# 1

# INTRODUCTION



**There are two primary reasons why people become computing professionals: interest and money. The lucky ones get paid large amounts of money to do things that they are interested in. What they are interested in, and what they get paid for, is solving problems by writing computer programs or developing hardware devices. When computers were rare and expensive, they had little impact on most people's lives; where they did have an impact (such as in code making and breaking by governments), it was hidden and indirect. From the 1960s to the present, however, computers have followed consistent patterns of becoming exponentially more powerful and linearly cheaper in most terms: processing power, memory storage capacity, network bandwidth and so on. Because of this, and their general versatility, computers have become nearly ubiquitous in the industrialized world. The average household unwittingly contains in excess of ten 'computers' – everything from simple microprocessors performing a very limited range of functions, such as ensuring that the freezer does not defrost and the toaster does not burst into flames, to an Internet-connected PC which may also receive satellite television signals and control household systems, such as heating and cooling. Even embedded computers are becoming more powerful and the next wave of development is**

**expected to be the wireless interconnection of many of these devices with other pieces of equipment inside and outside the home. This is already happening with the ability to remotely program satellite and cable television recorders over the Internet or via a mobile phone** (`www.sky.com/portal/site/skycom/remoterecord/`)**.**

The combination of dependence on the correct functioning of these devices and the potential for abuse and misuse by both their owners and third parties (governments, criminals, pranksters or commercial interests) creates the biggest risks that industrial societies have ever faced. It is suggested that we are now in the midst of a social revolution every bit as far-reaching as the industrial revolution: the 'information revolution' moving us from the industrial age to the information age. It used to be reasonable for computer geeks to ignore the potential real-world effects of their work and leave such concerns to others. However, the ubiquity of computer technology means that computing professionals must now consider their work in the same light as the chemist and the nuclear physicist in terms of its potential impact on individuals and society. This is not just in the interests of society, but in the interests of computing professionals themselves. From supporting and promoting professional attitudes to taking part in political debate, the abdication of responsibility by computer nerds needs to stop. The alternative is abuse and misuse of power by large corporations and governments.

This is not to say that a professional attitude and attention to the social and legal ramifications of computing development is entirely altruistic. Despite the huge growth in computer usage and Internet access seen in the last 10 years, to the point where a majority of the population in industrialized countries will use a computer and access the Internet at least weekly, computers and the Internet remain a mystery to most of those users. Where such mystery holds sway, there is always the potential for social reactions (economic, legal and individual) to produce adverse effects on the lives of computing professionals. An extreme example of public reaction to advancing technology can be seen in the area of genetic modification. This might seem a long way from the world of the computer geek but consider that genome sequencing would not be possible on the scale currently undertaken without the processing capabilities of large computers. Without large-scale genome sequencing, genetic modification would be almost impossible to target efficiently.

The public reaction to genetically modified foodstuffs in Europe is, in the opinion of most scientists, completely uninformed and so biased against the technology that even developments which would solve known problems with pesticide and fertilizer use with apparently minimal other risks are blocked under the reaction to 'frankenfood'. Closer to home, for most computing professionals, is the constant discussion over the availability of sexual material online. Despite being utterly discredited (Time, 24 July 1995), an incredibly flawed study from over 10 years ago (Time, 3 July 1995) which claimed that 83.5% of Internet traffic consisted of pornography is still being quoted as a legitimate source by news organizations and lobby groups. In particular such 'statistics' are bandied about by those who advocate severe censorship and control of Internet access and computer usage, even to the point of suggesting that encryption which does not have a 'back door' for law enforcement should be banned, or that truly general-purpose computers be replaced by consumer electronic devices that limit access to information.

Most university engineering courses now include some element of study into social, legal and ethical aspects of the subject. Unlike much of the curriculum in engineering, however, this topic is not one in which a method of solving problems is transmitted from teacher to student. The aim of such a course is, or at least in our opinion should be, to provide a starting point for students to question the effects of their and their colleagues' work. In this book, we aim to raise many questions and provide information about the known and predicted effects of new technology on society. Where possible, parallels are drawn to previous technological developments, sometimes going back centuries, sometimes only a few years. Sometimes opinions are offered on the desirability or otherwise of these effects. It should be noted that such opinions are not always actually held by the authors but are presented to stimulate debate and deeper thought. In particular, each chapter includes some individual case studies and discussion topics. These discussion topics may be structured as a question for debate with starting points on each side put forward or may offer a completely one-sided presentation of the benefits or detriments of a particular aspect of new technology. Such one-sided arguments often form the core of lobbying or public relations exercises by powerful groups and the ability to tell the argument from the polemic and to pick apart a biased view is important.

All of the topics covered in this book could have (and most have had) one or more books written on them. We recommend some of the best (in our opinion) at the end of each chapter. Identifying the ideal order to present these topics was a difficult task and it was obvious to us that there are many equally valid orders. We have therefore made each chapter as self-contained as possible. This means that there are as many references forward to later chapters as references backwards to previous ones. It also means that some material is repeated where important background issues overlap. Readers should feel free to study the material presented in any order they feel appropriate, possibly skipping some chapters entirely. However, the order makes sense to us and we feel there is a reasonable logical progression from issue to issue and chapter to chapter which allows the book to be read as a whole in the order presented.

Before delving into each of the topics in detail, in this chapter we cover some of the major themes which will emerge again and again under the various headings.

## The Canadian Cyborg

Steve Mann is a professor of engineering at the University of Toronto. He styles himself a 'cyborg' and has been using wearable computers for over twenty years, recording and broadcasting what he sees, accessing computer files and the Internet constantly to 'augment his memory'. Professor Mann is a world-famous researcher in wearable computing. In 2002, he followed his usual routine when flying to St John in New Brunswick, Canada, informing the airline and airport of his equipment and requesting permission not to have his equipment put through the X-ray machine because it is more sensitive than normal machines to their effects. On his way to St John on 16 February, he was allowed to pass through security with the usual scrutiny. On the way back, however, airport security insisted he turn his equipment on and off for them and put it through the scanners. He was then strip searched and claimed that electrodes he wears to monitor his

vital signs were 'ripped from him' during the process. His psychological adjustment to the technology led to him feeling disoriented and requiring a wheelchair for boarding the plane. He also claimed that some of his equipment was significantly damaged and since he did not have funds to immediately replace it, he was feeling significant psychological distress from the 'withdrawal'.

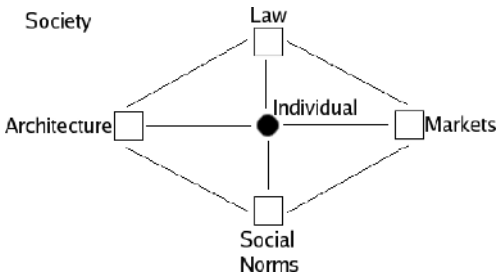
Internet addiction disorder (IAD) is recognized by some psychologists as a psychological condition (though, as with many new conditions, there are significant numbers of psychologists who do not believe in the concept) and there is evidence that regular users may suffer psychological changes when denied access to their mobile (cell) phones. As the number of people constantly used to being in touch with the virtual world increases, the real world is going to have to make adjustments for people with psychological dependencies on their technology. More details on the airport incident can be found at `news.zdnet.com/2100-9584_22-5068619.html` and more general information about Steve Mann at `www.eecg.toronto.edu/~mann` and at `wearcam.org`.

Steve Mann's "wearable computer" and "reality mediator" inventions of the 1970s have evolved into what looks like ordinary eyeglasses.


## LESSIG'S FOUR MODALITIES ANALYSIS

In his seminal 1999 book, Professor Lawrence Lessig described a means of considering how technology and human society interact. In various chapters in our book, this 'four modalities' approach to analysis will be used (sometimes formally, by describing the element of each mode, and sometimes more informally). Lessig's concept is that there are four interconnected influences on human behaviour: law, social norms, markets and architecture. In the physical world, architecture means physics and geography but online architecture is simply computer code. Markets are the economic realities and how they influence behaviour. Social norms are the pressures put on us by people we know and law is the expressed and enforced

power of the state. Each of these interacts with the others and puts pressure on the individual. Each is also acted on by society as a whole. None are completely fixed or completely understood and the interactions are sometimes subtle and sometimes gross.




## PROPHET AND LOSS: FAILING TO FORESEE THE FUTURE

Intelligent, well-educated experts in science and technology have been making far-reaching pronouncements about the future for centuries. Some of the biggest howlers of failed predictions include:

*'The abdomen, the chest and the brain will forever be shut from the intrusion of the wise and humane surgeon' – Sir John Eric Ericksen, British surgeon to Queen Victoria, 1873*

*'This telephone has too many shortcomings to be considered as a means of communication. The device is inherently of no value to us' – Western Union internal memo, 1876*

*'Radio has no future. Heavier-than-air flying machines are impossible. X-rays will prove to be a hoax' – Lord Kelvin, physicist and inventor, 1899*

*'The problem with television is that the people must sit and keep their eyes glued on a screen; the average American family hasn't time for it' – New York Times, 1949*

*'Man will never reach the moon, regardless of all future scientific advances' – Lee De Forest, radio pioneer, 1957*

*'There is no reason anyone would want a computer in their home' – Ken Olson, president, chairman and founder of DEC, 1977*

*'640 kB ought to be enough for anybody' – Bill Gates, 1981*

*'I predict the Internet will go spectacularly supernova and in 1996 catastrophically collapse' – Bob Metcalf, 3Com Founder, 1995*

The closest to reality any of these came is Bob Metcalf whose prediction of catastrophic failure applied, but only to the 'dot com' investment bubble, not to the technology or the spread of its usage to almost every home and workplace and even to public toilets! So, when considering the future it is often 'better to keep silent and be thought a fool than speak and confirm the opinion'. Which technologies will become widespread and last and which will die as they are born or flash like a nova is difficult to predict. What is becoming ever more certain is that technology will continue to evolve although we may be reaching the limits of society to adapt to new technology quickly enough for it to be economically viable. Already it can be seen that sufficient technology with wide acceptance can become highly entrenched and outlast several generations of possible replacement purely by commercial inertia (consider the humble audio compact disc, now beginning to show its age but remaining a significant medium for purchase of music 20 years after its introduction, and the audio cassette tape still with its niche markets more than 40 years on). Entirely new technologies are not the only force at work. At least as strong is the combination of new technologies with old (see Chapter 2 for more on this), such as telephony over an Internet connection (voice over Internet protocol) or video on demand delivered to third-generation mobile phones.

## INFORMATION SYSTEM PARTITION

In what is now regarded as a classic exposition of the influence of technology on society Meyrowitz (1985) in No Sense of Place argues that television produced seismic upheaval in the social order by giving people access to hitherto restricted

information systems: children access to the adult information world, women access to the male information world, ethnic minorities access to the majority's information world and the poor access to the information world of the rich. There are those who have regarded this with horror, such as campaigners insisting that all television broadcast be suitable for young children (i.e. no sex, no violence, no swearing, no moral shades of grey, etc.). There are also those who have objected to the broadcasting of the truth about them or their organizations.

The debate about censorship of information available on the Internet is simply an expansion and intensification of this earlier debate, made more complex by the open and many-to-many nature of Internet protocols. Broadcast television is becoming easier to regulate and more regulated in some ways (e.g. subchannel 'ratings' information allows parents to restrict what their children have access to on the family satellite or cable receivers) and yet less regulated and less easy to regulate in others (hundreds of channels, many of them sourced directly from other countries, and much more extreme adult material being broadcast which was before only allowed distribution in the physical form of videocassettes and DVDs). At the same time, more and more material, including full video feeds, is becoming available over the Internet with much less possibility for restriction by either regulators or parents (see Chapter 4 for more details).

Consider the difference in reporting of the First World War (strong censorship, 'patriotic movies', newsreel cinema footage months old) and the Iraq War (reporters embedded with the attacking troops and in a hotel inside the capital), or the famous sequence of BBC reporter John Simpson 'liberating' Kabul ahead of US and UK troops. The failed coup against Mikhail Gorbachev which brought down the Soviet Union followed the standard pattern of previous power shifts in the Kremlin. Unfortunately for the plotters, Gorbachev's reforms had already lost them control of the information system inhabited by the ordinary people of Moscow. During previous coups, the control of information allowed the assumption of power by plotters before anyone who had the possibility to oppose them could rally support. This time, access to the dissemination of information nationally and internationally allowed Boris Yeltsin to rally support for resistance. It is no coincidence that the most physically and politically oppressive regimes in the world also tend to have

some of the most restrictive information systems in place. It is often said that 'you don't miss what you've never had' but it is even more true that 'you don't miss what you don't know exists'.

## THE LAW IS AN ASS

When first encountering law, it often seems bewildering with its own strange nomenclature and ways of using five words where it appears that one would do. As it is studied, however, it begins to make sense and a scientist will begin to see the logic involved. This is the most dangerous stage because as one studies in more depth one realizes that law is not truly logical, and that to assume it is can produce grave errors in interpretation. Each piece of law, whether it is a statute, a judicial precedent or an international treaty, is developed somewhat in isolation from other elements of the law. While attempts are always made to ensure that laws do not contradict each other, the existing body of law is too large to avoid such problems. Legislation is the result of individual opinions of existing law, the ideal state of society and the pragmatic view of what might work.

Increasingly, law is both affected by and affects technology, and computer technology particularly. While engineers should not be expected to be lawyers, they do need a basic understanding of the law as it affects them for two reasons: firstly, to know when they (or their organization) need the advice of expensive lawyers; secondly, in order to engage in the political debates that develop the law. The first of these is fairly obvious – why pay for expensive legal advice when the situation is clear cut even to a layman? On the other hand, many computing professionals would question why they should bother with the illogical and messy business of political debate. After all they are interested in the clean joys of hacking elegant code rather than the messy world of the politician. When computers were confined to hobbyists and large corporations' internal data processing, that may have been possible. Now, however, with laws that allow patenting of software ideas (in the United States and maybe soon the European Union), laws that restrict the distribution of computer code (anything from encryption algorithms to device drivers) and laws that decide who has the rights to use particular words in a URL (so far only in second- and

third-level domain names but possibly soon referring to the whole of the URL), the everyday interests of the computer literate are subject to more and more regulation. If that regulation was sane, reasonable, unbiased and developed in such a way as to not unduly hamper the development of new technology, it could be left to the politicians and judges to get on with. Unfortunately this is not the case. Far too few politicians and judges have more than a very basic understanding of the strengths and limitations of science in general, much less information and computation theories and practicalities. Such misunderstandings can be seen in the issued statements of both judges and politicians, for example the necessity of describing the Internet as 'not something you just dump something on. It's not a truck. It's a series of tubes' (`www.pcmag.com/article2/0,1895,1985071,00.asp`).

Politicians do not seem to understand that the immense economic potential of the Internet and the Web rests primarily upon its open, end-to-end nature. When judges in France decide that it is the responsibility of US companies to prevent French citizens from accessing the data on their US servers in order to comply with French censorship laws on Nazi issues, they are demonstrating an utter lack of understanding of the international nature of the Web and the Internet. Since politicians and judges do not understand the nature of the technology, they listen to vocal demands for a variety of restrictions on technological development and they pass laws which may or may not have the desired effect but which often place terrible burdens on both the work and personal computer usage of computing professionals. In order to prevent unreasonable burdens, those who understand the technology must become sufficiently politically involved to at least reduce, if not eliminate, the negative impact on their lives. In order to suitably influence the political and judicial arenas, however, one needs a basic understanding of the existing legal situation, and particularly of the law relating to technology.

While all the topics in this book have some relevant legal content there are some which are almost entirely legal in nature, such as copyrights and patents, privacy and surveillance, and censorship and freedom of speech. The law is complex and the law is an ass, but so long as that is kept in mind it can be understood to the extent needed.

### Tati vs Kitetoa

A French journalist, Antoine Champagne, ran a website called `kitetoa.com`. On this website, Champagne and some friends publicized their 'White Hat cracking' exercises. Generally, they did this some time after having contacted companies with holes in their systems and, in many cases, having helped the companies plug those holes. When they posted data retrieved from the companies' intranets, they sanitized it to avoid data protection violations, trade secret disclosures and similar issues.

Lawyers for Tati (a French clothiers) alleged that Champagne 'cracked' their computer network and fraudulently accessed Microsoft Access databases on their system between 1999 and 2001. Champagne states that he merely used open proxies on their system to access documents freely available on the system.

As proof of no harm, Champagne produced e-mail exchanges with Tati.fr's systems administrators thanking him for notifying them and for his help in plugging their security holes. The prosecutor in France slapped Champagne with a €1000 fine suspended pending 5 years free of conviction for similar offences under France's computer misuse laws.

Champagne has been threatened by French police with confiscation of his computers if he runs foul of such laws again. `www.kitetoa.com` is still up and running at the time of writing and all the details are available there (in French) but details of new vulnerabilities are no longer posted.

## GLOBALIZATION

One of the significant impacts of modern computer and communication technology is that the barriers between societies are being reduced. Sometimes that reduces tensions and produces a lessening of suffering: it is more difficult to ignore starving people in a famine thousands of miles away when their faces and pleas for help

appear on television screens in our living rooms. At other times it can increase tensions and even lead to armed conflict: nations separated by thousands of miles may have no conflict despite fundamental ideological divisions, but when the borderless flow of information spreads (sometimes misunderstood) ideas from one place to another it can lead to conflict. One example of this was the violent protests in 2006 in nations as far away as Indonesia against publication in 2005 in a Danish newspaper of cartoons satirizing the prophet Muhammad.

The Internet in particular is accelerating this globalization of information. The many-to-many nature of Internet communication prevents governments from keeping any significant control of information arriving from elsewhere in the world. From radical sermons by religious fanatics to Western ideas of democracy and freedom of speech and thought, each individual can now follow an information path they choose, away from the control of national and local leaders. The problems of jurisdiction and the increased clash of cultures created by global communications systems are a recurring theme in many of our chapters.

## THE DIGITAL DIVIDE

The world has long been divided into rich and poor, educated and ignorant, free and controlled. There are equivalent divides on national and international levels. The spread of computer and communication technology has changed the nature of these divides in unexpected ways. In many cases, of course, it has simply widened the divide: the children of the rich have access to the latest top-quality equipment and sources of information, allowing them to maintain their position relative to the uninformed poor. This has always been the case to some extent, in that children from poor homes could not afford encyclopedias and other textbooks or the fees of top-quality private schools. As the cost of computers and Internet access has reduced, access to an equivalent level of information has penetrated lower and lower on the economic scale, but there remains a significant underclass in industrialized society without access to, or knowledge of how to use, such trappings of modern life.

The double-edged nature of the information revolution is also noticeable on a global scale, with the development of outsourcing of computer programming, drug manufacture (and even research and development) and information-centric jobs such as enquiry call centres to countries such as India. Of course, this is leading to the rapid development of a digital divide in those countries even worse than that seen in the industrialized world. The instantaneous communications offered by world-wide telephone and computer networks have merged the stock markets and money markets into a nearly continuously traded global whole. No longer does the market stop when the trader leaves the office: it continues trading around the world and, by the time they start work again the following morning, seismic shifts in fortunes may have occurred. Computer-based trading has allowed the development of automated trading systems which track the stock market as a whole or individual stock prices and perform trades dependent on conditions set by a broker. In some cases, the combination of unusual events (such as major security alerts, major industrial accidents or currency value collapses) and automated trading can lead to a spiralling or oscillating sequence of market trades. Deliberate delays in processing trades or decision making have had to be introduced to avoid too much volatility in the markets.

## Individual Stock Market Trading: Pump and Dump Scams

Individual access to computer and telephone communications can also have a significant impact on stocks and shares, the basis of the capitalist economic system. Pump-and-dump scams have been around as long as the stock market: the price of a stock is 'pumped up' by spreading rumours that there is some reason it is about to jump (a new contract, a new product distribution approval or a takeover bid). Once enough people have bought in, driving the price up (the pump), the original holders of the stock sell at a vastly inflated price (the dump), leaving those who fell for the rumour to take the losses as the stock adjusts

back to its natural price. This shows all the classic aspects of traditional confidence tricks: rely on people's greed, have them do something slightly suspect or even downright illegal (trading on 'inside information' is illegal on most stock markets) and then sting them for their money. The slightly illegal nature of the victims' own activities reduce the chances of complaints to law enforcement agencies. New variations on the pump-and-dump scam involve using usenet, email or other online communications tools to spread the pump information. In another recent variation, voicemail messages are left on mobile phones as though to a wrong number (quite plausible since many mobile-phone voicemail services do not include a personalized message, even where the facility is present). The US Security and Exchange Commission (SEC) prosecuted Michael O'Grady of Georgia in May 2005 (O'Grady pleaded guilty: `www.usatoday.com/money/industries/telecom/2005-05-03-voicemail_x.htm`) and has previously prosecuted email and usenet pump-and-dump scammers. As both information and trading move faster and faster, wild surges in stock market prices are becoming more and more common, which can destabilize the entire world economy.

Developing nations are attempting to leapfrog into the information age without passing through an industrial age, just as Japan leapfrogged the early industrial technologies into the electronics era after the Second World War. Whether they will succeed is impossible to judge but outsourcing of everything from call centres to accounting shows the potential.

## SERVANT OR MASTER: COMPUTERS MAKING DECISIONS

Some of the most difficult issues in computing today arise when computer software and hardware is responsible for making decisions which affect people's lives.

We have briefly covered above the problems that may be caused by automated stock-market-trading systems. When these activities cause problems they can result in significant financial loss and possibly even have macro-economic effects in fragile situations. However, even more serious are those circumstances in which lives, not money, are at stake.

From computer control systems in cars, planes and boats to automated dosing machines in hospitals, computers are constantly involved in potentially life-threatening activities in the modern world. Where the decision made by a computer program leads to financial loss or to injury or death, who should be held responsible?

There is a significant level of response to negative incidents in which people 'blame the computer'. When the negative incident is that one's tax bill is out by a few pounds or dollars, this may be an acceptable and humorous way of defusing a sensitive topic or it may enrage the subject of the error. When the result of a computer error is to release dangerous (even fatal) dosages of radiation during radiotherapy for cancer, as happened in 1986 in Georgia (New York Times, via `tinyurl.com/3dkj5c`) the question of who, if anyone, is to blame becomes much more serious. When a medical practitioner makes a mistake and gives a patient a damaging dose of a treatment, an investigation will be carried out by the appropriate regulatory body to determine whether that practitioner is allowed to continue practicing and out of court settlements, or court cases, assign damages usually paid by insurance companies. When computer software is found to have failed, who is responsible?

Software engineering is a difficult task and errors may occur due to any number of causes: requirements may have been incorrectly transmitted to the software team by the customer; errors in the hardware may cause errors in operation; errors in software libraries or compilers may cause errors in the final object code; errors in programming, testing or installation may cause faults; carelessness or negligence may be the root cause, or the problem may be the result of previously unknown interactions within the complex computer system. Assigning blame, preventing future occurrences and developing better software are all necessary steps when someone has been injured or killed (or where such injury or death was avoided only by luck or human intervention). Computer systems are so complex, however,

that it is often claimed that perfect software is impossible to produce. How much liability do individuals in software houses have for the results of their work? If their work is then used to produce safety critical software when they did not originally expect it to be so used, do they still remain liable for the consequences?

As more artificial intelligence software is developed and the possibility of self-awareness of computer software becomes apparent, what are the limits of responsibility of the programmers for the actions of their work? If the programmers are not liable then who, if anyone, is?

# DISCUSSION TOPICS

## Can Laws Be Immoral?

The apparatus of the state decides what is legal and not legal. In the industrialized world, it is claimed that the rights of minorities are protected but within living memory it was illegal to be a homosexual in the United Kingdom. Under the Nazi regime, it was not only legal, it was required, that Jews, gypsies and others were put into concentration camps to be killed or allowed to die. In the People's Republic of China, it is illegal to post discussions of freedom of speech or free and fair elections onto the Internet. In many states in the United States, it is legal to have sex with someone aged 16 but not to take nude pictures of them. In the democracies of the industrialized world, it is generally not illegal to campaign for a change in the law to decriminalize something (e.g. various narcotics and other recreational pharmaceuticals). Other countries regard things differently. Sometimes only those in the legislature have freedom to discuss changes in the law. If one believes a law is immoral, is it moral to break that law? It is sometimes said that 'the only crime is getting caught'.

## Genetically Modified Food, Technologically Modified Humans

The idea of a soul-less humanoid machine has been around since biblical times (Psalms 139:15–16). Science fiction has been dealing with the concept since Mary

Shelley's Frankenstein. We have Professor Steve Mann constantly connected to his computers and the Internet; we have people with implanted technology keeping them alive (pacemakers and even completely artificial hearts); and we have almost humanoid robots.

The public furore over genetically modified food (so-called 'frankenfoods') shows how poorly the public sometimes understand scientific advances and risks. Debates over choosing the sex of which embryos produced in vitro are implanted have raged amid speculation about 'designer babies' selected for hair and eye colour, intelligence or sporting ability, while selecting out certain serious genetic defects has become almost routine. Terry Schiavo became known throughout the United States and the world after (arguably) entering a persistent vegetative state; she was the centre of a political and judicial struggle still being played out long after she was allowed to die.

People have been attacked by mobs simply for being thought to be carrying one of the 'new plagues' (AIDS, for instance). Will we see persecution of those with pacemakers or artificial hearts or those whose gestation was decided by genetic selection, for being 'different', not human? Those who differ from the ordinary person can feel isolated and shut out of normal life because they look different. Will people have to hide their augmentations or will society accept technologically modified humans more easily than genetically modified food?

## The Haves and the Have-nots

Large parts of Africa, Asia and South America still have not emerged properly into the industrial revolution. Agrarian societies subject to drought and famine when the harvest fails are a world away from the epidemic of obesity in the industrialized societies. The industrialized world is now undergoing an information revolution. Just as large parts of the world have already been left behind, portions of the population in the industrialized world are being left behind in the information revolution. Illiteracy often dooms people to low-paid work and exclusion from many aspects of social interaction. Computer literacy is becoming a similar skill.

Governments and commercial entities are moving as much of their interactions with individuals as they can onto computer systems, supposedly to achieve cost savings (though these are not always evident). Once it becomes uneconomic to support both physical and virtual shop fronts, many retailers may move solely to electronic transactions. Choice for those outside the Internet loop may significantly diminish. Just as those without cars are disadvantaged by the change to edge-of-town supermarkets whose cheaper prices through economies of scale are more than outweighed by the cost of bus or taxi fares to those without personal transport, so those without Internet access may be forced to pay higher prices or do without certain goods altogether. Public libraries may continue to provide free access to information in both paper and electronic forms but, as the Internet becomes 'the world's library', those without the skills to make use of it may find themselves increasingly out of touch.

Various solutions to these problems have been suggested, from the $200 computer for the developing world to limited Web access via a (television) set top box. Whether a digital underclass will emerge is yet to be seen, but it is already a political issue in many countries where the availability of broadband Internet for all is becoming a government policy even when half their population have yet to make use of even narrowband Internet access.

## REFERENCES

**Meyrowitz, J.** (1985) *No Sense of Place*, Oxford University Press, Oxford. ISBN 0-19-504231-X.

## RELATED READING

**Akdeniz, Y.** (1999) *Sex on the Net*, South Street Press, Reading. ISBN 1-902932-00-5.

**Furnell, S.** (2002) *Cybercrime: Vandalizing the Information Society*, Addison Wesley, Harlow. ISBN 0-201-72159-7.

**Goodman, D.** (2004) *Spam Wars: Our Last Best Chance to Defeat Spammers, Scammers and Hackers*, Select Books, New York. ISBN 1-59-079063-4.

**Hafner, K.** and **Lyon, M.** (1996) *Where Wizards Stay Up Late*, Free Press, London. ISBN 0-7434-6837-6.

**Lessig, L.** (1999) *Code and Other Laws of Cyberspace*, Basic Books, New York. ISBN 0-465-03913-8.

**Lessig, L.** (2001) *The Future of Ideas*, Random House, New York. ISBN 0-375-50578-4.

**Lessig, L.** (2004) *Free Culture*, Penguin, London. ISBN 1-594-20006-8.

**Levy, S.** (1994) *Hackers: Heroes of the computer revolution*, Penguin, London. ISBN 0-14-100051-1.

**Levy, S.** (2000) *Crypto: Secrecy and Privacy in the New Code War*, Penguin, London. ISBN 0-140-244-328.

**Mueller, M.L.** (2002) *Ruling the Root*, MIT Press, Cambridge, MA. ISBN 0-262-13412-8.