Understanding Digital Culture
NEW PRODUCT for 2009!  
Remote Monitoring Software for Mac OS X!

Monitor the online activity of your children or employees from anywhere: at work, in another room, at an internet kiosk, on vacation, on a business trip – even if you're thousands of miles away.

Automatically records every web site they visit, every keystroke they type, and every program they launch, plus sends copies of chats, instant messages and emails sent and received.

eBlaster recordings are organized into an easy-to-read Activity Report that is automatically sent to any email address you choose ... as often as you like. eBlaster Activity Reports can be sent to another computer in your home, your office email address or any web-based email service like Google Gmail, Yahoo mail and others.

See inappropriate messages from strangers to your children or between employees right away! eBlaster Instant Notification keeps you 'in-the-know' by automatically sending you an exact copy of their emails, chats and instant messages as they occur.


The above advertisement for ‘eBlaster’ surveillance software in many respects epitomises one of the most important public issues related to the information age: the increased ability to gather data about others which, up until recently, would have been considered impossible and/or immoral. Thoughtful consideration of the above passage suggests this is a much more complex issue than it first appears. At first it seems repugnant ... spying on the personal communications of one’s children and one’s employees ... monitoring their every virtual manoeuvre ... but upon second glance, it is easy to see the rationale behind such activity: the protection of one’s children and the legitimate concern that employees do not misuse company equipment and instead
get on with the activities they are paid to undertake. Who would argue with either of those two goals?

In previous times people, to a certain extent, would have had to trust their children not to behave inappropriately or endanger themselves, and employers would have to trust their employees to do their jobs and not take undue advantage of company property. Most of the time such trust was (and still is) well-placed, but not always. It is clear that the notion of trust involves a certain amount of risk for the person or organisation doing the trusting.

This applies to the larger contexts of nations and governments as well. Few would disagree that most advanced economic states are increasingly becoming surveillance societies. Perhaps at the more extreme end of this trend is the United Kingdom. Living through decades of terrorist threats and attacks from the IRA in the 1970s and 1980s, only to once again be put into a climate of fear during the post 9/11 ‘war on terror’ and the target of yet further attacks, the UK has become one of the most surveilled societies in the world, with London at the epicentre of this trend. A typical London resident can now expect to be photographed 300 times a day by CCTV cameras, have their cars tracked through number plate recognition systems, their city movements tracked through the use of public transport (Oyster) cards, and potentially even their pedestrian movements located through the triangulation of their mobile phone signals (BBC, 2006). While on the extreme end, the case of the UK and London is not unique, as most countries have stepped up their surveillance procedures in the wake of the 9/11 attacks in order to minimise the risk posed by international terrorism.

Such scenarios of widespread CCTV and government surveillance conjure up fears of a ‘big brother’ society in which governments and law enforcement agencies amass huge amounts of data on individuals and continually monitor the movements of their citizens. This was the modus operandi of Fascist and Stalinist regimes of the recent past, and these are quite rightly legitimate concerns over which to be vigilant. However, this chapter will demonstrate that data collection and surveillance by governments is only one part of the overall picture of surveillance in the digital age. The opening passage suggests that surveillance and risk reduction is not only the occupation of governments looking to curb internal and external threats, but also individuals who want to protect their children, monitor their spouses, or invade others’ privacy for personal gain, and businesses who want greater control over their employees, as well as gain insights into their customers.

This chapter will investigate the status of privacy and surveillance in the information age. It will start with a consideration of the changing nature of ‘privacy’ within Western culture and how current security and commercial concerns may be leading to further changes in our expectations of privacy. Then the context and amount of surveillance currently taking place in digital environments will be considered, followed by a discussion of the motivations behind the increases in surveillance currently taking place, with a particular emphasis on the political-economic dimension of surveillance strategies. The last section of the chapter will consider the potentially negative consequences of ubiquitous digital surveillance.
THE CHANGING CULTURAL CONTEXTS OF PRIVACY

The concept of privacy is complicated and hard to define. Much like the ideas of 'community' or 'identity' also discussed in this book, 'privacy' is generally considered to be an important part of life and yet its meaning is varied and contested. Spinello (2003) suggests that in general there are three elements to the notion of privacy: solitude, secrecy and anonymity.

Often, popular understandings of privacy are related to the concept of solitude: the ability to feel alone, isolated or cut-off from others, or colloquially, to be 'alone with one's thoughts'. Perri (1988) argues that this notion has its Western cultural roots in the idea of 'interiority' or the 'examined', 'contemplative' life as first articulated by the ancient Greeks, then rediscovered during the Enlightenment period. Those involved in the Romantic Movement in the eighteenth and nineteenth centuries later related this notion of interiority with the concept of 'solitude'. In solitude, away from others, one could find one's 'authentic' self by escaping from the self of sociability: an inauthentic self tainted by social interactions with others. In Western culture today, part of the idea of privacy and the demand for private space derives from this romantic notion of only being able to be oneself, by oneself.

The second major element in the cultural construction of privacy revolves around the concept of secrecy, as in being able to limit or have control over the amount of information others can know about oneself or 'The claim of individuals, groups or institutions to determine for themselves when, how and to what extent, information about them is communicated to others' (Perri, 1998 quoted in McGrath, 2004). This engages with the perceived right in Western culture to 'one's own business'. In personal matters that have no palpable effect on the rights of others, people are seen to have the right to a certain degree of autonomy over one's public face: the image one presents to the rest of the world. Thus, it is up to the individual to choose what information about one and one's life is available, and to whom.

Last, privacy has an element of anonymity. This can be seen as a peculiarly modern element of privacy. People are seen to be deserving of the right of protection from unwanted attention and scrutiny, or the right to simply be 'a face in the crowd' and go about one's business unhindered by the surveillance or attention of others.

It is important to remember that privacy is a concept with a culturally and historically contingent meaning. Western conceptions of privacy differ greatly from culture in other parts of the world. This is obviously the case as compared to tribal or Aboriginal cultures, but is also true of modern industrialised societies such as Japan (see Nakada and Tamura, 2005). Even within Western culture the importance of privacy has changed over time. In medieval times and up until industrialisation, the interdependency and small social scale of rural and village life, and the small family dwellings, provided very little in the way of what we now call privacy (and almost no anonymity). Contemporary conceptions of private life and personal space simply did not exist.
It was largely in the Victorian era and the period of industrial urbanisation during the late 1800s in which modern notions and expectations of privacy developed. The industrial period created a burgeoning middle class that had greater standards of material wealth, allowing for the creation of larger, multi-roomed houses. The capitalist economic structure of paid salaried work in factories and other forms of mass production developed at the time allowed for a complete separation of home and work life, where ‘home’ became associated with the private sphere and work with public life. Lyon (2001) argues that the modern division of public and private life emerged in this period. These new urban industrial landscapes, organised around the physical separation of home and work, combined to create rigid distinctions of public and private life articulated in the urban landscape through the creation of suburban areas of ‘private’ dwelling and central areas of ‘public’ work and leisure reproduced in the public and private areas of middle-class housing.

Thus, everyday life was divided by the public sphere of work and sociable leisure, and a home or family life which was seen as a secluded retreat from public life. The home was (and still is) seen as the bastion of privacy and private life. But the advent of mass media in the latter half of the twentieth century began to complicate these notions of private and public life. The mass media created public figures and celebrities to a degree previously unknown. For these public personalities, the idea of privacy (especially in terms of ‘anonymity’) started to erode as it began to be considered reasonable to invade the privacy of figures on the basis that the lives of such figures were of public interest. The rise of media celebrity in the twentieth century has helped to change our idea of privacy and the right to a private life.

Perri (1998) suggests that in the data-driven networked society, the cultural construction of privacy will once again change. In the face of a culture in which the spaces in our lives that are not surveilled are increasingly few and far between, ‘solitude’ and ‘anonymity’ will feature less prominently as a right, and the primary concern for privacy will shift emphasis towards the notion of confidentiality, particularly the confidentiality of (inevitably collected) personal information about individuals, and what can be done with that information (Perri, 1998; McGrath, 2004). This shift is likely to be driven by two cultural imperatives currently contributing towards the cultural and legal construction of privacy and the right to a private life: ‘security’ and ‘commercial enterprise’.

Privacy as a legal construction: a contradiction?

Mills (2008) suggests that there are four broad categories of privacy related to different spheres of legal rights:

1. Freedom of personal autonomy, the most obvious being freedom of choice.
2. The right to control personal information, which relates to defamation, or the right not to have one’s personal information disclosed to the public.
3 The right to control personal property, including one’s name and likeness, as well as information about oneself.

4 The right to control and protect personal physical space, which suggests a freedom from unwarranted intrusion, surveillance and intimidation.

These rights are set in balance against societal demands for a certain amount of social control, security and conformity. The right to personal autonomy, for example, is not an unlimited right to do whatever one wants. It is clear that states have legal course to invade privacy in certain circumstances, especially when there is considered to be a threat to life or to state security. Today’s political climate has seen a shift away from an emphasis on privacy and towards ‘security’. The right to control personal physical space and the right to control many aspects of personal information and personal property (especially biological codes used in identification such as DNA and retinal scans) has taken a back seat to worries about crime and terrorism.

Passed in the wake of the September 11, 2001 attacks, the USA-PATRIOT Act was a landmark foray into increasing surveillance of populations. In particular, the Act expanded the ability of government agencies to use traditional forms of surveillance, as well as newer forms of digital communications and activity monitoring without needing to obtain search warrants and court orders. As a result, authorities in the US are now able to obtain a variety of information on individuals by, for example, conducting roving wiretapping on mobile and landline phones, monitoring the reading habits of users of public libraries, and obtaining information from private companies about customer web surfing habits and individual consumer profiles (Taylor et al., 2006).

In Europe, where there has been traditionally much more concern with enshrining and protecting rights to privacy legally (there is no legal ‘right’ to privacy in the US), most countries have devised their own legislation in response to terrorist attacks, which tend to follow the USA PATRIOT Act in the expansion of the surveillance powers of government, but to lesser extremes. These tend to focus on increased communications surveillance, increased identity requirements (especially for immigrants) and increased CCTV surveillance.

At the same time as the context of terrorism and crime have encouraged more data collection on the part of governments, the other impetus for the increasing collection of data has been the economic value of information about individuals. Trading in personal information databases has become big business and an ever more important part of the marketing and advertising of goods. This has spurred on a need for more privacy-enabling legislation to help prevent the widespread misuse of personal information by private organisations.

In terms of privacy-enabling legislation, the United States has tended to have a very fragmented approach to legislating the activities of private organisations. Overall, American legislation tends to concentrate on forbidding certain specific actions of intrusion and eavesdropping on communications, and has very little regulation over the distribution of processing of personal data (Van Dijk, 2006). Many loopholes exist with regard to the restriction of use of personal data in US contexts and this is largely due to the
conflict between the demands of privacy legislation, and strong protection of freedom of speech within the American legal system (Mills, 2008). The selling of or distribution of personal information can be considered a form of commercial free speech, therefore American legislators are less likely to apply stringent laws that limit such actions.

By contrast, the European Union has tended to have a much more coherent approach, with much more emphasis on privacy protection and less on free speech. The EU directive on personal data protection is the most stringent in the world in terms of limiting the collection and distribution of information about individuals. In particular, Van Dijk (2006: 151–152) suggest that the directive:

- Is extremely broad in its definition of ‘personal data’.
- Stresses the collection of data necessary only for specific or legitimate purposes, and that such data can only be collected and distributed with the express consent of the individual.
- Provides a list of categories of personal data that cannot be processed at all, including racial or ethnic origin, religious beliefs, political opinions, union memberships, health status or sexual behaviour.

Van Dijk argues that these benefits do not suggest that this legislation is ideal, but it does mean that, at present, Europe is at the leading edge in terms of privacy-enabling legislation. At the same time (as will be seen below) the European Union is somewhat contradictory in its ambitions to both enhance privacy legislation for personal data collected by private enterprise, while at the same time increasing the data retention requirements placed on private communications firms.

**DIGITAL SURVEILLANCE: SPACES, TRACES AND TOOLS**

David Lyon (2001) argued that there has been a change in the nature of surveillance as human interactions at long distances have become more common. In pre-modern contexts, relationships were primarily based on face-to-face interactions, in which both actors were co-present in the same space and time. However, as Giddens (1991) suggested in his concept of *time-space distanciation*, as modernity and capitalism progressed, human relationships (especially within economic spheres) were extended across longer distances of space and yet still had to be coordinated in time. The availability of long distance telecommunications and the general physical mobility of individuals in late modernity has only amplified this process, to the point where *telepresence* has begun to replace *co-presence* in human interactions.

This move from co-presence to telepresence has meant that surveillance has come to rely less on a watching, witnessing or policing of physical bodies based on physical proximity (embodied surveillance) towards the surveillance of what Lyon refers to as...
'personal traces', or the metaphorical footsteps that people leave behind in the course of their activities. Within contemporary law enforcement this can be seen in the increasing use of CCTV cameras, as well as forensic – and particularly DNA – evidence. Within online contexts, this refers to the traces of internet activity left behind by an individual. Such online surveillance shows an increased concern for where people have been and what they have done and less concern with observations of current activities and the notion of catching someone ‘in the act’, as with embodied surveillance. How this is accomplished is considered below.

Key tools of digital surveillance

Within the online sphere of digital communications there are many tools that allow organisations and individuals to track, trace and monitor the actions of others. These tools run parallel to the well-known offline instruments of biometrics, RFID, CCTV, credit card transaction data, public record keeping and registers, loyalty shopping card schemes, public transportation travel cards and number plate recognition systems. The digital age has provided states, organisations and individuals with a number of new opportunities for the surveillance of populations.

State surveillance tools

In terms of direct state surveillance, one of the most powerful, although nebulous resources is a system called Echelon. Echelon is a secret data collection system run jointly by the governments of the United States, United Kingdom, Canada, Australia and New Zealand. Being a classified security system, details of how it operates are vague, but Echelon is said to screen all international communications (including phone and internet) for intelligence by sifting through communication texts for phrases, keywords and phone numbers that are deemed relevant for security purposes. In addition to Echelon, the United States also employs Carnivore, a kind of internet ‘wiretap’ system used by the FBI to monitor all incoming data into a particular IP address. To implement the use of Carnivore on US citizens, the FBI must justify its use to obtain a court order (see Marlin-Bennett, 2004).

Some countries are now using the internationally networked architecture of the internet to claim a right to surveil communications data that not only originates or terminates within their borders, but also information that passes through their infrastructure on the way to another country. In 2008 the US government passed the Foreign Intelligence Surveillance Act, which states that all internet communications going through the United States are now subject to government surveillance through various methods of ‘wireless wiretapping’. Similarly, Sweden, an important northern European regional hub for internet traffic, passed the New Signal Surveillance Act in 2008, which permits Sweden’s National Defence to access all internet and telephone conversations in and out of (and through) Sweden. This involves a large number of communications, which originate in Norway, Finland, Denmark and Russia (Irion, 2009).
At the same time, and in lieu of direct state surveillance, many governments are passing data retention legislation, which compels private telecommunications and internet companies to keep a record of all communications on their system for long periods of time, so that data can be accessed and used by governments in criminal and security investigations. For example, in 2006, the European Union passed the Data Retention Directive. This law was designed to assist in the coordination of criminal investigations within the EU. It demands that all providers of electronic communications services (such as mobile phone and internet service providers) must retain identifiable phone call and email data for at least six months and up to two years after the communication is made (the duration varies between countries). This data includes at minimum the originator and receiver of the communication, as well as the date, location and duration of the communication (Bigami, 2007). Many other countries have similar laws. In Russia, data must be kept for three years. However, in Australia there are no data retention requirements at present. In the United States, lax privacy laws has meant that most communications companies already retain customer communications data to use for marketing purposes (see below), but in 2009 legislation was put forward by the US Congress to ensure that this is the case. In its present form, this legislation would demand communications companies retain communications for a minimum of two years.

Commercial and private digital surveillance tools

One of the most popular forms of surveillance by commercial enterprises, and by now a fundamental part of web surfing, are internet or HTTP ‘cookies’. A cookie is a small piece of text that is automatically downloaded onto a computer when its browser visits a web page. It then records one’s internet activity and sends this information back to its home web site. The role of cookies is to provide authentication of a user and coherence within a browsing or surfing session. Cookies are fundamental to the interactive and personalised experience of the web as they record user preferences as well as web surfing activity. Web browsers normally have the facility to disable cookies to preserve privacy, but disabling cookies makes many web sites (especially those with a login or some sort of personalisation, such as MyAmazon or eBay) impossible to use.

In addition, free internet services such as search engines and email are used to collect data. Internet search engines such as Google, Bing and Yahoo! store the IP address and search terms of every search performed on their sites. These details are used to help direct targeted advertising at web surfers on the basis of an overall profile of search interests. Google currently keeps every search performed attached to your IP address for 13 months, Microsoft for eighteen and Yahoo! for nine, before the data is anonymised. Similarly, free online email providers such as Googlemail use automated data mining to scan messages and mailboxes for words and terms in order to gain insights into a user’s interests for advertising purposes. In addition, in many workplaces, employee email is routinely monitored by employers. In 2001, it was suggested that 27 per cent of online workers worldwide already had their email monitored (Schulman, 2001).

Keylogging is a less popular, but perhaps a more clandestine form of digital surveillance. A keylogger is a software program that monitors keystrokes on a computer
keyboard. In corporate use, keyloggers can be purposefully installed on employee computers to surveil employee activity (even words, phrases and messages, which are later deleted), or anyone else using company computers. Keyloggers can also be installed surreptitiously on personal or business computers through trojans downloaded during web surfing. Such malicious code can then send keystrokes associated with login and password data to a third party, creating opportunities for fraud, theft and invasions of privacy.

Last, interactive digital video recorders such as TiVo or SkyPlus record a viewer's television viewing and recording habits, which are then stored in a database and used to create a profile of them and their interests. This profile is used to personalise the television experience and draw insights into what kind of programmes an individual might want to record and even to record these automatically for that person. At the same time, this large amount of personal data is stored on company databanks and used in market profiling and targeted advertising research.

**Mobile phone surveillance**

As a last category of surveillance, one can set out the mobile phone as an extremely important mobile surveillance tool that not only captures digital communications, but also real-world locations and movements. Any mobile phone can have its position triangulated within a number of metres through its proximity to surrounding mobile phone masts, as long as the phone is switched on. This positional data is kept by mobile phone companies for between several months and several years and has already been used frequently in criminal investigations.

A new surveillance technique being used by the FBI under US wiretapping law is the roving bug. Roving bugs occur when the microphone of a mobile phone is remotely switched on using an installed piece of software downloaded without the knowledge of the phone user. The microphone can then be switched on without the holder knowing and nearby voice conversations can be monitored and recorded. The microphone can even be switched on when the phone is 'off'. The only way to completely disable the bug is to remove the mobile phone battery.

Last, for personal and business use, there are a number of mobile phone tracking software applications available such as Phonesitter or Mobilespy. These allow a third party to track and monitor the position of a mobile phone on the internet with GPS accuracy. Typical uses for these applications include parents and employers who wish to monitor the movements of their children and employees.

**THE RISE OF SURVEILLANCE: CAUSES AND PROCESSES**

What the previous section demonstrates is that surveillance is pervasive, and particularly so within online and digital contexts. At no point in the past have government agencies, private companies, or even lone individuals been able to collect so much
information about others, in terms of their (virtual and physical) movements, their interactions and communications, or their interests and tastes. From this realisation, it is worth considering how this situation has arisen.

For Lyon (2001), there are four main strands of theory in which surveillance and its increasing pervasiveness in everyday life is discussed within the sociological literature: the rise of nation-state surveillance, the rise of bureaucratic structures, ‘techno-logic’ and the workings of capitalist political economy. More generally, one can see these themes relating to the overall imperatives of security, control, technology and commercial enterprise that provide major influences on the structure of society. The themes of security, control and technology will be discussed below. The discussion of commercial enterprise and political economy is sufficiently large to be taken up on its own in the next section.

Security imperatives: surveillance and the nation-state

Most people tend to think of surveillance and invasions of privacy as primarily resulting from an abuse of power of the nation-state. This is articulated in the general concern that we as a society are turning into a kind of ‘big brother’ state, in which large, all-seeing government organisations subjugate populations through excessive surveillance and record-keeping of its citizens. Fears of such a possibility are legitimated in the very real experiences of populations under Nazi dictatorship and Eastern-European Stalinist regimes, and are further ingrained into the Western cultural imagination through works such as George Orwell’s classic 1984.

Indeed, there is a substantial literature on surveillance within the social sciences which dwells upon the idea that, from their inception, nation-states have been worried about risks and threats to their security both from within and without their borders. As a result, nation-states have always had political imperatives to engage in surveillance. In the case of threats from outside, this involved espionage and the securing of borders. Inside these borders, it involved controlling and securing internal populations through surveillance. Much of this securing has been achieved by what Foucault referred to as ‘biopower’, or the systematic way in which states subjugate bodies and control/classify populations. In the nineteenth century, state initiatives such as public health legislation (including health documentation and record keeping), state education (involving the regulation and record keeping of the activities of juveniles) and the general collection of facts on populations through census data, employment and taxation records, are all examples of biopower that came to prominence in the early days of the modern nation-state.

At the turn of the century, such biopower was enhanced though concerns for increased social control and law enforcement and led to further means of record keeping, classification and identification of populations associated with criminality through biometric identifiers such as fingerprinting (early 1900s) and eugenics (late 1800s). In a post 9/11 era, the use of biometric identifiers has been rekindled and emphasised
through the use of DNA profiles, retinal scans, facial recognition technologies and other biometric identifiers that are increasingly seen as a central element in pushes towards increased security measures for passports and ID cards.

Of course, the increasing powers of surveillance by governments have not gone without criticism, even within a post 9/11 culture. One of the more interesting academic arguments has been provided by Georgio Agamben (1998, 2005), who argued that even before 9/11, governments had been increasingly operating under a ‘state of exception’, a situation in which governments, in the interests of ‘security’, were using extended powers associated with emergency legislation (such as martial law) in order to operate beyond the law. The war on terror intensified this process, and Agamben has noted how state practices of surveillance and biological ‘tattooing’ have spread from those who have been convicted (or suspected of committing) of criminal acts to the general populace. Fingerprinting, picture taking, face scanning and retinal scanning are the sorts of measures that were reserved for convicts and suspects, but now all of us are increasingly having our biometric data stored in databases and our actions monitored. All of us, in effect, are being treated as potential threats, suspected criminals, or terrorists.

Surveillance, control imperatives and bureaucratic structures

As a second theme in the literature on surveillance, Lyon (2001) suggests that the rise in surveillance can also be seen as resulting from the growing influence and intensity of bureaucratic structures, both state and private. Bureaucracy, in its ideal form, involves the rationalisation of large organisations and procedures to produce maximum efficiency. Behaviour in a bureaucracy is modelled on the most efficient means to produce a particular end. In this sense, sociologist Max Weber saw bureaucracy as the archetypal modern form of organisation: logical, rational and efficient.

Beninger (1986) argued that the rise of bureaucratic structures, and the roots of the information revolution more generally, lay in a ‘crisis of control’ brought about by the industrial revolution. He suggested that the increased scale of activity involving long distance travel and the increased speed of both travel and industrial production created the need for forms of control that went beyond the distributed control structures of the face-to-face social realm to the centralised, hierarchical, rationalised, bureaucratic realm. This centralisation of control was enforced by the advanced of communications technology and infrastructure of the time (telegraphy, telephone and mail).

In the post World War Two era, with the expansion of worldwide trade and globalisation, information technology, Beninger argued, began to supplement and replace the role of rationalised bureaucratic structures with automated coordination of activities centralised in information technology. Overall, Beninger suggests that the increasing prominence of information technology stems from a need to control and coordinate ever larger and faster processes of production across expanding spatial scales. Within this context, surveillance becomes just another means of securing efficiency and control among complexity and distance. Within market processes, surveillance of consumers
helps make the consumption process that much more efficient by supplying, for example, targeted advertising or pre-approved credit cards. In the contexts of the state, the surveillance of all citizens as though they are under suspicion can be seen as the most efficient means to combat internal and external risks and threats.

**Techno-logic**

Lyon points to what he calls ‘techno-logic’, which is in effect an extension to the idea of surveillance as a consequence of rationalised bureaucracy. However, instead of resulting from an imperative of control and efficiency, in the theme of techno-logic, increased surveillance is a consequence of an increasing dependence on computers and machines. This approach is informed primarily by the work of Jacques Ellul (2001) and revolves around the idea that as computers become more integrated into society, the more society in its processes must reflect the demands of computerised ways of doing things. The central premise is that the use of technology, in this case surveillance technologies, creates a momentum of its own.

While such a suggestion can be seen as being somewhat technologically determinist, Lyon suggests the concept of ‘function creep’ as supporting the same premise. Function creep occurs when the use of a particular surveillance technology or method (such as CCTV being used to curb excessive vandalism at a school) begins to spread beyond its original (and reasonable) function and into other areas, or used in less reasonable ways. In this example, CCTV cameras used to prevent vandalism in one location might eventually spread into staff rooms and toilet facilities. Perhaps the introduction of cameras into all parts of the school paves the way for microphones to record conversations taking place within the school. Thus, the function creep progresses from a justifiable use of surveillance technology to one that is less justifiable and more invasive on personal freedoms.

**COMMERCIAL IMPERATIVES AND THE POLITICAL ECONOMY OF SURVEILLANCE**

The last strain of surveillance theory for Lyon is within the context of political economy. This set of discussions focusses on the economic imperatives of capitalism and the use of surveillance technologies in the workplace, but also more innovatively in the process of selling, marketing and consumption. In essence, the political-economic perspective brings in aspects of bureaucratic rationalisation as well as ‘techno-logic’, but adds to these the context of economic necessity built into capitalist structures.

**Marketing and personal data collection**

As suggested in Chapter 2, the main challenge within advanced industrial economies over the last few decades has been to expand stagnant markets and profit margins.
The strategy of globalisation has been followed to expand markets abroad, but there have also been efforts made to expand internally by getting people to buy more in domestic markets. One of the major strategies to encourage more individual consumption is to use marketing techniques that speak more directly to people’s interests and personalities, thereby creating products, services and advertisements with greater appeal to individuals. Such strategies are often referred to as ‘targeted’, ‘niche’ or ‘direct’ marketing, in which a group of people (or ‘market’) are identified on the basis of any number of certain characteristics. These characteristics may be anything, but common categories are age, income or lifestyle. This market segment or niche is then targeted for marketing by creating certain products, services and advertisements that are more likely to speak to the circumstances, experiences or characteristics of that population, which:

- Allows marketers and advertising firms to create more effective advertisements.
- Creates efficiency in the advertising/marketing process, in that advertising money is spent directly on the more likely buyers of a product, instead of a larger, less interested mass of people.

This kind of marketing process is driven by information, particularly information about consumers. The more information available about consumers, the more ‘understood’ a consumer is and thus a more direct target they become for advertisers. In previous decades, such information about consumers was obtained with publicly available data such as the census, surveys and mailing lists, which were cobbled together by direct marketing firms. Later on, as consumer culture became more automated through the prolific use of credit cards and ‘loyalty cards’, more information could be obtained, especially with regard to the purchasing habits of individuals. Not only was this information valuable to the organisation that collected it, in the sense that it gave them more insight into the habits and needs of their own customers, but increasingly this information became a valuable commodity in its own right, and was sold on to other firms and organisations.

This information-driven marketing strategy has undergone a revolution with the rise of the internet. Once the establishment of the web in the early 1990s made the internet a viable and usable environment for the average person, it was embraced by business as having massive potential to collect, store, analyse and exchange data on consumers (Zwick and Dholakia, 2004), as well as the potential to communicate more directly with them:

There is no doubt that the main reason for corporate interest in the information highway lies in the fact that it is seen as opening up vast new markets, which also means expanding the range and effectiveness of targeting, motivation research, product management, and sales communication – that is, a total marketing strategy. (Dawson and Bellamy-Foster, 1998: 58)
The internet and the web have been so revolutionary in this regard because every action that takes place on the web, every purchase, every search, every web site viewed and every communication, leaves a trace, data trail, footprint or record of that action. This means that, effectively, all consumer and non-consumer activities can be monitored (Zwick and Knott, 2009).

If one looks at a company such as Google and its use of some of the digital surveillance tools mentioned earlier in this chapter, it is easy to see how much data one private organisation can obtain. Google provides many valuable services to the web population absolutely free of charge: searching, email, blogging facilities (through owning Blogger), language translation and many, many more useful services. Google makes 99 per cent of its revenue from selling directed advertising to consumers based on the multitude of information it collects from the people who use its free services.

How so? Google is obviously the most popular search engine in the world and, as it happens, using any search engine leaves a record of what a specific computer (ISP number) searched for and when. Google stores this information for 13 months to help in its marketing efforts. Furthermore, Google also installs cookies on the computer of each visitor to a Google site, which monitors what web sites are visited and when. In addition, people who use Google’s unlimited email service, GoogleMail, are subject to having their mailboxes data-mined by automated search tools that collect information about what a user is talking about, their interests and the like. And if the same user also happens to use Blogger or Orkut, the blogging and social networking web sites owned by Google, all of the information provided by the user on those sites is monitored by Google as well, and becomes part of their database.

As one can imagine, Google is able to gain unprecedented amounts of information about the users of their services: what they are interested in, what they look at, who their friends are, what advertisements they have responded to in the past. From this information, they are able to present companies that have products and services to sell with a massive customer database and a way of targeting the specific type of person they imagine as receptive to their product. Google’s massive value ($157 billion in 2009 (Yahoo! Finance, Nov. 25 2009)) is based on its growing database of information about consumers and the value of that to advertisers.

Databases, data-mining and discourses

The interactive nature of the web means that in many respects, it can be thought of as a large data-creating database. This data can be operated on to aid in the marketing process, or outside business uses, and be operated on for security and law enforcement ambitions. These ‘operations’ tend to be referred to by two terms: data mining – using computer programs to sift through large datasets according to some specified criteria (Marlin-Bennett, 2004), and Dataveillance – the systematic use of personal data systems in the investigation or monitoring of the actions of one or more persons (Clarke, 1993). For surveillance and security, that may involve an effort such as Echelon searching for terms such as ‘bomb’ or ‘jihad’ in email communications. For marketing agencies, it might involve any one of many demographic, income or lifestyle variables.
Whether data mining or dataveillance, the operations performed on digital information gleaned from web surfing and communications are achieved through the construction of databases. As discussed in Chapter 1, databases can be considered the cultural form of late modernity and the information age (Manovich 2001). In addition, Poster (1995) has argued that databases are also discourses in the Foucauldian sense of the term. That is, a way of thinking about and categorising an object or subject that is manifested through language and embodies power relations within society. Thus, discourses basically ‘create’ subjects or selves. Poster identified computerised databases as a form of discourse, in that they are a configuration of language that constitute an individual subject according to certain ‘rules of formation’ (Aas, 2004). Databases create social identities for people on the basis of certain parameters. In terms of crime and security, this may be ‘suspicious/not suspicious’, ‘security risk’ or ‘potential tax dodger’. In marketing databases this may be a ‘high value/low value/non-value’ consumer, ‘people interested in expensive cars’, or ‘people with credit problems’.

Thus, what the internet has been able to achieve for marketers and for security agencies is a means with which to create, collect and categorise information about individuals in a multitude of ways. This information is then used to sort or categorise individuals based on whatever information seems relevant to an organisation or institution at a particular time. In that respect, the potential identities for an individual are endless and constantly changing. Online life has basically become raw material for the production of consumer (and other) identities, as all behaviour is turned into data points that are organised, manipulated and transformed into a dematerialised identity to be targeted by those who have something to sell (Zwick and Knott, 2009), or those looking for threats.

The result is that the virtual identities produced from databases become virtual bodies upon which power can be enacted, with consequences for the ‘real’ bodies at the computer:

As a meaningful text, the database is no-one's and everyone's, yet it ‘belongs’ to someone, to the social institution that owns it as property, to the corporation, the state, the military, the hospital, the library, the university. The database is a discourse of pure writing that directly amplifies the power of its owner/user. (Poster, 1995: 85)

The power of profiling

The production of identities through a collection of several bits of information is often alluded to by the concept of the profile. Profiling is defined by Clarke (1993: 403) as:

A means of generating subjects or prospects from within a larger population, and involved inferring a set of characteristics of a particular class of person from past experience, then searching data-holdings for individuals with a close fit to that set of characteristics.
Within digital culture, we often think of profiles in terms of representations that we create of ourselves, say on a social networking site, on a blog, or on a dating web site. Indeed these are good examples of how individuals willingly give up personal information to marketing firms and help to themselves, in exchange for a free service. However, the state has a long history of profiling individuals, especially in relation to crime (criminal profiling) and health (diagnosis). The marketing information revolution of the past three decades has allowed consumer profiling to become a dominant activity in the commercial world, and provides a means by which to identify individuals who are likely to be interested in particular products and services. Profiles are the targets, or the means by which direct or targeted marketing attempts to achieve its goals. According to Clarke (1993), profiling procedure involves six steps:

1. Define a class of person.
2. Use existing knowledge to define a profile of that class of person (their demographics, their ambitions, their motivations).
3. Express the profile formally (a set of characteristics to look for).
4. Acquire data concerning relevant populations.
5. Search data for individuals whose characteristics comply with the profile.
6. Take action (i.e., market to them or investigate them).

On the web, such profiling is a continuous process, as there is a continual input of new data from browsing habits, purchasing and communication data, as well as a never-ending amount of products and services to market. This continuous process is illustrated by Zwick and Dholakia (2004) using the example of Amazon.com and their personalised recommendation system. This system continually provides context-driven information (advertisements and recommendations) to their customers on the basis of running profiles. These profiles are maintained and authenticated by a series of features:

- A sign-in procedure authenticating the actual consumer, as opposed to just the computer being used.
- A record of purchase and browsing history on the Amazon.com site.
- Credit card information (including name, address).
- Cookies which keep track of online browsing behaviour.

Similarly to Google, this large amount of information collected by Amazon.com allows them to construct an image of their individual customers not only on the basis of what they purchase, but also where they live and what their overall interests would seem to be. This allows Amazon.com to then recommend books and items that may be more attractive and therefore easy to sell to a specific customer. One of the perceived benefits of this is an increased likelihood for impulse buying (Zwick and Dholakia, 2004).
Databases and profiling: pro’s and con’s

The point of creating databases and constructing profiles is to get closer to the individual: to make them measurable and thus ultimately predictable. While the tone of this section may seem quite critical, it should be pointed out that there are several benefits to profiling for business’s consumers. First, consumer profiling provides customers with a more personalised experience and therefore information on goods in which they might be interested: profiles help people get what they might want. Second, profiling helps to avoid inundating a consumer with irrelevant information characteristic of mass advertising (junk mail and spam). Third, profiling improves the economic efficiency of marketing activities by making contact with good consumer prospects for a product and weeding out the poor ones. Last, it has to be noted that the vast majority of the operations performed on databases and profile creation are automated (see Chapter 1). So although personal information is collected in abundance, which creates a more personalised experience, the information is not normally subject to direct human surveillance.

At the same time, there are a number of real and potential downsides to the ubiquitous use of database and profile identities. First of all, one could make the point that databases and profiles, just like any form of discourse, do not describe or represent identities as much as they create identities that make themselves true. What I mean by this is that, as Clarke (1993) suggests, profiles attempt to predict future behaviours. At the same time, these profiles also prejudice future behaviours (of consumers) by limiting the exposure of certain individuals or groups to certain types of information deemed irrelevant or not suitable to them by the profiling process. This process limits choices and thus constrains future actions in a kind of feedback loop between profile construction and the narrow range of options then tailored to that profile (Zwick and Knott, 2009).

Second, the identities and classifications created are done so externally, by agencies outside the individual, and not internally, as a choice of the subject or individual. In that sense, a profile or database identity is an erosion of personal autonomy, where knowledge of individuals is instead used to label and control them without their consent and often without their knowledge (Poster, 1995). This is significant because, in the digital environment, these disembodied virtual identities are what stand in for the individual. As far as the profiling agencies and businesses are concerned, these profiles are the consumer. In that sense it is significant that individuals themselves have little say in how they are classified and are in general not aware of the information used to classify them, or even of the people and agencies involved in doing the classifying. Poster refers to this process of disembodied, largely anonymous surveillance and sorting as a superpanopticon.

Third, the information collected in databases and used in profiling in many respects breaks the distinction between public and private information. Poster (1996) contrasts the contemporary situation with the not too distant past, when most people made their purchases with cash, as opposed to with credit or debit cards (obviously necessary for online purchasing). In the age of cash, individual purchases and economic transactions were private and largely anonymous. What shops you visited and what you bought was
between you and the proprietor. In the digital environment, all this has changed, ‘the
digital consumer is neither anonymous nor private’ (Zwick and Dholakia, 2004: 30).
Both this type of information, as well as information voluntarily supplied by consumers,
now gets collected by firms who often sell it on to other companies, or is inherited by
firms that purchase these companies. Even the databases of public or governmental
agencies can end up in private hands if that service becomes privatised or outsourced
to private companies. There is no real way of knowing where personal information will
end up or how it will be used. As Poster suggests, information becomes ‘everyone’s and
no one’s’, in that as personal (and often private) information has achieved commodity
status, it can also be seen as a publically saleable item.

WHY CARE ABOUT A SURVEILLANCE
SOCIETY?

What should be gathered from the previous sections is, first that privacy is a concept
with many facets revolving around two very broad notions of ‘solitude’ on the one hand
and ‘autonomy’ on the other. Second, that these ‘rights’ are not fixed or innate, but are
culturally, historically and legally contingent. However, despite the contingent nature of
privacy, it is important to note what the consequences might be of an increasing lack of
privacy in an age of constant and uncontrolled surveillance.

Spinello (2003) suggests that a lack of privacy can lead to losses of freedom for indi-
viduals in two forms: **extrinsic** and **intrinsic**. An extrinsic loss of freedom can be consid-
ered a real, palpable loss of freedom by having one’s behaviour or opportunities unjustly
limited by others, and can come in many forms. An intrinsic loss of freedom has more
to do with how people’s perceptions help to curtail their freedoms. This last section will
explore several ways in which negative or unjust consequences can emerge from too
much surveillance (especially of the digital variety) and how both extrinsic and intrinsic
losses of freedom can result.

People can potentially be affected by the use of information that they have not willingly
supplied. The use of personal or sensitive information collected without a person’s knowl-
dge or permission can have all manner of potential personal or financial consequences
for an individual. In a hypothetical example, a person may apply online for life insurance
(say, as a compulsory condition of obtaining a mortgage on a house). Now, perhaps jus-
tifiably so, an insurance company will require information about current medical condi-
tions, family medical histories, age, weight and the like in order to determine whether or
not the applicant is worthy of a policy, or poses too great a risk for the company to insure.
The applicant will willingly give up such information if they want a policy. However, sup-
pose that the life insurance company also used cookies from its website to track the
web surfing activities of the applicant as part of building a risk-assessment profile of the
applicant. After examining cookie data and web activity, the insurance company comes to
the conclusion that the applicant may engage in ‘risky’ sexual behaviour and refuses the
policy. In this case, the applicant is judged on more information than he/she voluntarily
submitted, and judged on data of which they are unaware.
This leads to the second point, that information collected about individuals can be used against them without their knowledge or knowledge of the data sources. Credit ratings, for example, are an important part of modern consumer society, which is founded on the idea that people need to borrow money to make large purchases, such as cars and houses. The lack of a good credit rating can severely hamper someone’s ability to participate in consumer culture to a ‘normal’ degree, and even prevent them from finding a place to live. Yet credit ratings are a very secretive process about which most people know very little. They can be adversely affected by certain kinds of information, which circulate through financial institutions whenever a credit card, a mortgage, a loan, or even connecting to phone, power and other domestic utilities is applied for. When trying to organise these services in their daily life, most people are not aware of what information is being used to judge them as reliable applicants, or the variety of sources from which the information is coming. It is like being accused of being unreliable by an unknown accuser, using unknown data and without having the ability to answer back. Given its clandestine nature and the variety of sources, decisions based on such information can be very difficult to dispute.

Third, the information used may not be correct, taken out of context, or unfairly used. For example, in the above example of an individual applying for an insurance policy, the decision to deny the application might be based on web surfing data from cookies which suggest that the applicant engages in risky sexual behaviour. But there are many ways in which that assumption might be a false one. The individual might be sharing a computer with someone else, or they could also be concerned about a friend’s health or behaviour and are looking up information with regard to these concerns. In either case, the decision to reject is based on mistaken assumptions (although they may be logical, or even reasonable assumptions) gleaned from cookie data.

To take a less hypothetical example from my own life, several years ago I purchased a self-help book online about Obsessive-Compulsive Disorder, through Amazon.com to give to a family member. To this day, whenever I log onto Amazon.com, it recommends books on OCD and displays this recommendation prominently on my personalised web page. In addition, I continue to get emails recommending OCD and other self-help books to me, with email subject headings like ‘Get Getting Over OCD (Guilford Self-help Workbook) (Guilford Self-help Workbook Series) by Jonathan S. Abramowitz for £12.83’. Amazon.com assumes that I suffer from OCD, and potentially anyone keeping track of my email communications or even walking into my office and noticing those emails on my computer can assume that I suffer from OCD as well. This seems like a reasonable assumption, but it is a wrong one because there is no context to the data in question (for a longer discussion about context and databases, see Chapter 1). Nonetheless, there is the temptation to make those inferences. Indeed, our previous discussion of ‘profiling’ suggested that surveillance for the purposes of monitoring crime and for gathering consumer data increasingly involves such inferences.

In addition, unlike analogue or ‘hard copy’ information, digital information about people has the potential for a permanent life span and can remain easily accessible indefinitely. In criticism of this trend, Blanchette and Johhnson (2002) provide a compelling argument for the necessity of ‘social forgetfulness’ in society. They suggest that in an
analogue world of paper, file folders and filing cabinets, a certain amount of social forgetfulness was automatically built into any bureaucratic system, as it was only possible to keep detailed and readily accessible data on a large amount of people for a relatively short period of time before files and storage facilities became full. As a result, records for much behaviour, such as juvenile crime records, school records, financial problems, bankruptcies and the like would eventually be either destroyed or sealed away in archives after a number of years:

In the paper-and-ink world, the sheer cumbersomeness of archiving and later finding information often promoted a form of institutional forgetfulness – a situation which parallels human memory. (Blanchette and Johnson, 2002: 34)

This forgetfulness corresponded with a general sense that it was necessary, especially in a democratic society, to allow people to eventually be forgiven (or at least forgotten) for past mistakes if their nature was not too serious and if the individual had reformed their ways. In a consumer society, such forgetfulness could be seen as vital. The need to overcome past mistakes in the form of personal bankruptcies or poor credit histories after a number of years of good financial behaviour is an example of how such forgetfulness can help to give people second chances to participate normally in society.

However, in the age of digitised record keeping and continuous collection of data, there are no physical or practical limitations to the duration that data about individuals can be kept, nor on the ease of access of such data. As a result, there is a danger that individuals will never be able to overcome their pasts. No transgression or misdemeanor will ever be forgotten, no second chances will ever be granted. In a networked and digitised surveillance society, mistakes made could conceivably haunt someone for the rest of their life, and continually interfere with financial and social well-being. The past will always be present, and the notion of ‘reform’ could very easily be replaced by ‘exclusion’ over perpetuity (Blanchette and Johnson, 2002).

Fifth, private data retained by commercial organisations is vulnerable to government seizure, especially under growing legal data retention requirements. Commercial data logging is always at risk of being turned over to government and law enforcement agencies for criminal cases as well as for private lawsuits. This has been recently demonstrated in court decisions in both the US and the UK, where the identities of anonymous bloggers and forum contributors have been subpoenaed by legal authorities and turned over by web administrators (Dyer, 2007; Gibb, 2009; Nasaw, 2009). Within security and personal defamation contexts, such measures seem to make sense, however, further incidents involving China and Yahoo! as well as India and Google have shown that such information can be demanded by governments when on the hunt to persecute political dissidents (Kahn, 2005; Snyder, 2008).

At the moment, such government manoeuvres seem far away from the reality of life under the relatively benign democratic governments of the West, but if that situation were to ever change, the sheer amount of personal information collected by commercial organisations would be a huge resource to an autocratic state, with consequences for all.
Also, the data collected by commercial and government organisations can never be fully secure, and leads to inevitable personal data breaches. Hardly a month goes by in any major post-industrial nation without some sort of scandal involving the leakage of personal information into public hands. Data can be left on trains, or in taxis, stolen from government or corporate computers during robberies, accidentally sent via email, or downloaded onto the internet. The examples are numerous:

- In September 2009, Demon internet, a UK ISP provider sent its customers a mass email regarding billing arrangements. Attached to this email was a file that contained the names, email addresses, telephone numbers and usernames/passwords of over 3,500 of its personal and business clients.

- Again in September 2009, the University of North Carolina School of Medicine was the victim of hacking, which compromised the personal information, including social security numbers, of 163,000 women.

- In June 2009, over 100,000 pension holders in the UK had their personal and banking details put at risk when a company contracted to develop software had one of their laptops, containing all this data unencrypted, stolen.

- In August 2009, the Rocky Mountain Bank of America accidentally sent a file with the names, addresses, tax identification numbers and bank loan information for 1,325 customers to an unknown Googlemail account.

Stories like these are commonplace, as suggested by the fact that these four incidents took place within four months of each other. Events such as these, as well as the rising number of cases of credit card fraud and identity theft, remind us of how much information about us is collected and held by corporate and public bodies on their computers and servers, and how vulnerable such databases are to human error as well as criminal intent. But past the headlines of data leaks and security breaches that make us feel concerned and vulnerable, there is a larger question about not only the security of personal data, but the sheer amount of it which needs to be protected.

Last, but by no means least importantly, are the intrinsic consequences of over-surveillance. Intrinsically, the effect of hypersurveillance, or digital panopticism is to create a state of consciousness in which one is aware of permanent visibility. The effect of this awareness is that it leads to a change of behaviour in the face of the inherent threat of surveillance. In other words, people limit their actions and behave differently when they feel as though they are being watched. When taken to extremes, this produces a sense of being continually oppressed under a regime of power. People become fearful not of doing wrong, but of being seen as wrong. Furthermore, as Blanchette and Johnson (2002) suggest, anxiety from the repercussions of making a mistake or doing something one may later regret is not conducive to a free or democratic way of life:

Privacy is not just something individuals want because it makes them feel good or is good for them; rather, privacy is good for society insofar as it promotes the development of the kinds
of individuals who are essential for democracy ... a world in which everything one does is recorded and never forgotten is not a world conducive to the development of democratic citizens. It is a world in which one must hesitate over every act because every act has permanence, may be recalled and come back to haunt one, so to speak. (Blanchette and Johnson, 2002: 36)

CONCLUSION

The growing density of surveillance practices in everyday life is not the product of some capitalist conspiracy or the evil effects of a plutocratic urge. No, it is the outcome of the complex ways in which we structure our political and economic relationships in societies that value mobility, speed, security and consumer freedom. (Lyon, 2001: 2)

This chapter has provided a general overview of many of the main issues regarding privacy and surveillance in the digital age. When considering such a discussion, it is important at the outset to realise that privacy as a concept is historically, culturally, and legally contingent. Thus, it is reasonable to expect that just as our expectations of privacy have changed in the past, they might very well change in the future.

Our increasing use of, and dependence on, digital communication technologies in everyday life, through work, shopping, entertainment and social interaction has led to the point where movements (both virtual and real), communications, tastes, financial situations and even (to a degree), our thoughts, interests and opinions can be monitored and recorded to an unprecedented degree. One of the key perceived advantages of these digital technologies is that they can (hopefully) help to reduce risks through the continual collection of data about individuals and their actions. However, the reduction of risk is inherently tied to an increase in the amount of control that pervades society. This is a current tension within a contemporary society that has, on the one hand, an unprecedented ability to monitor the actions of individuals and, on the other, has an implicit cultural and explicit legal value for individual rights and freedoms. Here the phrase ‘knowledge is power’ (in this case, knowledge of other people) certainly springs to mind and points us towards the increasing amount of state surveillance (as well as by individuals interested in gaining power over others) that is possible in the digital age.

At the same time, it must be recognised that the lion’s share of surveillance data is not collected by governments, but by private corporations operating under the central principle at work in the information age: that information itself has attained the status of a commodity. It could also be suggested that ‘knowledge is revenue’. In this respect, personal data collection has become an ordinary and often lucrative part of the web and other digital communication technologies where such information is solicited, collected, sold and used to aid in marketing and advertising strategies. The sheer variety
of organisations collecting and distributing information, combined with the sheer mass of information being collected, makes this kind of information potentially much more vulnerable than the classic fears of a ‘big brother’ society.

**FURTHER READING**