A Report on the Surveillance Society

For the Information Commissioner, by the Surveillance Studies Network

Public Discussion Document

September 2006

Edited by:

David Murakami Wood and Kirstie Ball

From material by:

Louise Amoore
Kirstie Ball
Steve Graham
Nicola Green
David Lyon
David Murakami Wood
Clive Norris
Jason Pridmore
Charles Raab
Ann Rudinow Saetnan

London 2016: Everything is Under Control[1]

As 18-year-old Ben Jones and his fellow anti-war protestors walk through the centre of London, they are monitored constantly. Small remote control UAVs (Unmanned Aerial Vehicles) circle overhead[2]. These spy planes were introduced for the Olympics of 2012 and the 'success' of what the adverts call the 'friendly flying eyes in the sky' has been hailed by the Mayor as a reason for their continued use[3]. Now people have almost stopped noticing them. Tiny cameras embedded in lampposts and walls at eye level as well as up above allow the more efficient operation of the now universal facial recognition systems.[4] Morphing software which combines images from multiple cameras to build up a three-dimensional picture is also being pioneered, although campaigners and lawyers argue that it is inaccurate and not a 'real' image. Almost universal wireless networking allows the cameras to be freed from bulky boxes and wires. In addition, it is linked to intelligent street lighting which provides 'ideal' lighting conditions for facial recognition, and also to automated floodlighting and extra cameras which are activated by 'unusual' movement. Many important state buildings which had been surrounded by concrete barricades after 2001 now appear open once again, but are instead protected by a variety of sensors linked to impenetrable automated barricades that sink into the ground when not immediately needed.

Walking back towards the Underground, Ben and his mate, Aaron, accidentally stray into the Westminster Exclusion Zone. They are stopped by private security personnel employed by the Westminster Business Improvement District (BID)[5], who are remotely supervised by police operators via their handheld computers[6] and helmet-mounted microcameras, which scan the two boys[7]. Ben submits to the usual DNA swab, which is analysed instantaneously, and hands over his ID card, which is swiped. As the info flicks up on his screen, the officer jokes that it seems ironic that an anti-capitalist like him has just been on holiday in the USA[8]. Ben grimaces politely. ID cards are still supposedly voluntary and Aaron, who comes from a very Christian family, refuses to have one. His mum says it is 'the mark of the beast', but he just wants to be left alone. He's finding it hard now, though: not having a card means he has effectively opted out of the chance to apply for government jobs and receive benefits or student loans, and he can't travel by plane or mainline train even within Britain. He's beginning to wonder if it's worth it and how he can live. It's about to get worse for him: as a young black male with no ID card, he scores highly in police risk profiles and the police control room instructs the security personnel to bring him in for extra questioning[9] …

This imagined 2016 is not that far away.

In 2004, the Information Commissioner, Richard Thomas, the officer empowered by Parliament to act as a watchdog on the use of our personal data, warned that we were 'sleepwalking into a surveillance society'[10].

But we are already living in a surveillance society:

- Video cameras are watching us everywhere – in buildings, shopping streets, roads and residential areas. Automatic systems can now recognise number plates (and increasingly faces).
- Electronic tags make sure those on probation do not break their release conditions, and people arrested by police have samples of their DNA taken and kept whether they are guilty or not. 'Criminal tendencies' are identified earlier and earlier in life.
- We are constantly asked to prove our identity, for benefits, healthcare, and so on. The government now plans to introduce a new system of biometric ID cards, including 'biometrics' (fingerprints and iris scans) linked to a massive database of personal information.
- When we travel abroad, who we are, where we go and what we carry with us is checked and monitored and the details stored. Our passports are changing: computer chips carry information, and like ID cards, there are proposals for biometric passports.
- Many schools use smart cards and even biometrics to monitor where children are, what they eat or the books they borrow from the library.
- Our spending habits are analysed by software, and the data sold to all kinds of businesses. When we call service centres or apply for loans, insurance or mortgages, how quickly we are served and what we are offered depends on what we spend, where we live and who we are.
- Our telephones, e-mails and internet use can be tapped and screened for key words and phrases by British and American intelligence services.
- Our work is more and more closely monitored for performance and productivity, and even our attitudes and lifestyle outside work are increasingly scrutinised by the organisations that employ us[11].

The surveillance society has come about almost without us realising.

It is the sum total of many different technological changes, many policy decisions, and many social developments. Some of it is essential for providing the services we need: health, benefits, education. Some of it is more questionable. Some of it may be unjustified, intrusive and oppressive. People may have many different opinions. But in fact most people know very little about the surveillance society: it is seen as the stuff of science fiction, not everyday life. So there has been very little public debate about surveillance. The surveillance industry is already massive and (especially since 9/11) is growing much faster than other industries[12]: the global industry is estimated to be worth almost $1 trillion US dollars, covering a massive range of goods and services from military equipment through high street CCTV to smart cards. The surveillance society has come about often slowly, subtly and imperceptibly and by the unforeseen combination of many small paths into one bigger road. It is a road whose direction we urgently need to discuss and debate.

Looking After You

Geeta is 69 years old, and is living alone in her flat. In addition to emergency motion detectors in all the rooms, her bath has an inbuilt heart rate monitor, her toilet has a device which measures her blood sugar levels, and her kitchen has a number of sensors which detect gas leaks, fire and floods. She has a panic button linked to the local authority call centre, which can instantly call and check on her if it's pressed. But the presence of sensors and cameras all over her home means that her family know she is safe so she gets fewer family visits than she used to, which leaves her feeling a little isolated. However, she finds the RFID (Radio Frequency Identification) scanners in her fridge and cupboards extremely useful: every time she runs low on groceries, her household management computer automatically orders from her local supermarket over the internet. Her subscription to home delivery means that she does not need to make unnecessary visits to the shops. She is also used to her regular 'Well Woman' checks. However, unknown to her, the NHS constantly compares Geeta's results with those of other women of her age from every other health authority in the country.[13] This enables them to decide on risk factors so that, for example, a heart attack can be predicted with a much greater degree of accuracy. As a result, Geeta is provided with dietary advice as she is in a high-risk group for heart disease. But there are problems: the NHS is now continually fending off large cash offers by insurance companies to access health information on a 'need to know' basis. With depleted resources, these offers are increasingly tempting, but for now NHS bosses are still wary of a scandal like that in Iceland, which turned over its whole DNA database to private companies for research and private profit.[14]

What's wrong with a Surveillance Society?

Surveillance is not a malign plot hatched by evil powers. Much surveillance has good or at least neutral intentions behind it: desires for safety, welfare, health, efficiency, speed and co-ordination. Some surveillance intentionally aims to limit and control our behaviour or movements, often without our knowledge or consent. And some surveillance has this effect without intending it. However, this does not mean that all this is acceptable: understanding the effects of surveillance and the impacts they have on our personal lives and on society is crucial.

We have become increasingly concerned with risks and dangers, rather than with more positively intended social goals. As more and more everyday situations are thought of in terms of 'risk', what was previously exceptional security becomes normal. However, we rarely think about the unintended consequences that lead to inequalities of access and opportunity and distinctions of class, race, gender, geography and citizenship not only being made worse but also becoming intrinsic to the way all everyday decisions are made.

Surveillance processes and practices also help create a world where we know we are not really trusted. Surveillance fosters suspicion.[15] Employers who install keystroke monitors at workstations or tracking devices in service vehicles are saying that they do not trust their employees. The welfare benefits administrator who seeks evidence of double-dipping or solicits tip-offs about a possible 'spouse-in-the-house' is saying they do not trust their clients. And when parents start to use webcams and GPS systems to check on their teenagers' activities, they are saying they do not trust them either.

The final question for surveillance society is whether we have become so hypnotised by the 'need' to find high-tech solutions to crime, terrorism, fraud and many other problems that we forget to ask whether these solutions are even appropriate, and whether there might be other, non-technological or less invasive answers.

This short document, and the full report which accompanies it, is designed to start to address these questions, to inspire much-needed public discussion. We may want to live in a surveillance society, but if so, it is something we should decide with our eyes open, not in our sleep. In the following pages the surveillance society, and its consequences, are described in more detail.

What is the Surveillance Society?

The surveillance society is a society which is organised and structured using surveillance-based techniques. To be under surveillance means having information about one's movements and activities recorded by technologies, on behalf of the organisations and governments that structure our society. This information is then sorted, sifted and categorised, and used as a basis for decisions which affect our life chances. Such decisions concern our entitlement and access to benefits, work, products and services and criminal justice; our health and well-being and our movement through public and private spaces.

The following pages outline some of the key characteristics of the surveillance society: technology, data flow, convergence; social sorting; technological lock-in and failure.

Technology

It is worth remembering that surveillance has been important throughout history and that some of the most authoritarian regimes, such as the former East Germany, have been based on nothing more sophisticated than paper files and informers.[16] But advanced technologies have changed surveillance. New surveillance technologies are smaller and more powerful, allow many more kinds of information to be collected, stored and connected together, and operate more instantaneously. This document cannot hope to cover every surveillance technology nor every area in which such technologies are used. It is instead designed to indicate some key changes that have taken place in five areas: the database, telecommunications, CCTV, biometrics, and tagging and tracking technologies.

The Database

The foundation for all new surveillance technologies is the computer database. Massive amounts of data can now be gathered, tabulated and cross-referenced far faster and more accurately than old-fashioned paper files. Huge stores of personal data held on ordinary people are now central to both private business and public services. Different data sets may be matched against each other to identify persons and suspicious patterns of activity. The data may also be 'mined' – analysed in great depth by sophisticated technologies to reveal patterns that may require further investigation.

Every transaction provides a 'data trail', linkable to an individual or type of person or place.[17] These transactions include the use of credit cards, bank cards, mobile phones, the internet, a purchase, search or phone call. Additional data are generated through loyalty card programmes, customer surveys, focus groups, promotional contests, product information requests, call centre contacts, website 'cookies', consumer feedback forums and credit transactions. This is often overlaid with data from public sources such as National Statistics and non-profit organisations or specialist data collection companies, to create 'profiles' of individuals or communities. Even more sophisticated techniques called Knowledge Discovery in Databases (KDD) now identify hidden

patterns and predict future transactions in an increasingly personal way, for example the way *Amazon.com* offers customers books or DVDs that they might like.[18]

Databases are a key part of change in public services, for example the National Health Service (NHS)'s controversial IT programme, *Connecting for Health*, the largest in Europe.[19] This will connect up Electronic Patient Records (EPR) and local information to create a complete national digital database of all personal health records. Some two million people a year are arrested by the police in England and Wales. Fingerprint impressions and DNA samples are now taken from virtually all arrestees and stay in police databases regardless of guilt or innocence. There are now nearly six million sets of prints in the database,[20] and the National DNA Database, set up in 1995, now records the DNA of 3.45 million individuals, or 5.2% of the total population. It is worth noting that 40% of black males are now profiled on the database compared with 9% of white and 13% of Asian males.[21] Further police databases include Automatic Number Plate Recognition (ANPR), the Violent Offender and Sex Offender Register (ViSOR), and a proposed Facial Images National Database (FIND). Soon, these are all planned to be connected via the Police National Computer (PNC)[22] which will eventually be accessible not only at police stations but, with the development of Airwave, the new police digital communications system, the patrol officer on the street via a handheld computer.[23]

National borders are becoming 'smart borders', with huge databases behind the scenes processing information about individuals and their journeys. Profiling is used create watch lists of dangerous passengers or identify groups who might be more 'risky'. Overt racial profiling is even being suggested as official policy[24].

Surveillance is Coming Home

Arriving back from a holiday in Florida in 2016, the Jones family face a rather different border. Both Britain's and the USA's immigration and border control services, along with those of all EU countries and other G10 industrialised countries, are outsourced to the same transnational private consortium, BorderGuard[25]. Continued fears of illegal immigration and government rhetoric about the 'War on Terror' led these governments to implement a 'smart border' scheme. Passport control is now a series of cameras and scanners taking images of face, iris and fingers, which are compared with those on the standardised biometric passports, or in Britain's case, the ID card, introduced across the G10 countries and the EU[26]. The data on the built-in RFID chip now includes all citizenship, immigration, visa and criminal justice data, along with health information, and is compared instantaneously with both national and international databases, as well as a whole raft of data-mined information on consumer transactions that BorderGuard gets from specialist companies[27]. For most of the family the transition is swift, but for grandmother Geeta there are problems. Pakistan has not yet signed up to the full version of the smart borders scheme and Geeta has never bought a biometric passport. She consequently has to wait in line for several hours and is subjected to various extra searches and questions. Despite her British ID, mother Yasmin's obviously 'Asian' features also mean that her movement through the border triggers alerts and extra questions. Then, at customs, everyone is subjected to a full-body scan, a virtual strip search …[28]

Telecommunications

'Telecommunications' includes not only the old-fashioned fixed-line telephone system with voice calls and faxes, but also mobile phones (including voice, text, images, sounds and location-based information) and computer communications such as the internet ('broadband', etc.). In the days of

analogue state-run telephone systems, it used to be that telephones had to be 'tapped' (usually by the police or security services) to be under surveillance. Three things have changed: the telephone technologies themselves (mobile phones, optic fibre, wireless, etc.), the combination of telecoms and computer storage and processing (e-mail, websites, etc.), and the move to private telecoms companies. Current changes mean increasing convergence of technologies, and 'interoperability' – different technologies working together.

For any of these technologies to 'work' requires the exchange of signals or data between different devices, and this exchange can be monitored. For example, mobile phones can be located, and website visits catalogued by Internet Service Providers (ISPs). As telecommunications technologies are more connected, more information is produced. The law is now demanding that such information is kept for analysis: in February 2006, both the EU and the Home Office have proposed that the data should be retained for up to two years in order to be available for police scrutiny.

Nations also routinely filter vast amounts of telephone, telex, e-mail and fax traffic for reasons of 'national interest' (both security and economic interests). For example, the so-called 'ECHELON' system, the global surveillance network operated by the American National Security Agency (NSA), maintains a huge base at Menwith Hill in North Yorkshire, which routinely automatically filters all telecommunications traffic passing thorough the UK for key words and phrases and increasingly employs more sophisticated algorithms for advanced speech and even meaning recognition[29].

Virtual Surveillance

After Ben is let go by the police, he goes on his way, but his own handheld computer[30] is now being tracked via the Galileo system[31]. He is also put on a watchlist for communications monitoring and his ISP is served an automated RIP 2 Act 2009 order that all his internet traffic and e-mail communications must be saved and passed to the police[32]. As most telephony is now conducted over the internet (and old landlines are disappearing), this covers all Ben's communications. One unforeseen result of the surveillance of Ben's communications is that Ben's younger brother Toby, who occasionally uses Ben's accounts (largely just because he enjoys cracking[33]), is also drawn into the surveillance. Toby lives most of his life online on Massively Multiplayer Online Games (MMOGs), virtual worlds that have their own rules and entire alternative economies[34]. However even here the surveillance society has penetrated. These worlds of data and behaviour of 'avatars' online are monitored, particularly by companies, which aim to understand the new opportunities for emerging real-life markets, and there exists a whole new class of corporate game players who exist only to research the habits of people via their avatars and virally market both virtual and real products inside and outside these worlds to their players[35]. Police have also begun to experiment with software that monitors virtual worlds to identify avatars who exhibit certain types of behaviour which could indicate real-world criminal tendencies in their players[36]. This of course is hugely controversial among gamers, who argue that the escapism of virtual worlds should not be mistaken for real life.

Video Surveillance

Although it goes back to the 1960s, the period of growth of closed-circuit television (CCTV) in the UK dates from the late 1980s, prompted by attempts to reverse the decline of city centre shopping districts as well as fear of terrorism, crime and hooliganism. There may now be as many as 4.2 million CCTV cameras in Britain: one for every fourteen people,[37] and a person can be captured on

over 300 cameras each day.[38] An estimated £500 million of public money has been invested in the CCTV infrastructure over the last decade,[39] but a Home Office study concluded that 'the CCTV schemes that have been assessed had little overall effect on crime levels'.[40]

Digitisation has allowed increasingly automated use of CCTV systems. Vehicle number plates are being used to identify the registered owner. Camera-based enforcement of speed restrictions increased from just over 300,000 in 1996 to over two million in 2004 and is raising an estimated £113 million in fines a year.[41] This increase in state surveillance has received a consistently negative press,[42] despite the fact that speed cameras, unlike open street CCTV, have a significant impact in reducing death and injuries cause by traffic accidents.[43]

The intensification of surveillance of the motorist is set to expand rapidly. In March 2005 the Association of Chief Police Officers demanded a national network of number-plate readers 'utilising police, local authority, Highways Agency, other partner and commercial sector cameras'[44], including the integration of the existing town centres and high street cameras[45], with a National ANPR (Automatic Number Plate Recognition) Data Centre. This would have the operational capacity to process 35 million ANPR reads every day, increasing to 50 million by 2008, stored for two years.

Driving Change

When Gareth drives out of the estate, the wrought-iron gates swing open automatically, and the exact time of departure and the number and identities of the driver and passengers are recorded by camera. On the roads, ANPR has been operating nationwide since 2008 and there are now so many cameras that there is no longer any point in trying to second-guess where they are with scanners or maps. In any case, the handheld computer that Gareth plugs into his car is linked to the Galileo global satellite navigation system and to state congestion cameras and helps to provide the quickest route. Finding the shortest route is also less expensive since through the ANPR system car mileage is automatically charged to Gareth's bank account[46].

Biometrics

Almost all new ID systems also use some kind of 'biometric' or body trace: fingerprints, iris scans, facial topography and hand scans are all used on different passports and ID card systems. Biometrics are often presented as being infallible. The idea is that accuracy will be increased and fraud reduced. PINs and passwords may be forgotten or lost, but the body provides a constant, direct link between record and person. They have been particularly promoted by the USA since 9/11 and America has pushed for common standards for biometric passports.

Biometric entry systems (using voice and hand scan in particular) are now common for access to many office buildings or private company property, and in some airports, for example the Privium iris-scanning system at Schiphol Airport in the Netherlands, but biometrics are moving into the streets too. In British cities there have also been experiments with automatic 'face recognition' software in Newham (London), Birmingham, Tameside, Manchester, and other locations. Face recognition, and other biometric CCTV systems, still do not really work properly outdoors or in crowded city streets full of fast-moving people. However, there is huge investment in improving them.

Your Health is Our Business!

In 2016, Gareth works as a call centre manager. As in 2006, employees are still monitored every minute of the day, via a computer which records every activity they perform and for how long they perform it. However, surveillance for recruitment and benefits has intensified. Employees are now subject to a range of biometric and psychometric tests, and lifestyle surveys. Gareth feels it is important that the lifestyle profile of the employee match those of the customers to ensure better customer service.[47] He is also concerned that employees do not engage in dangerous sports, such as rugby or mountain biking, as this might cause long periods of absence through injury. Biometric testing, which involves mouth swabs and urine samples, easily analysed by the on-site nurse using a cheap kit, means that the employer can assess whether the prospective employee poses any productivity risk through health problems or substance abuse. It also enables the organisation to design a flexible benefits package depending on the employee's state of health. Some keen applicants for jobs have begun providing health information voluntarily and now the company often discards CVs that do not contain this information. Because of concerns about employees' health, many companies have become proactive. In conjunction with local gyms, employees use their workplace RFID smart access cards to get a reduced rate. Their gym attendance shows up on their electronic employment record, and employees who do not attend regularly are sometimes questioned about their lifestyle in their annual appraisals. Periodic psychometric testing also indicates to management whether the employees' attitudes are compatible with the company's culture and values.

Locating, Tracking and Tagging

Surveillance is increasingly about tracking people, through GIS (Geographic Information Systems), GPS (Global Positioning Systems), RFID chips, smart ID cards, transponders or the radio signals given off by mobile phones or portable computers.

Both GPS and RFID are increasingly being seen as solutions in law enforcement and personnel management. Electronic monitoring has also been introduced as a condition of being granted bail and in 2004/5 some 631 adults and 5751 juveniles, some as young as twelve years old, were 'tagged', allowing them to await trial at home rather than be remanded into custody.[48] Offenders released from prison are also increasingly subjected to electronic monitoring, either as a condition of early release from prison under the Home Detention Curfew Scheme,[49] or as a condition of being released on parole.[50]

Until recently RFID was restricted to large shipping containers, consumer goods and various kinds of smart cards' Recently a notable change has occurred largely unnoticed: the implantation of living beings. Chips containing information about immunisation records and ownership gradually replaced quarantine requirements for household pets in the EU from 28th February 2000 through the PETS scheme, which has since been extended beyond Europe[51]. The first human use of RFID chips has been in elderly people in the USA suffering from degenerative diseases, and around 70 people have now been implanted to enable carers to locate them easily[52]. Researchers and technological enthusiasts have also been implanting themselves with chips for several years[53], and at least one chain of Spanish nightclubs has offered patrons the chance to have cash and access privileges held on implanted chips[54]. However, a step-change occurred in February 2006 when a security company in Ohio, USA, implanted two of its workers with RFID chips to allow them to access company property[55]. The call for everyone to be implanted is now being seriously debated on some technology websites.

For the future, both RFID tags and GPS are seen simply by companies as a means to produce customised marketing in real time to particular consumers, offering discounts on mobile devices to retail outlets in a given location, for instance. Continued developments in the application of real-time location data to consumer profiles will provide yet another layer of data to assist corporations in targeting marketing campaigns to particular consumers, and potentially also allow tracking by law enforcement and other government surveillance.

The New Brandscape

In 2016, when the Jones family visit their local shopping centre, CCTV and security guards are still there. But some things are different. As well as controlling crime, spatial modelling of the 'brandscape'[56] and changing advertising according to the flow of different categories of consumer is now a strategic priority. The retail chains allow the shopping centre access to a huge shared database, modelled on reward card data, to generate information about shoppers. The system relies on RFID clothing tags, ubiquitous scanners and consumer datasets. Scanners in the doors of shops log the unique identifiers found in RFID tags embedded in shoppers' clothes. Intelligent billboards placed at eye level display advertising from a select range of products aimed at each consumer in real time. Sara is delighted to see the new download by her favourite band appear on the screen and Toby notices information about special modifications to his favourite online game world. Marketing messages can also be sent to consumers' handheld computers when they are near particular stores.

High-value customers are now invited to register for a new cashless scheme. This enables more 'valuable' consumers[57] to get an implanted chip instead.[58] This costs £200, but with all the special discounts at stores[59] this will soon be paid for (and more). People can load the chip with money, and pay in the different stores by getting their arm scanned rather than use a credit, debit or store card. The chipped shoppers also get access to a VIP lounge, spa and massage facilities on site. The marketing for the 'cashless' system tells consumers they are less of a target for muggers or pickpockets, and even credit card fraud. There have been rumours of shoppers being mugged in the car park and having the chips cut out of their arms, but the operators say that this is an 'urban myth'. Dad, Gareth, who was considering joining up, was also worried as he had seen a television programme about the chips being attacked by computer viruses. He worried because the consequences of being suspected of fraud are much more serious now. Because of more sophisticated predictive algorithms based on individual consumer profiles, being called by the bank is now as good as being found guilty: cards are automatically deactivated, and the consumer is required to provide independent evidence of identity and location to the bank.

Data Flows

Data gathered by surveillance technologies flow around computer networks. Many people may consent to giving data in one setting, but what happens if those data are then transferred elsewhere? Yet there is already little knowledge either among the public or among data-sharing agencies about where exactly those data go.

Function Creep
Surveillance appears to operate by a logic of its own. But that logic needs to be questioned, examined and checked, particularly where data flows from one setting to another and information gathered for one purpose finds uses in new setting and for new purposes. An example is Oyster transport cards in London, where personal data about public transport use is increasingly required in police inquiries.[60] Now, not only are the same data-mining techniques developed for profiling consumers being used by security and intelligence services to profile potential terrorists, but often the very data from which these profiles are created are the same. Medical diagnostic technologies are gradually being allowed to creep towards broader and broader contexts, weakening their predictive qualities for positive diagnosis along the way: those falsely diagnosed may well be disadvantaged. In the workplace, employee monitoring technologies can sometimes yield more information than intended, and management has the temptation to extend monitoring practice without consulting employees, which can affect pay or promotion decisions.

Convergence
More and more systems are designed with these data flows in mind. Interoperability is built in and there is increasing convergence of surveillance technologies. This means that new products can emerge entirely unforeseen and unregulated. For example, pressure is now on to find ID cards that work for several purposes – border crossing, fraud control, access to government information and perhaps commercial (video rental) and semi-commercial ones (libraries) as well. This gives immense power over files whose information is essential to life-chances, to those controlling identity databases.

Towards Pervasive Surveillance
Technologies are at their most important when they become ubiquitous, taken for granted, and largely invisible. Increasingly, we face many different 'passage points' through which we must pass in our daily lives, involving *both* electronic and physical parts working closely together: a combination of CCTV, biometrics, databases and tracking technologies. Surveillance is increasingly everywhere, all the time: it is pervasive.

Social Sorting

In the surveillance society, 'social sorting' is endemic. In government and commerce large personal information databases are analysed and categorised to define target markets and risky populations.[61] Once classified, it is difficult to break out of the box. Since 9/11 such sorting may possibly have contributed to safety in the air (we shall never know), but it has certainly led to crude profiling of groups, especially Muslims, which has produced inconvenience, hardship and even torture.

Social sorting increasingly defines surveillance society. It affords different opportunities to different groups and often amounts to subtle and sometimes unintended ways of ordering societies, making policy without democratic debate. Invisible, taken-for-granted systems of congestion charging and intelligent public transit have their uses, but they both sort the city into groups that can travel relatively freely and others who find travel difficult. At the same time they can be used for crime control and national security. No one has voted directly for such systems. They come about through drives for greater efficiency and effectiveness in the public services, pressure from technology corporations, the rise of 'risk' as a key theme in society, and the idea that we should spare little effort to pre-empt dangers.

Keeping Tabs on Kids

By 2016, tagging and tracking have become an absolutely critical part of education.[62] Following a series of high-profile cases in which pupils were lost, injured or killed, many schools, particularly primary schools and even nurseries, became very concerned with keeping tabs on the whereabouts of their pupils to avoid being sued.[63] Primary schools began adopting drug testing, in response to government policy aimed at identifying problem children early, tackling poor attendance and improving concentration in class – important in the face of the ever-present league tables.[64] In Toby Jones' school, a cashless card system was introduced, with most families using it as a way of monitoring what their children ate. After three years, NSC, the supermarket, bought the cashless card company, seeing it as a way in to lucrative youth markets, building brand awareness by providing educational equipment. Parents were asked to swipe their child's card at the supermarket checkout, which identified the school, the pupil and the parent, and NSC would provide extra school equipment depending on how much the parent's bought. Some of NSC's key suppliers[65] began to install their vending machines in schools. Toby's school continued with the scheme, and every time some new equipment arrived, the prominent 'NSC' brand could easily be seen. The local education authority monitored the types of food being consumed in Toby's school, and used it to inform various 'healthy eating' campaigns they ran. The card gradually became more integrated, holding data not only on the children's meal purchases, but also on their attendance, record of achievement, extra-curricular activities, drugs test results and internet access, and were even used as part of students' citizenship class. While the increase of surveillance in schools brought measurable benefits to the schools and pupils themselves, children have gradually started to accept more and more intrusive surveillance, location tracking and the remote monitoring of what they eat and where they go as normal …

Technological Lock-in

There may also be some technological responses to surveillance: some so-called privacy-enhancing technologies (PETs) could help limit or curb surveillance and their use should be encouraged where appropriate. However neither failure, not PETs, should mean that the answer is merely 'better technologies'. The more that states, organisations, people and society at large become dependent on surveillance technologies, the more there is a 'lock-in' which prevents other options for achieving the same objectives from being considered, and also a comprehension gap which increases our dependence on expertise outside the democratic system. For example, once ID cards are introduced, the government's reliance on those providing both technological and commercial expertise will inevitably increase.

We should be wary of any offers to fix what are taken to be technical problems with technical solutions. As we shall see, the real world of surveillance society is far too complex for such superficial responses. We also have to ask whether the government has the necessary tools to carry out meaningful regulation of increasingly complex surveillance technologies and practices. Can the genie be put back into the bottle?

Technological Failure

Of course, the promise of technologies is almost never delivered quite as anticipated. The biometric technologies for the USVISIT programme, for example, were downgraded from planned iris scans to digital fingerprints for logistical reasons[66]. Similarly, the biometrics elements of the UK's e-Borders programme have been subject to problems of implementation[67]. Face recognition continues to underperform in real-world situations. The Criminal Records Bureau revealed that around 2,700 people have been wrongly identified as having criminal convictions and as a consequence of the incorrect information doubles, a number were refused jobs[68]. In the proposed UK ID system, it has been estimated that as many as one in six persons may not be able to use their ID cards because of the technical problems with enrolling them in the system.[69]

Such errors may limit access to places or services, but in other cases, for example in medical surveillance, they may be life-threatening, and they are far more common than most people realise. Technological failure or inadequacy can therefore result in worse outcomes for life chances than a successful system.

What are the Consequences of the Surveillance Society?

While the surveillance society provides us with benefits and rights, it also has negative consequences, some of which are stark and potentially irreversible. Any public debate about surveillance needs to consider its effects on privacy, ethics and human rights; its impact on social inclusion and exclusion; changes to levels of choice, power and empowerment; whether those running such systems can ever be held to account and whether surveillance processes are transparent or not.

Privacy, Ethics, Human Rights

Many of the current arguments about surveillance are based on ideas about 'privacy'. Since the 1970s, many data protection laws have been introduced in Europe and privacy law elsewhere. However it has proved difficult to persuade policy makers of any deeper *social* dimensions of privacy,[70] let alone of the need to confront other non-privacy problems associated with the surveillance society. In many cases people do not even know something is wrong, let alone have the ability to identify what it is, know where to take the complaint and how to find redress.

Privacy is vital, but surveillance society poses ethical and human rights dilemmas beyond this. Ordinary people should not be merely expected to have to protect themselves. Three key issues are as follows:

Social Exclusion, Discrimination

As we show in the full Report, surveillance varies according to place and in relation to social class, ethnicity and gender. Surveillance, privacy invasion and privacy protection differentiate between groups, benefiting some and disadvantaging others. Surveillance has grown alongside changes in health and welfare, and in many cases such state services have been reduced to mere risk management, which demands full knowledge of the situation. So personal data are sought in order to know where to direct resources.[71] And because surveillance networks permit so much joining-up, insurance companies can work with police, or supermarkets can combine forces with other data gatherers so much more easily. The results are that frequently police hot-spots are predominantly in non-white areas, and large supermarkets are located in upscale or out-of-town neighbourhoods, more easily reached by those with cars.

Total Social Solutions?

In 2016, residential areas are more clearly divided between gated private communities, such as the one where the Jones family live, patrolled and monitored by well-equipped corporate security firms, and former council estates and low-cost housing like the Dobcroft Estate. For the Joneses, the camera and identification systems in and around the community keep insurance costs to a minimum[72]. On the Dobcroft Estate, Yasmin's work in a multi-agency social work team has now been subcontracted to a private consortium called, optimistically, Total Social Solutions. TSS is paid to monitor and enforce the 'Personal Behaviour Schemes'[73] of which everyone on the Dobcroft Estate is a 'customer' from birth[74] (and some are identified even before[75]). Many of those on higher levels of PBS, such as probation[76], now have implanted active RFID chips which register automatically with sensors installed in their homes and at the entrances of the estate[77]. The implants are supposedly voluntary, but like the schemes in shops and schools, compliance brings rewards, not least of which is earlier release from probation. At the moment the whole Dobcroft Estate is also subject to one of its periodic 'area-wide curfews' after 'youths' from the estate were supposedly identified by an elderly woman from the Sunnyview Retirement Village as causing trouble. The woman spotted the suspicious activity on the local video surveillance cameras, all of which can be watched on the local security channels on digital TV, which also includes a 'rogues' gallery' of those who have known to have infringed their PBSs[78]. All under-18s are currently barred from entering or leaving the estate from 6pm until 6am.

Choice, Power and Empowerment

So what say can we have in facing the surveillance society? Ordinary people can and do make a difference, especially when they insist that rules and laws be observed, question the system or refuse to have their data used for purposes for which they have insufficient information or about which they harbour doubts.

But how far can individuals and groups choose their exposure to surveillance and limit the personal information that is collected and used? Surveillance systems are frequently too technical for non-experts to understand and are disappearing into the everyday structures and systems of society: at work, at leisure, in the home, in schools, in travel and communications and in the public services. It seems harder to make a significant difference. For instance, not until some identity theft scandal breaks do consumers become aware of the extent of personal profiling carried out by major corporations,[79] and even then the focus tends to be on security – how to prevent similar fraud – rather than on curbing the power of businesses and state agencies over data. Individuals are seriously at a disadvantage in controlling the impacts of surveillance.

Transparency, Accountability

Business, transport and government infrastructures all have mushrooming surveillance capacities, but individuals and groups find it difficult to discover what happens to their personal information, who handles it, when and for what purpose. Yet little by little, their personal data are used to help shape their life chances, to guide their choices. Accountability needs to be assumed within organisations, especially when high-powered surveillance occurs routinely, with potentially damaging consequences. We must shift from self-protection of privacy to the accountability of data handlers, in addition to the work of official regulators in enforcing controls and pressing for the minimisation of surveillance.

The Regulatory Challenge

Is it possible to regulate surveillance, to keep its negative effects under control, and to make it compatible with the kind of society and democracy we wish to have?[80] Requiring assessments to be made of the impact of new projects on privacy and surveillance would contribute to public awareness and debate, and would add an important dimension to regulatory systems. There are many laws and codes of practice for protecting privacy. There are also technologies that provide some protection. There are dedicated regulatory agencies that enforce laws, help with people's complaints, and seek influence over government policies and business developments. There are pressure groups and the media that alert us to the dangers of surveillance. But the power and effectiveness of these regulatory mechanisms is questionable; they need rethinking and improvement. In any case, while privacy protection is part of the story, it is not the whole story. More people need to understand surveillance and participate in deciding what, if anything, should be done about it so that it serves people properly. But it is not enough for regulation to take place only in one country, or even in a group of countries such as the European Union. The flows of information that are involved in surveillance are truly global; so are the movements and activities that are kept under surveillance. There is a need for more integrated, more global, regulation, in order to meet these challenges.

The Hall of Mirrors

While surveillance is everywhere in 2016, people, particularly those educated or wealthy enough to appreciate or afford it, are increasingly aware of it and able to find new ways of dealing with it. Gareth Jones is signed up to a personal information management service that monitors his 'data shadow' online, automatically corrects incorrect information held on public and some consumer databases and alerts him to further problems. His expensive handheld computer can also block advertising messages from retailers. But unfortunately not everyone is able to change and access their personal information equally. Those less skilled in personal information management or less able to pay for others to manage their information for them are at a severe disadvantage. Campaigners have managed to make it far easier to access and change personal information held by the state and private companies working for the state, but this access is one of the many things now made conditional on having an ID card. There is an increasingly uneasy and as yet unresolved stand-off between citizens and the state about who knows what, who owns data and who has the right to change data. But in 2016, people are more used to watching and being watched. Many voluntarily carry out whole-life surveillance, or life logging, recording almost everything they do and storing it or placing it straight online[81] in real time. There is a great deal of vigilante surveillance by hardliners who feel that the state is 'not doing enough' to control terrorism, crime and illegal immigration[82], and unofficial websites of the 'suspect' have proliferated, leading to all kinds of mistakes and misidentifications[83]. Protestors, artists and surrealists all play with and resist pervasive surveillance in all sorts of ways, including disabling public surveillance devices[84], using 'sousveillance' technologies that reflect or counter surveillance[85]. Some anti-capitalist activists like Aaron and Ben like to spend their Saturday afternoons slapping highly adhesive aluminium sheeting and tiny battery-powered microwave transmitters to the entrances of shops to disrupt wireless signals.[86] Life logging is also not all that it can seem, and with increasingly sophisticated data management and video production software, lives can be adjusted or even entirely created for purposes from pure entertainment through subversion to fraud. In 2016 there are increasing numbers of entirely virtual data shadows, who have no real-world counterpart, who appear to exist and are themselves the subjects of information management and online surveillance by automated systems working quietly and invisibly, inhabitants of an endless hall of mirrors …

References

Note: All web pages were accessible as of 1 September 2006.

[1] These glimpses of a possible future are taken from Section C of the full Report, which also includes a full 'Week in the Life' of a typical family in 2006.
[2] UAVs have been in use by the US military for some years: currently the best-known example is the 'Predator' reconnaissance drone aircraft used in Iraq; see: 'Predator RQ-1 / MQ-1 / MQ-9 Unmanned Aerial Vehicle (UAV), USA', *airforce-technology.com*, 2006, http://www.airforce-technology.com/projects/predator/ . Many uses have been suggested in the UK, see: Jha, A.,'On the horizon ... pilotless planes as fishermen's and firefighters' friends', *The Guardian*, 30 August 2006, http://www.guardian.co.uk/science/story/0,,1860825,00.html . In Los Angeles police are already experimenting with small remote control spy planes called 'SkySeer': Bowes, P., 'High hopes for drone in LA skies', *BBC News*, 6 June 2006, http://news.bbc.co.uk/1/hi/world/americas/5051142.stm .
[3] Major sporting events have had a history of being used for the testing and introduction of new surveillance technologies. For instance, on CCTV and the 2002 World Cup in Japan, see: Abe, K., (2004) 'Everyday policing in Japan: surveillance, media, government and public opinion', *International Sociology*, 19, 215–231; and on CCTV and the Athens Olympics, see: Samatas, M. (2004) *Surveillance in Greece*, Athens: Pella.
[4] See Crime and Justice and Infrastructure Expert Reports. One of the big problems with facial recognition had been the angle of view of CCTV cameras; see e.g.: Introna, L. and Wood, D. (2004) 'Picturing algorithmic surveillance: the politics of facial recognition systems', *Surveillance & Society*, 2(2/3): 177-198.
[5] Urban governance is already being turned over to public–private partnerships, Town Centre Management organisations (http://www.atcm.org/) and BIDs. According to the government, BIDs provide 'an investment in the local trading environment through the provision of added value services': http://www.ukbids.org/ . In 2016 one of the biggest regulation issues is information sharing between state and private security firms acting on behalf of or instead of the state, especially now the Police National Computer (PNC) links so many databases together, and now that police, probation, prison and social services are so interconnected.
[6] Many police services are already trialling these, see e.g.: 'Pocket computers put police 'in the picture'', *West Yorkshire Police*, 28 March 2006, http://www.westyorkshire.police.uk/section-item.asp?sid=12&iid=2226 , and the 'Airwave' scheme (see Crime and Justice Expert Report) is designed to build them in.
[7] Again, helmet cameras linked live to control rooms are being introduced in several areas already; see e.g.: 'Police use anti-yob head cameras', *BBC News*, 23 March 2006, http://news.bbc.co.uk/1/hi/wales/north_east/4836598.stm .
[8] In 2016, the police and their private allies have access to just about every database now linked by the PNC.
[9] In 2016, there are still arguments in the media and politics around the police doing this. But they argue that ID cards provide an easy way of determining someone's good faith and cannot take the risk of assuming the innocence of people who do not have one.
[10] Ford, R., 'Beware rise of Big Brother state, warns data watchdog', *The Times*, 16 August 2004, http://www.timesonline.co.uk/article/0,,2-1218615_1,00.html
[11] The full extent of surveillance on people's everyday lives is documented in Part C of the full Report.
[12] Figures derived from *SecurityStockWatch.com 100 Index*, August 2006: http://www.securitystockwatch.com/ .
[13] See, for example; 'The future of screening', *BBC News*, 14 December 2002, http://news.bbc.co.uk/1/hi/health/2570787.stm .
[14] McKie, R., 'Icelandic DNA project hit by privacy storm', *The Observer*, 16 May 2004, http://observer.guardian.co.uk/international/story/0,6903,1217842,00.html . Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database*, London: The Wellcome Trust.
[15] This is discussed in Lyon, D. *Surveillance after September 11*, Cambridge, UK: Polity Press, 45–48, 142ff.
[16] Garton Ash, T. (1997) *The File: A Personal History*, New York: Vintage.
[17] Cash transactions, for example, although usually unable to be linked to a consumer directly, are often analysed against similar past transactions and types of consumers who have made the same purchases.
[18] See Fink, J. and Kosba. A. (2000) 'A review and analysis of commercial user modeling servers for personalization on the world wide web', *User Modeling and User-Adapted Interaction*, 10, 209–249.
[19] The Wanless Report (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report*, London: HM Treasury.
[20] PITO (2005) *Police Information Technology Organisation, Annual Report 2004 – 2005*, HC 261, London: The Stationery Office.
[21] Randerson, J., 'DNA of 37% of black men held by police', *The Guardian*, 5 January 2006, http://www.guardian.co.uk/frontpage/story/0,,1678168,00.html .

[22] PITO (2006) *Facial Images National Database (FIND)*, http://www.pito.org.uk/products/FIND.php .
[23] ACPO (Association of Chief Police Officers**)** (2002) *Infinet: A National Strategy for Mobile Information*, Association of Chief Police Officers.
[24] Informal racial profiling undoubtedly already occurs and has occurred for a long time. It has also been suggested by UK police as a formal policy, see: 'No racial profiling by anti-terror police, says minister' *Times Online*, 2 August 2005, http://www.timesonline.co.uk/article/0,,22989-1717624,00.html . For background, see: 'Racial Profiling: Old and New', *ACLU*, http://www.aclu.org/racialjustice/racialprofiling/index.html .
[25] See the Borders Expert Report.
[26] The International Civil Aviation Authority agreed standards for Machine Readable Travel Documents (MRTDs) in 2004. This process has been driven by the current G8's Secure and Facilitated International Travel Initiative (SAFTI): 'G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel', *Statewatch*, 2004, http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm .
This is despite concerns over the ease of cloning of RFID chips: Johnson, B., 'Hackers crack new biometric passports', *The Guardian*, 7 August 2006, http://politics.guardian.co.uk/homeaffairs/story/0,,1838754,00.html . The fact that UK ID cards could easily morph into or merge with biometric passports has already been noted: Lettice, J., 'UK biometric ID card morphs into £30 'passport lite'', *The Register*, 8 July 2005, http://www.theregister.co.uk/2005/07/08/id_card_as_passport/ .
[27] See Consumer Expert Report. In 2016 there are still ongoing issues between states and outsourced border security about the intellectual property issues around travel data. The UK government maintains its 'right' to sell ID data, as was proposed in 2006: Elliot, F., 'ID plans: powers set to widen', *The Independent*, 6 August 2006, http://news.independent.co.uk/uk/politics/article1216000.ece . The only voice that still remains lost is that of the citizen.
[28] These full-body scanners come in several forms and are already being piloted, for example, the low-level X-ray-based Secure 1000 from Rapiscan: http://www.rapiscansystems.com/sec1000.html , tested at Heathrow airport, see: Lettice, J. ''See through clothes' scanner gets outing at Heathrow', *The Register*, 8 November 2004, http://www.theregister.co.uk/2004/11/08/heathrow_scanner_pilot/ ; and the millimetre-wave scanners being developed by QinetiQ, and tested by Eurotunnel: http://www.qinetiq.com/home/newsroom/news_releases_homepage/2004/3rd_quarter/Next_generation_security_screening.html .
[29] Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: the state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (AKA Interception Capabilities 2000)*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme.
[30] In 2016, most people now have these devices, which incorporate roaming wireless internet access, telephone services, computer navigation and more. The navigation function also ensures that the devices (and therefore their operators) are trackable.
[31] Galileo is the European civil alternative to the US military GPS system. The first satellite was launched in 2004 and some services will be operational by 2008, see: 'Galileo, European Satellite Navigation System' CEC Directorate General Energy and Transport, http://ec.europa.eu/dgs/energy_transport/galileo/intro/future_en.htm .
[32] The current Regulation of Investigatory Powers (RIP) Act allows limited record retention, but it is assumed that by 2016 police and security services will want remaining 'loopholes' closed, most probably in response to a some highly publicised scandal connected to terrorism or paedophilia.
[33] 'Cracking' refers to 'the act of breaking into a computer system', *The New Hacker's Dictionary*, http://www.outpost9.com/reference/jargon/jargon_toc.html
[34] MMOGs, by some estimates, currently have around 13 million subscribers, with the largest being *World Of Warcraft*, http://www.worldofwarcraft.com/index.xml , and the Korean game family, *Lineage I*, http://www.lineage.com/ , and *II*, http://www.lineage2.com/ . Other virtual worlds are more like analogues of the real world, and include *Second Life*: http://secondlife.com . They are becoming increasingly immersive and their economies intersect more and more with the real world, with items from the games being traded for 'real' money on auction sites such as *ebay*, http://www.ebay.com . See *MMOGCHART.COM*, http://www.mmogchart.com/ for some statistical analysis.
[35] There have already been some accounts of 'virtual surveillance'; see e.g.: 'Confessions of a Virtual Intelligence Analyst', *Terranova*, 15 March 2006,

http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html . Marketing analysts have already identified significant emerging virtual markets which means that companies are starting to target game worlds, see e.g.: Burns, E., 'Marketing Opportunities Emerge in Online Gaming Venues, *ClikZ*, 1 August 2006, http://www.clickz.com/showPage.html?page=3623035 , and the first 'virtual billboards' have already been launched, see: Shields, M., 'Massive Unveils Toyota Ad Units Within Anarchy', *Mediaweek*, 19 July 2006, http://www.mediaweek.com/mw/news/interactive/article_display.jsp?vnu_content_id=1002876380 .

[36] This was following a number of incidents over several years featuring spillover incidents from MMOGs and real-world crime; see e.g.: 'Chinese gamer sentenced to life', *BBC News*, 8 June 2005, http://news.bbc.co.uk/1/hi/technology/4072704.stm .

[37] McCahill, M. and Norris, C. (2003), 'Estimating the Extent, Sophistication and Legality of CCTV in London', in M. Gill (ed.) *CCTV*, Leicester: Perpetuity Press.

[38] Norris, C and Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford: Berg, 42.

[39] Norris, C. (2006) 'Closed Circuit Television: a review of its development and its implications for privacy', paper prepared for the *Department of Home Land Security Data Privacy and Integrity Advisory Committee* quarterly meeting, 7 June, San Francisco, CA.

[40] Gill, M. and A. Spriggs (2005). *Assessing the Impact of CCTV*. London: Home Office Research, Development and Statistics Directorate, 43, 60–61.

[41] Wilkins, G. and Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office; Ransford, F., Perry, D. Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, London: Home Office.

[42] McCahill and Norris, 2003, *op cit*.

[43] PA Consulting (2004) *Denying Criminals the Use of the Road*, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary .

[44] ibid.: 6.

[45] ibid.: 18.

[46] There are many potential schemes. See e.g.: Independent Transport Commission (2006) *Paying to Drive*, http://trg1.civil.soton.ac.uk/itc/p2d_main.pdf .

[47] A downside of this is that an organisation would only employ a particular type of person, and thus have a less diverse workforce – see Workplace Surveillance Expert Report.

[48] NPS (2006a) - National Probation Service - *Electronic Monitoring:* 6. http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes .

[49] The HDC scheme allows for those sentenced to between three months' but under four years' imprisonment to be released between two weeks and four and a half months early on a curfew enforced by electronic monitoring. In 2004/5 19,096 people were release early under the scheme (NPS, *op. cit*.:6).

[50] NPS, *op cit.*

[51] For details, see the Department of Environment, Food and Rural Affairs (DEFRA) PETS website: http://www.defra.gov.uk/animalh/quarantine/pets/index.htm .

[52] The company involved is Verichip Corporation: http://www.verichipcorp.com/ .

[53] Amal Graafstra is one such high-profile enthusiast and advocate of self-chipping. Explanations, pictures and videos can be downloaded from his website at http://amal.net/rfid.html .

[54] Graham-Rowe, D.,'Clubbers chose chip implants to jump queues', *New Scientist*, 21 May 2004, http://www.newscientist.com/article.ns?id=dn5022 .

[55] Waters, R., 'US group implants electronic tags in workers', *Financial Times*, 12 February 2006, http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html .

[56] The origin of the term 'brandscape' is defined by the UK Design Council as the 'The total experiential reach and engagement of a brand. A term that encompasses all those who touch and interact with the brand including customers, suppliers, employees, competitors, re-sellers, distributors, partners, etc': http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D_rPJLjJbFNakH0E0GQvlo&Document%5B@id%3D5232%5D/Chapter/@id=7 .

[57] The most valuable are determined by a credit check and reference to their consumer profile. Being a valuable customer means that you are likely to spend more. Implants become a status symbol.

[58] See Baja Beach (nd.) 'Zona VIP,' http://www.bajabeach.es/ .

[59] This will enable the database to record further individuals' particular choices.

[60] See 'Oyster data use rises in crime clampdown', *The Guardian*, 13 March 2006, http://politics.guardian.co.uk/foi/story/0,,1730771,00.html .

[61] See Oscar Gandy's classic study, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO: Westview, 1993.
[62] It is now in an embryonic form in the USA. See, e.g: Leff, L. 'Students ordered to wear tracking tags', *Associated Press*, 9 February 2005, http://www.msnbc.msn.com/id/6942751/ .
[63] See e.g.: 'Neglect ruling in girl pond death', *BBC News*, 23 March 2006, http://news.bbc.co.uk/1/hi/england/coventry_warwickshire/4837614.stm .
[64] In the UK, educational league tables rank schools according to the exam results of their pupils.
[65] For example Nestlé, Unilever, Pepsico, etc.
[66] United States Visitor and Immigrant Status Indicator Technology, in place at all land, air and sea ports of entry from 2004.
[67] See: Amoore, L. (2006) 'Biometric Borders: Governing Mobilities in the War on Terror', *Political Geography* 25(2): 336-351.
[68] 'Criminal records mix-up uncovered', *BBC News*, 21 May, 2006, http://news.bbc.co.uk/1/hi/uk/5001624.stm .
[69] See: Grayling, A.C. (2005) *In Freedom's Name: The Case against Identity Cards*, London: Liberty.
[70] See the excellent treatment of the sociality of privacy in: Regan, P. (1995) *Legislating Privacy*, Chapel Hill: University of North Carolina Press.
[71] See: Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.
[72] The Association of British Insurers (ABI) has called for this in a major report on housing: ABI(n.d.) *Securing the Nation: The Case for Safer Homes*, London: ABI, 12. http://www.abi.org.uk/BookShop/ResearchReports/Securing%20the%20Nation%20July%202006.pdf
[73] It is envisaged here that Anti-Social Behaviour Orders, Intensive Supervision Schemes and the like (see the Crime and Justice Expert Report) have all been standardised into general Personal Behaviour Schemes for those fitting certain patterns of risk of offending. Since all the residents of the Dobcroft Estate fit at least one criterion by the very fact of living on an estate where crime is likely to occur, they are all subject to PBSs.
[74] The growing enthusiasm for earlier intervention has already extended this far back in life, see e.g.: Woolf, M., ''Failures' targeted at birth', *The Independent*, 16 July 2006, http://news.independent.co.uk/uk/politics/article1180225.ece .
[75] So-called 'biocriminology', or the genetic aspects of criminal behaviour, are enjoying a revival of interest at the moment; see e.g.: Rose, D. (2006) 'Lives of crime', *Prospect* 125(August), http://www.prospect-magazine.co.uk/article_details.php?id=7604 . For an earlier critique of this approach, see: Rose, N. (2000) 'The biology of culpability: pathological identity and crime control in a biological culture', *Theoretical Criminology*, 4 (1), 5–34.
[76] By 2016, prison is now just another level of PBS. Social work, probation and prison are all now a continuum, and largely privately managed.
[77] Supposedly to improve security for the residents, the Dobcroft Estate was fenced in 2010, leaving only four entrances and exits, which are monitored by Community Support Officers, cameras and RFID scanners.
[78] Such a scheme was introduced as an experiment in Shoreditch in London in 2006. It was immediately dubbed 'ASBO TV', see e.g.: Swinford, S., 'Asbo TV helps residents watch out', *Times Online*, 8 January 2006, http://www.timesonline.co.uk/article/0,,2087-1974974,00.html .
[79] See the *New York Times* editorial: 'The data-fleecing of America', 21 June 2005.
[80] See Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd edn, Cambridge, MA: MIT Press.
[81]Life logging is developing out of web logging. Many technologies are already being developed to support it; see e.g.: Ward, M. 'Log your life via your phone', *BBC News*, 10 March 2004, http://news.bbc.co.uk/1/hi/technology/3497596.stm .
[82] See the Borders Expert Report, and e.g. the US Minutemen border security vigilantes: http://www.minutemanproject.com/ .
[83] This has already been noted in connection with the panic over paedophiles that resulted in a paediatrician being driven out of her home in 2000, see e.g.: Allison, R., 'Doctor driven out of home by vigilantes', *The Guardian*, 30 August 2000, http://www.guardian.co.uk/child/story/0,7369,361031,00.html . We simple assume that in 2016, technologies will allow such errors to circulate faster and more widely.
[84] Guides to such resistance already proliferate; see e.g.: 'Guide to Closed Circuit Television (CCTV) destruction', *Schnews*, http://www.schnews.org.uk/diyguide/guidetoclosedcircuittelevisionccctvdestruction.htm .
[85] See Mann, S., Nolan, J. and Wellman, B. (2004) 'Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments', *Surveillance & Society*, 1(3), 331–355.

[86] RFID is a line-of-sight technology. Interference can be achieved with microwaves, sheet metal, brick and even tree sap, see e.g.: 'RFID Technology', *RFID Centre*, http://www.rfidc.com/docs/rfid.htm .