayPal are particularly susceptible to this type of attack.

- usually achieved by creating a website identical to the secure site
- user is sent email requesting them to log in, and providing a link to the bogus site
- when user logs in, password is stored and used to access the account by the attacker
- difficult to guard against, particularly if using HTML email

Currently no law specifically against this, though some experts think this may come under the Computer Misuse Act, and may also be testable under trademark laws (passing off as another's web site).

Cryptovirus or RansomWare

A form of trojan that has been around since 1989 (as the “PC CYBORG” trojan), this type of malware is becoming more common. It infects the target computer by encrypting the owner's personal files. The victim is then contacted and offered a key to decrypt the files in exchange for cash or valuable information (see [11]).

Whilst the effects of early variants of this type of virus were relatively easy to decrypt, the latest sightings are more worrying, with more complex encryption algorithms and longer key lengths being used. [iv]

[iv] The Register, 24 July 2006 `http://www.theregister.co.uk/2006/07/24/ransomware/`

Note

See also the section on security [http://www.service.ex.ac.uk/cmit/modules/the_internet/webct/ch06.html] in MIT2114/2214 “The Internet”, which also looks at spyware and other forms of intrusion.

Content Regulation

- restriction of content entering country, domain or organisation
- motives need to be clear; blocking needs to be as objective as possible
- where is the line drawn between regulation and censorship?

Many people (especially governments) wish to have some method of restricting the content of providers in both traditional and digital media. In May 1998, OFTEL (Office of Telecommunications) expressed concerns over the difficulties of regulating the ever-changing digital media, when it published evidence given to an inquiry by the Select Committee on Culture, Media and Sport. A European Green Paper discussing these problems was published in 1997.

Examples of Singapore, Australia and China:

- Controlling and monitoring what is available to local users
- Restricting access to “undesirable” resources
- See, for example, EFA: Internet Censorship Laws in Australia [http://www.efa.org.au/Issues/Censor/cens1.html]

Organisations and individuals are also often keen to restrict content (for example, the university, schools, parents, etc.

Motivations for restricting content are varied - political, financial, moral - and the controls are often extremely subjective (what is a “bad” website?).

See also Chapter 1, *Education and Research*.

Firewalls and Intranets

- mechanism for content regulation and data filtering
- can be used both ways:
  - blocking unwanted traffic from entering the sub-network
  - preventing subnet users' use of unauthorised material/sites

Often, the best way to safeguard information is to fence it in, using a *firewall*. This is a way of organising a company network so that all external traffic goes through a single computer, which can act as a filter to prevent an unwanted flow of information. Everything behind the firewall is protected from the outside world, the Internet at large, because the firewall host prevents unwanted or unknown data packets from entering the internal network, often called the *intranet*. Firewalls are often also used to prevent employees from accessing non-work-related Internet resources, restricting them only to the resources available within the intranet, or perhaps a predetermined selection of web sites.

The use of a personal firewall (such as ZoneAlarm [http://www.zonelabs.com/], or the firewall built into Windows XP or Vista) on your own computer can often reveal unwanted data movements in both directions. It works by checking all incoming and outgoing data types, and reports anything unusual, which you can then allow (if you know what has initiated it) or block (if you're not sure).

Privacy and Data Protection

- Do you value your personal data?
- Legislation to protect personal data
- Legislation to promote better access to public data

You may not realise it, but your personal details are a valuable asset. In a world where businesses are increasingly looking to target individuals more effectively, data about those individuals is in demand. Buying and selling lists of email addresses and demographic details is big business, and it's now common for companies to trade “free” software for personal information. You should consider carefully what the company is likely to do with that information *before* you give it to them.

The Data Protection Acts

The concept of data protection exists mainly to protect an individual's personal data held by a third party, and governs how that data can be stored and accessed. A typical example is credit information used by banks and retailers to check an individual's credit-worthiness.

It's important to note that what is being protected is not the data itself, but the subject of the data; the individual. The data protection act gives the individual the right to access their data, no matter where it is stored.

The original Data Protection Act of 1986 was designed to protect personal data stored by companies and organisations from being misused. The 1998 Data Protection Act strengthened this to conform to the European Data Directive. Details of the European Data Protection Act can be found at the Europa [http://www.europa.eu/] website.

The UK Data Protection Registrar issues guidelines covering the law in Britain, and including the Data Protection Act 1998, which came into effect on 1 March 2000, and the Privacy

and Electronic Communications (EC Directive) Regulations 2003. See the Information Commissioner's website [http://www.ico.gov.uk/] for more information.

The University's Data Protection Officer has produced leaflets outlining your rights to your data: for further information, see the University web pages on Data Protection [http://as.exeter.ac.uk/library/about/special/recordsmanagement/dataprotection/].

The Freedom of Information Act 2000 also extends the rights of citizens to gain access to the operation and decision-making processes of all public bodies, including universities.

Privacy and social networking

- Personal information is willingly divulged
- We have little control over who has access to it
- It can be frighteningly persistent, yet seem ephemeral
- Could it come back to haunt us?

But perhaps the greatest threat to privacy is of our own making. We are happy to divulge so much personal information now, in the interests of sharing experiences with friends and family on Facebook, or upload videos and photographs of our children to Flickr or YouTube, without thinking about the implications. Even something as innocuous as sharing your family tree online can have potential consequences (does your bank ask you for your mother's maiden name as a "security" question?).

For example, the recent changes to Facebook's security policy were widely criticised, as their 'simplification' encouraged wider sharing and made it more difficult to control access to personal data[v]. It's in the interests of those running the site that you share as much information as possible, so the defaults will always encourage sharing.

It's also clear how much the social networking companies value your personal data when you try to remove information. An art project in Italy (Seppukoo [http://www.seppukoo.com/]) encourages Facebook users to "commit virtual suicide" by unfriending all their contacts. Upset by the implications of this, Facebook has blocked their IP addresses and sent a Cease and Desist letter to the organisers, requesting the removal of the site[vi].

Of course, the real conundrum of the Internet is that information is both ephemeral (appearing and disappearing in an instant) and persistent (forever online, and copied to who-knows-where). We're trusting unknown companies and individuals with our most personal details, which may be used against us in the future.

Further reading

[v] BBC News [http://news.bbc.co.uk/1/hi/8405334.stm], 10 Dec 2009
[vi] See article in Daily Online Examiner [http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=120004]

A good collection of articles detailing the opinions and all sides in these issues can be found in *High Noon on the Electronic Frontier* (Ludlow 1996), especially parts I and II. Although these are rather dated, they still give insights into the mind of the computer criminal.

There is a more detailed discussion of privacy, with numerous case studies, in *Database Nation* (Garfinkel 2000). Bruce Schneier has a blog [http://www.schneier.com/blog/] which is an excellent commentary on current security issues, and complements his books, *Secrets and Lies* (2000) and *Beyond Fear* (2003).

For an overview of all aspects of commercial cryptographic systems, there are some excellent articles on the RSA [http://www.rsa.com/] and PGP [http://www.pgpi.org/] websites.

A number of government bodies issue guidelines on computer and internet misuse, including Ofcom [http://www.ofcom.org.uk/], the DTI (e-security [http://www.dti.gov.uk/industries/information_security] and e-communications [http://www.dti.gov.uk/industries/ecommunications/]), etc.

Relevant legislation has been cited within the text, and is collected in the bibliography under Acts of Parliament.

A number of journals are available in this area, including *Computers and Security*, *Computer Law and Security Report* [Elsevier ScienceDirect [http://www.library.ex.ac.uk/electronic/]], Journal of Information, Law and Technology [online [http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/]]

Chapter 6. Intelligence and Ubiquity

Future trends in computing and the Internet

- Intelligent computers?
- Autonomous agents?
- Calm technologies?
- Cyborg bodies?

What is Artificial Intelligence (AI)?

> Any sufficiently advanced technology is indistinguishable from magic.
>
> —Arthur C. Clarke, “Profiles of The Future”, 1961

- Hard AI - using computers to mimic the brain, to understand its workings
- Soft AI - learning about computing from the way we think the brain may work

In reality, any use of computers that seems to work in a brain-like way or exhibits properties we associate with human intelligence. e.g.:

- Expert systems - logical, rule-based system that finds answers by asking a series of simple questions; often used for diagnosis, fault-finding or problem solving.
- Heuristic systems - programs that find answers by making 'intelligent guesses'; used where calculating an answer would take too long or would need more evidence/data.
- Neural networks - software that emulates (very simply) the neural patterns of the brain; able to exhibit learning after a period of training; used where sample data is available and learning is required.

Uses of AI on the Internet

AI tends to be used on the Internet for two distinct purposes:

- Technical: to automate the monitoring, routing and repair of the Internet infrastructure
- Human-centred: to make the Internet easier to use by providing more humanistic interfaces

Of these two domains, the technical realm is perhaps the most susceptible to benefit from these advances. It's a restricted, fairly predictable and machine-readable area where computers can accurately analyse the flow of information and respond to it.

The human domain is rather more tricky, for the most part. As humans, we are very good at various tasks which are notoriously difficult for computers to grasp. For example, we are excellent at analysing and recognising visual information, and we have a complex system of language which tends to resist machine-recognition.

Whilst in the technical domain, the advances that are made are largley invisible, it's in the human domain that the greatest impact of AI will occur.

AI in Infrastructure

- Adaptive software
  - used to route IP (Internet Protocol) traffic round troublespots
  - used to limit bandwidth or prioritise traffic in busy periods
  - used to track and kill viruses and hacker attacks
- Expert systems
  - diagnose and repair network faults automatically
  - guide human call-centre operatives in diagnosing faults

The highly networked infrastructure of the Internet closely resembles some of the classic problems in mathematics, notably the *Travelling Salesman Problem*, which attempts to find the shortest route between a number of visited points in a network (of Internet routers, or potential sales opportunities). As the number of visits and the size of the network grows, it's increasingly difficult to calculate an exact strategy for the shortest route, as the possible combinations become so immense.

So guesswork is needed, in the form of *heuristics*, to create a “good enough” answer, and this is what happens in most IP routers.

Similarly, software systems often deploy *expert systems* where a complex problem with many variables needs to be solved. Expert systems work by questioning a human or machine, or sensing conditions, according to a sequence of prompts. The response to each prompt changes the behaviour of the system and causing differing sets of questions or conditions to be used. The prompts and responses are said to capture the behaviour of an knowledgeable expert in diagnosing problems.

The most prevalent use now is in technical support call-centres, where the system of prompts and responses generates a solution (in theory at least) without the operative needing expert knowledge themselves.

AI in Usability and Interaction

- Natural language interfaces (e.g. Ask Jeeves - www.ask.co.uk)
- Speech-based interfaces & voice recognition
- Automatic translation of web pages (e.g. Babelfish, or translate.google.com)
- Picture recognition and searching (e.g. www.google.co.uk/imghp, TinEye, etc.)
- Expert systems - provide troubleshooting advice or subject specific diagnosis

The ability to handle the most natural way of interacting with each other, language and speech, has proved difficult for interface designers to solve. Speech-based interfaces (both for recognition and production of natural language) are still relatively limited. Screen readers and text-to-speech applications still sound rather artificial and are prone to intonation and emphasis errors, though speech recognition has improved, with the ability to parse unbroken speech now fairly common, albeit still needing a training period to adapt to an individual's voice pattern. Speech recognition is also widely used in simple command-based interfaces, where there is a controlled vocabulary and a restricted set of possible commands expected.

Automatic translation is also still limited in accuracy, though most web search engines have some capability to produce a rough draft of a translation - enough to get the general sense of the text in most cases.

There have been various attempts at using more intelligent techniques for searching and categorising images, which is a surprisingly difficult task. Accurate recognition of the contents of a picture is still a long way off, but there are applications which allow searches for 'similar' content with some degree of success. For example, TinEye's Reverse Image Search [http://www.tineye.com/] looks for images that are based on one that you upload to it - good for seeing where a logo has been used or modified. And Eyealike [http://www.eyealike.com/], Polar Rose [http://www.polarrose.com/] and Viewdle [http://www.viewdle.com/] all use facial recognition software to look for similar faces - apparently very popular on online dating sites!

Autonomous Agents, Crawlers and Bots

- Software programs with “intelligence” to act autonomously
- May be trained to search for personal interests
- Many types, including *cancelbots*, *mailbots*, *searchbots*, etc.
- More listed at the BotSpot [http://www.botspot.com/] website...

Most web search engines use robots (known as spiders or webcrawlers) to gather data for their databases. There are other uses for robots too, in fact, you can download them and let them do your searching for you.

In fact, there are agents in much everyday software, that exhibit some form of independent behaviour in response to their surrounding. A basic agent behaviour is built into MS Windows, for example, to respond to potentially problematic conditions such as lack of disk space (in this case, the agent initiates a “disk cleanup” task.

Other uses are rather cleverer, such as bots that monitor web traffic and respond to potential hazards (anti-virus and firewall), through to natural language interfaces which allow you to use human language to give instructions to a program.

Bots and agents can also be used in malware, to take over a computer and respond to commands from an outside controller, perhaps capturing sensitive information or allowing privileged access.

So what is an agent anyway?

- **Autonomous.** Agents operate without the direct intervention of humans or others, and have some kind of control over their actions and internal state;
- **Socially Reactive.** Agents perceive their environment, (which may be the physical world, a user via a graphical user interface, a collection of other agents, the Internet, or perhaps all of these combined), and respond in a timely fashion to changes that occur in it;
- **Pro-active.** Agents do not simply act in response to their environment, they are able to exhibit goal-directed behaviour by taking the initiative.

From Wooldridge and Jennings (1995)

Agents in Online Communities

- Widely used in MUDs, MOOs and other online communities
  - They can be librarians, direction finders, information gatherers and even gossips
- More recently, used
- Primitive robots are easy to program

Ken Schweller

- Buena Vista University, Storm Lake, Iowa College Town MOO, created for the staff & students of the Computer Science Dept.
- Developed a `user-programmable' chatterbot (a `MrChat' style bot?), that could easily be taught to interact with a particular personality or role.

Chatterbots were developed to provide a natural language interface within a restricted domain of knowledge - they can talk with some appearance of understanding within the limits of their programmed “knowledge”.

The most famous, *Eliza*, emulates a Rogerian psychoanalyst, asking very reflective questions and turning responses back onto the subject. A further development, A.L.I.C.E., was written to try to pass the Turing Test, a crude measure of the effectiveness of an artificially intelligent entity (talk to a recent implementation at pandorabots.com [http://www.pandorabots.com/pandora/talk?botid=f5d922d97e345aa1]).

Lenny Foner and Julia

- Graduate student at MIT;
- Observed MUDders who tried to chat up Julia, a TinyMUD bot;
- Written up in his paper *What's an agent, anyway?* (Foner 1993 [http://www.ex.ac.uk/cmit/modules/cyberspace/Agents--Julia.pdf])

Foner's paper highlighted the fact that there are social and psychological considerations to even the most primitive virtual communities, and that software programs can be used to monitor and assist participants with some degree of “awareness” of these considerations.

The exceprts make insteresting reading, and it's quite clear that the male participant was convinced by the bot's personality for a considerable time - it's not clear whether Julia passed the Turing Test, or he failed it!

Common sense?

- Real-world knowledge is the key to realistic interaction
- Because real-world knowledge is difficult to program, current chatterbots use a restricted domain, or use tactics such as changing the subject or saying something provocative to keep conversation moving

Robots for Data Harvesting

- Agents or Robots are also used to wander the web, cataloguing or collating statistics
  - Usually called webcrawlers or harvesters
  - Most search engines employ webcrawlers
- Often also used to gather personal data from the web, such as email addresses or telephone numbers
  - avoid placing personal data on the web if you don't like spam!

Robot Protocols

- Robot access can easily overload servers
- Robot Exclusion Protocol
  - Gives guidance on acceptable behaviour
- Friendliness cannot be enforced easily

Robots can cause damage by quickly and repeatedly accessing web files, causing the server to overload. They can also become confused when accessing dynamically generated web pages, such as databases, product catalogues and even web logs. The Robot Exclusion Protocol allows sites to offer guidance to robots, indicating what is `acceptable behaviour' on that site. The site administrator provides hints (in a file called robots.txt) that show where robots will have problems gathering data. Robots cannot be forced to follow certain behaviour patterns, but it's good manners to program your bot to follow these protocols.

Aside: Robot Ethics

- Asimov's Three Laws of Robotics
  1. A robot may not injure a human being, or, through inaction, allow a human being to come to harm.
  2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
  3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Handbook of Robotics, 56th Edition, AD 2058, as quoted in Asimov (1942) *I, Robot*.

Some examples of current progress in robotics:

2008. Boston Dynamics Big Dog, Available at: http://www.youtube.com/watch?v=W1czBcnX1Ww [Accessed March 1, 2010].

2009a. James May - Gemenoid Robot "clone" of its designer *HQ*, Available at: http://www.youtube.com/watch?v=XAO_DTeoVm8 [Accessed March 1, 2010].

2009b. KOBIAN: Emotional humanoid robot, Available at: http://www.youtube.com/watch?v=2FBUt336wBI [Accessed March 1, 2010].

2008. Robots with a mind of their own, Available at: http://www.youtube.com/watch?v=SkvpEfAPXn4 [Accessed March 1, 2010].

AI today and tomorrow

Today's Internet is already using AI technologies to create a faster, safer, easier-to-use environment.

- Online retailers are using customer statistics to `guess' your preferences and make recommendations about other products you may like;
- Search engines use agents to scour the web for new information;
- Search engines use their statistics to create site ratings and make sure the most popular sites are presented first in their results;
- Search engines use statistical analysis to predict the things you're interested in and to guess advertisers you're most likely to click onto.

The Ubiquitous Computer

- Embedded computers already built into many objects
- Becoming more intelligent
- Becoming more connected (e.g. Bluetooth “personal area network)”

In the future, the Internet will become pervasive and ubiquitous, with even the smallest devices connected together. Computers are already embedded into many objects, and as processing power increases and size decreases, these objects will be more intelligent and more connected.

Wearable computers and intelligent clothing will talk to the devices you come into contact with, and even set the correct programme on the washing machine! Rather than using your PC or laptop to access the Internet, you'll use “Internet Appliances” which have a single purpose, e.g. a dedicated emailer (built into the collar of your jacket, perhaps?), an online shopping appliance in the kitchen for the groceries, a fully interactive TV with video on demaind, a car that avoids traffic jams, and emails the garage when it needs a repair or service.

Of course, this has a downside - we will always be connected, always locatable and never “offline” - will our privacy suffer?

Calm Technology

- Proposed by Mark Weiser in early 90s
- Technology recedes into the background
- Embedded devices reduce our need to learn interfaces
- Move towards “information appliances”

Further reading: Mark Weiser's homepage `http://www.ubiq.com/weiser/`, and *The Invisible Computer*, Norman (1998)

Wearable Computers

- Devices will become more robust and embeddable
- Washable and wearable information devices soon possible
- Military applications are driving this technology
- MIT Media Lab at the forefront (`http://www.media.mit.edu/wearables/`)

As the desire to create more pervasive applications for the Internet grows, hardware is evolving too - into smaller, more durable and more flexible forms, that allow devices to “go anywhere”. Already, some retailers use intelligent tags to track clothing in their stores, both before and after purchase, giving the possibility clothes that alert staff that their wearer is a loyal customer.

Perhaps more interestingly, there is also the potential for our clothes to become part of our

The Cyborg Body

- Already use technology to replace/enhance senses
  - e.g. hearing aids, spectacles
- Not too great a leap towards sensory *augmentation*
  - e.g. night vision
- Some technologies already in use (implanted RFID, etc.)
- The next stage in human evolution?

Marshall McLuhan's was the first to examine the idea of technology as an extension of our senses, in *Understanding Media: the extensions of man* ([52]).

Chapter 7. Cyberspace Philosophy

- Defining cyberspace
- Analysing the properties of cyberspace
- Predicting the effects of cyberspace
  - on knowledge
  - on ethics
  - on our understanding of reality

What is Cyberspace?

Defining cyberspace is really a matter of context. For example, John Perry Barlow, a founder of the Electronic Frontier Foundation, famously defined it as “... where you are when you are talking on the telephone.”. Others have defined it more narrowly, as the interactive space that is used for all computer mediated communication, or even the space that the web resides in. William Gibson, who coined the term in his Sci-fi novel *Neuromancer* (1984), suggested it was a “consensual hallucination”. Here, we'll take the broadest of views.

A common factor in almost all definitions of cyberspace is the sense of place that they convey - cyberspace is most definitely a place where you chat, explore, research and play.

The Shape of Cyberspace

How can we discover the geography of the Internet? How does this geography alter our perception of the real and virtual worlds?

Mathematical approaches

Since the Internet is really just a set of interconnected points, it is readily examined using the formal techniques of topology or graph theory.

A common technique is to use Internet traffic diagnostics, such as the **ping** and **traceroute** commands to explore the structure of the nodes that connect to form the internet. Webcrawlers (as used by search engines) can also explore and discover the underlying network.

The resulting maps are a snapshot of the Internet's topology at a give point in time, and aside from being quite beautiful, also clearly illustrate the concentration of data paths at key points in the network, and the resilience of the Internet through its use of multiple pathways between nodes.

Further reading: Opte.org [`http://www.opte.org/`]; Internet Mapping Project [`http://www.cheswick.com/ches/map/`].

Approaches from Geography

One of the most attractive methods of examining the structure of the Internet comes from the field of traditional cartography. Maps of the Internet can be made in many ways, such as overlaying a physical map of the world with nodes and links, or taking a central node and drawing network connections radiating out from this.

Further reading: CyberGeography.org [http://www.cybergeography.org/home.html]

The Death of Distance

The implementation of the Internet on a global scale has been a fundamental part of the globalisation of industry and commerce. A similar revolution occurred with the first intercontinental telegraph links, where there was suddenly the possibility of sending information almost instantaneously in a world where transatlantic travel still took weeks.

Many commentators have examined how our perception of the world's size and shape has changed because of this, from Marshall McLuhan's “global village” through to Frances Cairncross coining the “death of distance” phrase to sum up the effects of instant communication.

What we are beginning to realise is that the world (and in particular, human society) is a form of network in itself, and one in which the degree of connectedness is increasing rapidly with the advent of the internet. The rise of social networking sites such as Facebook and MySpace have made this phenomenon so much more tangible.

For further reading, examine Milgram's “Small World Problem”, which popularised the idea of “six degrees of separation” (1967), and was more recently tested by Duncan J. Watts in his book *Six Degrees*. The BBC has also featured this topic, see Whitehouse (1999a).

New Geographies

Since cyberspace is not bound by physical laws and real-world constraints, we can be more imaginitive in our use of spatial metaphors for online worlds. To some extent this has already been seen in computer games, where multidimensional (i.e. more than three dimensions) worlds, hyperspace jumps and wormholes become possible. Kant postulated that we are bound to a three-dimensional world only by experience, and that there is no theoretical problems with the existence of spaces of four, five, or more dimensions (Browne Garnett Jr., 1965).

Cyberspace also allows us to experience something close to a perfect world too - virtual reality can model the world exactly, and create a place which is mathematically perfect, an idea which looks back to the philosophy of Plato and his ideal forms (Heim 1993, p.8).

Knowledge and the Internet

What is Knowledge?

There has long been discussion on the nature of knowledge, and on the differences between data, information, knowledge and wisdom. As we move into the information age, these questions will become more important. The reliability and usefulness of the information around us, and the techniques we will need to master to discern this and filter out the signal from the noise are all part of our philosophy of information.

Hyperlinks - meaningful and meaningless

As an example, let's look at the hyperlink. Hypertext links are both simple and complex. On the surface, they merely provide a reference to another online resource, which a browser can use to access that resource. But links can be used in many more ways than this simplicity would suggest. They can point to small or large amounts of information (a glossary entry, or a whole encyclopedia). They can reference local or remote resources. They can even be used to add irony (the e-zine *Suck [http://www.suck.com/]* was the exemplar of this), or to add meaning to an otherwise simple phrase. In effect, the link has become “a rhetorical device loaded with meaning.” (Shields 2000).

But the way the link appears does not necessarily indicate any of this - you have to click to discover the role and meaning of the link.

Dreyfus argues that this presents a paradox. The hyperlink was created “to use the speed and processing power of computers to relate a vast amount of information without needing to understand it or impose any authoritarian or even generally accepted structure on it” (2001, p.9), rather than for any purpose related to meaning or understanding.

Key readings: Dreyfus (2001, ch.1); Shields (2000); Landow (1997).

Transient and persistent

Information in cyberspace tends to be interactive, dynamic and temporary. Most web sites are restructured regularly, and their content changes often on a daily basis, which means that whilst the information is up to date and fresh, it can be difficult to return to it and rediscover it.

Despite this, web information can also be surprisingly persistent. Controversial documents that have been taken down from one website often appear in multiple mirrored locations. Often, the chances of survival of a resource are primarily dependent upon the number of people interested in the resource, often out of the control of the owner/webmaster.

There have been attempts at ensuring the core material of the web does not disappear unnoticed. For example, the WayBack Machine [http://www.archive.org/] attempts to archive a significant proportion of web information for future generations. But the most successful and most widely used archive is the cache that some search engines store of the

pages they have catalogued. Coupled with the power of the search engine, the cached copies of websites can be startlingly persistent, again showing that information can live well beyond its owner's control.

Further reading: Brown & Duguid (2000)

Memory and Findability

Another observation on the use of knowledge arises from the power of Google and other search engines to find almost everything we need at the click of a button. There is no longer a need to remember facts, we can just google them. We are only limited by the skill with which we use the search engine, and how specific and trustworthy we need the answer to be.

It's clear that developing this type of “informational intelligence” is a much better strategy in the long-term than memorising facts (especially if you have as poor memory retention as I have).

Further reading: Morville (2005)

Authority and the creation of canonical works

One of the casualties, perhaps, of this early stage in the information age, is the canonical work, the authoritative, quotable, stable text that print publication inevitably tends to produce. How do we develop systems of classification, authority and structure that allow us to reference online materials? And how do we cope with the transience that we discussed earlier with respect to this referencing.

Again, search engines can help here, with Google keeping cached copies of many pages that have long since disappeared, but there is little systematic archiving of useful material outside of the organisations that are generating it.

Kleinberg (1999)

The Semantic Web

One attempt at imposing structure and *metadata* onto the web as it exists today involves adding extra, meaningful, but invisible information to each web resource, so that information-processing applications such as Google can more effectively analyse and catalogue web information. The *Semantic Web [http://www.w3.org/2001/sw/]* is a group organised by the World Wide Web Consortium, of technologies and individuals that are attempting to do this.

At the core of the Semantic Web initiative is the creation of *ontologies*, which are structured vocabularies of common terms and their relationships, and which allow a measure of interoperability between different web applications.

At the grass roots level, there is also a strong movement towards reusing and “repurposing” data that is available on the Internet (often called *mashups*. For example, data available from Google Maps can be combined with data from a telephone directory to create a more *semantic*

map, which provides information such as contact details. If combined with business websites, there's the possiblity of mapping which has a very rich set of information associated with each location. See, for example, Flickr maps [`http://www.flickr.com/map/`] where mapping information is applied to photographs.

Cyberspace and Responsibility

The prevalence and speed of communications technologies are giving rise to a number of ethical dilemmas which philosophers are beginning to puzzle over, as they try to understand the new information landscape.

Many centre around issues of access. For some societies, a lack of access to information is a generational problem; the use of ICTs needs to be learned, and as ICT is integratesd into schools, the problems will disappear over time.

More often, availability of access is more linked to availibility of resources and wealth in general. The digital divide is often referred to as a resource problem, and in many third world countries

Being a Good Cybercitizen

Key reading: Graham (1999).

Is cyberspace really a space?

What are its distinctive characteristics? John Perry Barlow, former lyricist for the Grateful Dead and now a respected voice on the implications of technology, suggested that “Cyberspace is where your money is”.

In his groundbreaking novel Neuromancer, author William Gibson laid the foundation of thought about cyberspace as a space separate from the physical world:

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...
>
> —William Gibson, *Neuromancer* (1984).

Gibson's view of cyberspace, seen from a time before the Internet was well known, is of a data space where information is represented as shapes and forms that can be navigated through. We have a little way to go before this navigable space with its strong spatial metaphors can be realised for the ordinary Internet user, but progress in virtual reality technologies has shown that it will be possible.

In the film *The Matrix*, cyberspace is an escape from reality, a creation which gives participants a semblance of normality and protects its inhabitants from the truth of how the

world really is. It's a place where almost everyone plays according to the rules because they believe that cyberspace is real, but where the realisation that the matrix is just software frees an inhabitant to do “impossible” things, to subvert the rules (of society, of physics, etc.). The Matrix seems real because the majority believe it to be real.

To some extent, we already have navigable spaces on the Internet. The World Wide Web is a “space” in the sense that we move through it and are able to explore and map its contours and boundaries. Efforts are being made to construct a geography of this new space, examining the pathways taken by data and the structures of the web sites themselves.

But the Web is a highly abstract space, and usually gives us no sense of place. MUDs and MOOs, on the other hand, are specifically constructed to have the characteristics of place, in order to make the virtual space more “real” and familiar.

Clay Shirky suggests that their social nature was an accidental side-effect of the games culture, and had to evolve rather than being deliberately planned and created:

> Had the developers of the original MUD set out to create a purely social arena like LambdaMOO, they would have failed. Ideas, both cultural and computational, about social organization of electronic spaces were too embryonic in the late 70s; any such attempt would have bogged down in the details. By starting with a game and letting it develop from there, places like LambdaMOO have been able to organize organically.
>
> —Clay Shirky (web reference now unavailable)

Margaret Wertheim (1999) draws parallels with the spiritual realms so predominant in the medieval period, and argues that cyberspace is directly analagous to these 'other spaces'.

> As with the medievals, we in the technologically charged West on the eve of the twenty-first century increasingly contend with a two-phase reality.
>
> —(Wertheim 1999:228)

She believes that both the spiritual world of Dante and the information space of cyberspace are real in a metaphysical sense

> Despite its lack of physicality, cyberspace is a real place. I am there--whatever this statement may ultimately turn out to mean.
>
> —(Wertheim 1999:229)

Sherry Turkle (1995) talks of the way that our `being' in cyberspace can be radically different to our physical being; a way to explore the identities we'd like to have. This creation of multiple identities can significantly help some people suffering from some mental illnesses, or even just shyness.

Gordon Graham (1999) examines cyberspace as a `radically new' technology, commenting that

> If 'being' in cyberspace is a new kind of being, distinct from but nonetheless just as metaphysically substantive as `being' in the flesh for instance, then there can be little doubt that the Internet is indeed a radically new technology.

—(Graham 1999:24)

To some, the future appears to be rather bleak given the possibilities for abuse and infringement of civil liberties that cyberspace seems to offer:

> ...there is every potential, if we are not careful, for cyberspace to be less like Heaven, and more like Hell.
>
> —(Wertheim 1999:298)

though it's my opinion that, if we address the problems outlined in this module trhough education, technology and democratic governance of the Internet, we have the chance to build a more utopian global society than is possible in real life.

Chapter 8. The Future of Cyberspace

The Internet as a Technological Revolution

- Is the Internet revolutionary, or merely another progressive step?

Bibliography

Articles, Books and Web Resources

Note

Copies marked [GBS] or [CMIT] are CMIT staff's personal copies, but may be borrowed from the CMIT office by arrangement.

[1] Philip E Agre and Marc Rotenberg. 1998. *Technology and Privacy: The New Landscape*. MIT Press. Cambridge, MA. [Personal copy: GBS].

[2] Chris Anderson. 2006. *The Long Tail*. Random House Business. London. [Main Library 658.802 AND [http://lib.ex.ac.uk/record=b1817309]] .

[3] Robert Ayres. 1999. *The Essence of Professional Issues in Computing*. Prentice Hall. London. [Main Library 001.64 AYE [http://lib.exeter.ac.uk/record=b1630951~S6]].

[4] Paul Bambury. 1998. “A Taxonomy of Internet Commerce”. *First Monday*. 3. 10. http://www.firstmonday.org/issues/issue3_10/bambury/ . 2006-02-03.

[5] Richard Barbrook. 1998. “The Hi-Tech Gift Economy”. *First Monday*. 3. 12. http://www.firstmonday.org/issues/issue3_12/barbrook/ . 2005-12-23.

[6] Daniel Bell. 1973. *The Coming of Post-industrial Society*. Basic Books. New York. [Main Library 301.243 BEL [http://lib.exeter.ac.uk/record=b1070689~S6]] .

[7] Yochai Benkler. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press. New Haven. [Personal copy: GBS] .

[8] Tim Berners-Lee. 1999. *Weaving the Web: The Past, Present and Future of the World Wide Web by its Inventor*. Orion Business. London. [Main Library 001.64404 BER [http://lib.exeter.ac.uk/record=b1681989~S6]] .

[9] British Library. 2003. *Treasures in Full: Caxton's Chaucer*. http://www.bl.uk/treasures/caxton/homepage.html . 2006-01-30.

[10] British Library. 2006. “Intellectual Property: A Balance”. http://www.bl.uk/news/pdf/ipmanifesto.pdf . 2009-05-11.

[11] Lloyd Bridges. 2008. “The changing face of malware”. *Network Security*. 2008. 1. http://www.sciencedirect.com/science/article/B6VJG-4RNS8H7-B/2/bf940bf4a4110e9a934925f4d28be3b5 . 2008-03-01.

[12] John Seely Brown and Paul Duguid. 1996. “The Social Life of Documents”. *First Monday*. 1. 1. http://www.firstmonday.org/issues/issue1/documents/index.html . 2005-10-19.

[13] John Seely Brown and Paul Duguid. 2000. *The Social Life of Information*. Harvard Business School Press. Boston, MA. Excerpts available from: http://www.firstmonday.org/issues/issue5_4/index.html. 2005-10-19. [St Luke's Library 301.243 BRO].

[14] Vannevar Bush. 1945. “As We May Think”. *Atlantic Monthly*. 176. 101-108. Available from http://www.theatlantic.com/doc/194507/bush. 2010-01-25.

[15] Manuel Castells. 1996. *The Rise of the Network Society*. Blackwell. Oxford. [Main Library 001.64 CAS [http://lib.exeter.ac.uk/record=b1657918~S6]] .

[16] Manuel Castells. 1997. *The Power of Identity*. Blackwell. Oxford. [Main Library 001.64 CAS [http://lib.exeter.ac.uk/record=b1203246~S6]] .

[17] Manuel Castells. 1998. *End of Millenium*. Blackwell. Oxford. [Main Library 001.64 CAS [http://lib.exeter.ac.uk/record=b1203245~S6]] .

[18] Manuel Castells. 2001. *The Internet Galaxy: reflections on the Internet, Business and Society*. Blackwell. Oxford. [Main Library 001.64404 CAS [http://lib.exeter.ac.uk/record=b1676080~S6]] .

[19] Michael Chissick and Alistair Kelman. 1999. *Electronic Commerce: Law and Practice*. Sweet & Maxwell. London.

[20] W R Cornish. 2007. *Intellectual Property: patents, copyrights and allied rights*. Sixth. Sweet and Maxwell. London. [Main library 346.41048 COR [http://lib.ex.ac.uk/record=b1810246]/ Law Library: KN 111 COR].

[21] Mike Crang, Phil Crang, and Jon May. 1999. *Virtual Geographies: Bodies, Space and Relations*. Routledge. London.

[22] Jesús Cendrós Guasch and Luis Ugas. 2007. “The Digital Gap in Maracaibo City in Venezuela”. *Telematics and Informatics*. 24. 41-47. Available through Elsevier ScienceDirect via EBSCO [http://ejournals.ebsco.com/home.asp].

[23] Whitfield Diffie and Susan Landau. 1998. *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press. Cambridge, MA.

[24] Hubert L Dreyfus. 2001. *On the Internet*. Routledge. London.

[25] Esther Dyson. 1997. *Release 2.0: A design for living in the digital age*. Viking. London.

[26] May Y Chau. 1999. “Web mining technology and academic librarianship: Human-machine connections for the twenty-first century”. *First Monday*. 4. 6. http://www.firstmonday.org/issues/issue4_6/chau/index.html . 2006-01-11.

[27] Benjamin Edelman. 2008. “Typosquatting: Unintended Adventures in Browsing”. *McAfee Security Journal*. http://blog.wired.com/27bstroke6/files/mcafee_security_journal_fall_2008.pdf . 2008-02-21.

[28] Janet H Fisher. 1993. “Copyright: The glue of the system”. http://www.press.umich.edu/jep/works/fisher.copyright.html . 2006-02-24.

[29] Dominique Foray. 2004. *The Economics of Knowledge*. MIT Press. Cambridge, MA. [CMIT Office].

[30] Oliver Froehling. 1999. *Internauts and guerilleros: the Zapatista rebellion in Chiapas, Mexico and its extension into cyberspace*. In *Virtual Geographies* .

[31] Christian Fuchs and Eva Horak. 2008. “Africa and the Digital Divide”. *Telematics and Informatics*. 25. 99-116. Available through Elsevier ScienceDirect via EBSCO [http://ejournals.ebsco.com/home.asp].

[32] Simson Garfinkel. 2000. *Database Nation: The death of privacy in the 21st century*. O'Reilly and Associates. Sebastopol, CA.

[33] Simson Garfinkel and Gene Spafford. 2002. *Web Security, Privacy and Commerce*. O'Reilly and Associates. Sebastopol, CA. Second.

[34] William Gibson. 1984. *Neuromancer*. Ace. New York. [Main Library 818.5/GIB-3].

[35] William Gibson. 1988. *Mona Lisa Overdrive*. Bantam. New York.

[36] Gordon Graham. 1999. *The Internet:// A philosophical inquiry*. Routledge. London.

[37] Andreas Grosche. 2006. “Software Patents - Boon or Bane for Europe?”. *International Journal of Law and Information Technology*. 14. 3. 257-309. http://ijlit.oxfordjournals.org/cgi/content/abstract/14/3/257. 2010-02-08.

[38] Michael Heim. 1993. *The Metaphysics of Virtual Reality*. OUP. Oxford.

[39] Andrew Herman and Thomas Swiss. 2000. *The World Wide Web and Contemporary Cultural Theory*. Routledge. London. [Main Library 301.243 HER].

[40] Richard Hollingham. 2004. *Losing the Past*. First broadcast 6 & 13 October 2004 on BBC Radio 4. . http://www.bbc.co.uk/radio4/history/losing_the_past.shtml . 2006-02-03. Also available from the local media archive [http://services.ex.ac.uk/cmit/media/audio/].

[41] Bernardo A Huberman. 2001. *The Laws of the Web: Patterns in the Ecology of Information*. MIT Press. Cambridge, MA.

[42] Burt Kaliski. 2003. “TWIRL and RSA Key Size”. *RSA Technical Notes and Reports*. http://www.rsa.com/rsalabs/node.asp?id=2004 . 2008-03-01.

[43] Jon M Kleinberg. 1999. “Authoritative sources in a hyperlinked environment”. *Journal of the ACM*. 46. 604-632.

[44] Raymond Kurzweil. 2000. *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. Penguin. New York. [Main Library 006.3 KUR [http://lib.exeter.ac.uk/record=b1826281~S6]].

[45] George P Landow. 1997. *Hypertext 2.0: The Convergence of Contemporary Critical Theory and Technology*. Johns Hopkins University Press. Baltimore, OH. [Main Library: 1×NL, 2×SL 801.95 LAN].

[46] Lawrence Lessig. 1999. *Code and Other Laws of Cyberspace*. Basic Books. New York. [Law Library KL 156 LES [http://lib.ex.ac.uk/record=b1690793]].

[47] Lawrence Lessig. 2001. *The Future of Ideas: The Fate of the Commons in a Connected World*. Random House. New York. [Law Library KN 277 LES [http://lib.ex.ac.uk/record=b1690751]].

[48] Lawrence Lessig. 2004. *Free Culture: The Nature and Future of Creativity*. Penguin Press. New York.

[49] Peter Ludlow. 1996. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. MIT Press. Cambridge, MA. Preprints also available from: http://www-personal.umich.edu/~ludlow/highnoon.html [Accessed 23 September 2005].

[50] Jean François Lyotard. 1991. *The Inhuman: Reflections on Time*. Blackwell. Oxford. [Main Library 194 LYO [http://lib.exeter.ac.uk/record=b1128547~S6]] .

[51] Hugh Mackay, Wendy Maples, and Paul Reynolds. 2001. *Investigating the Information Society*. Routledge. London.

[52] Marshall McLuhan. 1964. *Understanding Media: The Extensions of Man*. Routledge & Kegan Paul. London.

[53] Stanley Milgram. 1967. “The Small World Problem”. *Psychology Today*. May 1967. 60-67.

[54] Paul Milgrom. 2004. *Putting Auction Theory to Work*. Cambridge University Press. Cambridge. [Main Library 658.84 MIL].

[55] William Mitchell. 1995. *City of Bits: Space, Place and the Infobahn*. MIT Press. Cambridge, MA.

[56] Peter Morville. 2005. *Ambient Findability*. O'Reilly Media. Sebastopol, CA.

[57] Lance Mueller. 2006. “Webjacking, and how to boot it out”. *Network Security*. 2006. 8. 15-18. http://www.sciencedirect.com/science/article/B6VJG-4KWYM39-6/2/4ee40dd84d5755578b06efa99ea32681 . 2008-03-01.

[58] Donald A Norman. 1998. *The Invisible Computer*. MIT Press. Cambridge, MA. [Main Library 001.644 NOR].

[59] James A O'Brien and George M Marakas. 2005. *Management Information Systems*. Seventh. McGraw-Hill. New York. [Main Library: 658.054 OBR/X [http://lib.ex.ac.uk/record=b1774826]].

[60] Andrew Odlyzko. 1997. “The Economics of Electronic Journals”. *First Monday*. 2. 8. http://www.firstmonday.dk/issues/issue2_8/odlyzko/index.html . 2005-10-27.

[61] Adam L Penenberg. 2009. *Viral Loop: The Power of Pass-It-On*. Sceptre. London. [GBS].

[62] Eric S Raymond. 1998. “The Cathedral and the Bazaar”. *First Monday*. 3. 3. http://www.firstmonday.org/issues/issue3_3/raymond/ . 2007-02-09.

[63] Bruce Schneier. 2000. *Secrets and Lies: Digital Security in a Networked World*. John Wiley and Sons. Chichester, UK.

[64] Bruce Schneier. 2003. *Beyond Fear: Thinking Sensibly sbout Security in an Uncertain World*. Copernicus / Springer Verlag. New York.

[65] Rob Shields. 2000. *Hypertext Links: The Ethic of the Index and its Space-Time Effects*. In [101] .

[66] Simon Singh. 1999. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate. London. [Main Library 001.5436 SIN [http://lib.ex.ac.uk/record=b1658453]].

[67] Ken Steiglitz. 2007. *Snipers, Shills & Sharks: eBay and Human Behavior*. Princeton University Press. Princeton, NJ. [CMIT Office].

[68] Bruce Sterling. 1998. *A Good Old-Fashioned Future*. Bantam Books. New York. [Personal copy: GBS] .

[69] Vernor Vinge. 1993. "The Coming Technological Singularity: How to Survive in the Post-Human Era". *Vision-21: Interdisciplinary Science & Engineering in the Era of CyberSpace*. NASA Conference Publication CP-10129. http://rohan.sdsu.edu/faculty/vinge/misc/singularity.html. 2008-01-31.

[70] Margaret Wertheim. 1999. *The Pearly Gates of Cyberspace*. Virago.

[71] Bjorn Westberg. 2002. *Cross-Border Taxation of E-commerce*. International Bureau of Fiscal Documentation. Amsterdam. [Main Library 336.243 WES].

[72] David Whitehouse. 1999. *The WWW is very big but not very wide*. BBC News. http://news.bbc.co.uk/1/hi/sci/tech/443754.stm . 2005-08-16.

Acts of Parliament

[73] *Copyright, Designs and Patents Act*. 1988. c.48. http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm . 2006-02-24.

[74] *Computer Misuse Act*. 1990. c.18. http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm . 2006-02-24.

[75] *Trade Marks Act*. 1994. c.26. http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940026_en_1.htm . 2006-02-24.

[76] *Copyright and Rights in Databases Regulations*. 1997. Statutory Instrument 1997 No. 3032. http://www.opsi.gov.uk/si/si1997/19973032.htm . 2006-02-24.

[77] *Data Protection Act*. 1998. c.29. http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm . 2006-02-24.

[78] *Freedom of Information Act*. 2000. c.36. http://www.opsi.gov.uk/acts/acts2000/20000036.htm . 2006-02-24.

[79] *Regulation of Investigatory Powers Act*. 2000. c.23. http://www.opsi.gov.uk/acts/acts2000/20000023.htm . 2006-02-24.

Glossary of Terms

Content Filter	A piece of network software or hardware that analyses the Internet traffic passing through it, and which rejects or blocks any traffic containing unapproved words, phrases or URLs.
Digital Edition	A digitised copy of a document, book, manuscript or other artifact. Many digital editions are made available for public use, to allow easy access to rare or fragile resources.
eXtensible Markup Language	XML is the successor to SGML, and is the metalanguage of most of the latest generation of markup languages, such as XHTML, DocBook, TEI, etc. It is much stricter than SGML with its syntax, which makes it much easier for computers to read documents created with it. See `http://www.w3.org/XML/`.
FLOSS	“Free/Libre Open Source Software”, or just “Open Source Software” describes a type of software written by individuals or a community that is released for free use and adaptation into the community at large. The 'free' here is more akin to freedom of expression (hence the qualification, 'Libre'), rather than referring necessarily to a lack of financial recompense, though much of FLOSS is distributed free-of-charge too.
Local Mirror	A simple method of restricting access to the Internet, sometimes used by schools, where web pages or sites of interest are copied to a local web server on the school's intranet (local network).
Metalanguage	A language to describe other languages. SGML is the metalanguage that is used to define HTML. Terms such as verb, noun, adjective are all metalanguage terms used to describe English and other human languages.
SGML	Standard Generalized Markup Language
Walled Garden	A method of allowing restricted access to the Internet, often used in schools. The connection to the Internet backbone permits access only to known “safe” or approved sites, by blocking Internet traffic to all other sites.
XHTML	A more modern version of HTML written using XML. See `http://www.w3.org/TR/xhtml1/`.
XML	See eXtensible Markup Language.

Index

S

T

V

W

Colophon

These notes were prepared in DocBook XML, using the <oXygen/> XML editing suite. They were transformed with the DocBook XSL Stylesheets, to XHTML using XSLTProc, and to PDF using Saxon and Fop.