Digitizing surveillance: categorization, space, inequality

Abstract

In this article, we seek to add to current debates about surveillance and society by critically exploring the social implications of a new and emerging raft of surveillance practices: those that specifically surround digital techniques and technologies. The article has four parts. In the first, we outline the nature of digital surveillance and consider how it differs from other forms of surveillance. The second part of the article explores the interconnections between digital techniques and the changing political economies of cities and urban societies. Here we explore the essential ambivalence of digital surveillance within the context of wider trends towards privatization, liberalization and social polarization. The third part provides some insights into particular aspects of digital surveillance through three examples: algorithmic video surveillance (in which closed circuit television systems are linked to software for the recognition of movement or identity); the increasingly prevalent practices of digital prioritization in transport and communications; and the medical surveillance of populations, wherein databases are created for increasingly mixed state and commercial medical purposes. Following this, in part four, we reflect on the policy and research implications raised by the spread of digital surveillance.

Key words: automation, biometrics, cities, ICTs, social exclusion

Introduction

Wherever there has been the creation and enforcement of categories, there has been surveillance. Historically, this was reinforced through religious and cultural norms. With capitalism and the modern state,
such practices were systematized through rational organization: bureaucracy, management and policing. Now a further shift is taking place away from those direct supervisory techniques famously analysed by Foucault (1975). Advances in the technologies of sensing and recording have enabled a massive growth in the monitoring of individuals and groups without the need for constant direct observation or containment of those monitored within particular spaces (Deleuze, 1992; Gandy, 1993; Lianos, 2001; Lyon, 1994, 2001; Poster, 1990). For Gary Marx (1988), this ‘new surveillance’ is characterized by ‘the use of technical means to extract or create personal data . . . taken from individuals or contexts’ (Marx, 2002: 12).

Our aim in this article is to critically explore the social implications of the digital within the ‘new surveillance’. Bureaucratic and electromechanical surveillance systems (a foundation for the modern nation state, public health and welfare) are being supplemented and increasingly replaced by digital technologies and techniques, enabling what Jones (2001) calls ‘digital rule’. Digitization is significant for two reasons: first, it enables monitoring, prioritization and judgement to occur across widening geographical distances and with little time delay (Lyon, 1994); second, it allows the active sorting, identification, prioritization and tracking of bodies, behaviours and characteristics of subject populations on a continuous, real-time basis. Thus, digitization encourages a tendency towards automation. Crucially, the work of human operators shifts from direct mediation and discretion to the design, programming, supervision and maintenance of automated or semi-automatic surveillance systems (Lianos and Douglas, 2000).

Digitization facilitates a step change in the power, intensity and scope of surveillance. Surveillance is everywhere. Computers are everywhere. Their combination already has that air of inevitability that can attach itself to the history of technology. Computer technology certainly is, as Henman (1997) argues, a player in social policy processes, but it is crucial not to read social and policy implications and effects of digital surveillance deterministically from the intrinsic capabilities of the technologies involved. As McCahill (2002) and Thrift and French (2002) demonstrate, such techniques are mediated, at all levels, by social practices that interact with all aspects of the making and functioning of the technological system. Even apparently automated systems, far from being inhuman domains, involve con-
tinuous complex social practices and decisions that do much to shape
digital surveillance in practice.

This is important because a characteristic of digital surveillance
technologies is their extreme flexibility and ambivalence. On the one
hand, systems can be designed to socially exclude, based on automated
judgements of social or economic worth; on the other hand, the same
systems can be programmed to help overcome social barriers and
processes of marginalization. The broad social effects and policy
implications of digital surveillance are thus contingent and, while
flexible, are likely to be strongly biased by the political, economic and
social conditions that shape the principles embedded in their design
and implementation.

Currently, these conditions are marked by the widespread liberali-
zation and privatization of public services and spaces. This reflects a
movement from free, universal public services and spaces, based on
notions of citizenship, to markets and quasi-markets based on con-
sumerism. These markets continually differentiate between users
based on ability to pay, risk or eligibility of access. While there is
clearly much variation and detail in particular cases, this broad
political-economic bias means that digital surveillance is likely to be
grounded overwhelmingly towards supporting the processes of individu-
alization, commodification and consumerization that are necessary to
support broader political-economic shifts towards markets, quasi-
markets and prioritized public services and spaces (see Graham and
Marvin, 2001).

This article seeks, in four parts, to explore the nature, scope and
implications of the growth of digital surveillance techniques and
technologies. In the first, we outline the nature of digital surveillance
and consider how it differs from earlier forms. We argue that, while
the changes may be considered merely quantitative (size, coverage,
speed, and so on), important new forms of social practice are
facilitated by these changes. The second part develops an exploratory
analysis of the interconnections between digitization and the
changing political economies of cities and urban societies. Here we
examine the essential ambivalence of digital surveillance within the
context of wider trends towards privatization, liberalization and social
polarization. We argue that the techniques may facilitate better
services for mobile, affluent citizens, but that this is often paralleled
by a relative worsening of the position of more marginalized groups.
who are physically or electronically excluded or bypassed by automated surveillance. The third part illustrates these points through three examples: algorithmic video surveillance; digital prioritization in transport and communications; and, finally, electronic patient records and genetic research. Finally, in part four, we reflect on the policy challenges raised by the spread of digital surveillance.

**Digital surveillance: making a difference?**

Digital encoding works by reducing information to the minimum necessary for accurate reconstruction: the binary code of 1s and 0s. In contrast, analogue forms aim at perfect reproduction of the original. Digital surveillance thus makes the information more amenable to storage, transmission and computation. But is it sufficiently different from analogue forms to merit rethinking and retheorization?

Michel Foucault’s (1975) concept of ‘panopticism’ (the tendency towards a disciplinary state based on direct surveillance) is still a dominant metaphor. However, Poster claims that digitization requires a re-evaluation of this concept because Foucault failed to notice that late 20th-century technological and infrastructural developments were qualitatively different from the earlier examples he studied:

Today’s circuits of communication and the databases they generate constitute a Superpanopticon, a system of surveillance without walls, windows, towers or guards. The quantitative advances in the technologies of surveillance result in a qualitative change in the microphysics of power. (Poster, 1990: 93)

Oscar Gandy argues that information age capitalism operates through a panoptic sort (the processes by which people are categorized and valued on the basis of information contained in databases), claiming:

it is only the locational constraints, the notion of separation by space, occasioned by the initial conceptualisation of the panoptic system as a building and by the surveillance as visual that limits Foucault’s construct. But in an age of electronic networks, virtual memory, and remote access to distributed intelligence and data, disciplinary surveillance is no longer limited to single buildings, and observations no longer limited to line of sight. (Gandy, 1993: 23)

Digital sorting results in the creation of subjects through databases that do not replicate or imitate the original subject, but create a
multiplicity of selves that may be acted upon without the knowledge of the original. These ‘dividuals’ (Deleuze, 1992) – or data subjects – are increasingly more important for social identity than bodily selves (Lyon, 2001; van der Ploeg, 1999, 2002).

The obvious differences between digital surveillance and analogue surveillance are quantitative: computer hard drives can store far more information more conveniently and faster than analogue systems. However, the fundamental differences lie in what can be done with the information gathered. There are two basic processes.

Norris and Armstrong (1999), in their study of closed circuit television (CCTV) in Britain, argue that what is of most concern is the linking of cameras to databases and the integration of different databases. Digitization facilitates interconnection within and between surveillance points and systems. To be truly effective, linkage is often required so that captured and stored data can be compared. Technological reasons will always be found to integrate. However, political and economic arguments are not always either presented, heard or assigned equivalent importance, and thus a covert process of ‘surveillance creep’ (Marx, 1988: 2) occurs, whereby integration is presented as necessary or inevitable.

Importantly, digital systems also allow the application of automated processes: algorithmic surveillance. An algorithm is a mathematical term for a set of instructions: algorithms are the foundation of mathematics and computing. However, algorithms need to be translated into a form that computers are programmed to understand, namely software – essentially many coded algorithms linked together. Algorithmic surveillance refers to surveillance systems using software to extend raw data: from classification (sensor + database 1); through comparison (sensor + database 1 + software + database 2); to prediction or even reaction (sensor + database 1 + software + database 2 + alarm/weapon).

Many of the latest surveillance technologies have embedded digital and algorithmic features. A city centre CCTV system providing images that are watched and analysed by human operators may be digitally recorded and stored, but is not algorithmic. If the system includes software that compares the faces of the people observed with those in a database of suspects, it becomes algorithmic. Patient records in a health service computer are digital and are algorithmic to the extent that software determines the format of the information entered. However, the process becomes algorithmic surveillance when,
for example, software compares patient records against signs of particular disease risk factors and categorizes patients automatically.

Some have claimed that algorithmic systems improve on conventional systems. Marx argues that algorithmic surveillance provides the possibility of eliminating the potential for corruption and discrimination (1995: 238). For example, a racist police officer cannot decide to arrest any black male when a facial recognition system can decide categorically whether a particular individual is the wanted man. However, algorithmic surveillance can also intensify problems of conventional surveillance and of computerization. Already, in social policy processes, ‘the perceived objectivity of computers is used to validate statistics which support partisan views’ (Henman, 1997: 335). Algorithmic systems also pose new questions, particularly relating to the removal of human discretion. In the most extreme cases, such as the development of movement recognition software linked to an automatic lethal response in certain commercially available perimeter defence systems (see Doucet and Lloyd, 2001; Wright, 1998), this can lead to death without explanation or appeal. Even in less immediately vital situations, for example one person’s Internet traffic secretly bypassing another's because of algorithmic prioritization, the consequences can nevertheless be serious and exclusionary.

It is critical to stress here the subtle and stealthy quality of the ongoing social prioritizations and judgements that digital surveillance systems make possible. This means that critical social policy research must work to expose the ways in which these systems are being used to prioritize certain people’s mobilities, service quality and life chances, while simultaneously reducing those of less favoured groups. Importantly, both beneficiaries and losers may, in practice, be utterly unaware that digital prioritization has actually occurred. This gives many of these crucial processes a curiously invisible and opaque quality that is a major challenge to researchers and policy makers alike.

Digital surveillance and the changing political economies of the city

As Thrift and French (2002) have shown, there are now so many software-based surveillance and IT systems embedded in the infrastructure of cities that even the UK Audit Commission had enormous
difficulties finding them all when trying to ensure that they would all function in the new millennium. They were often unable to discover who was responsible for them and how they could be checked and reprogrammed. Thrift and French (2002) claim that the ubiquity of such systems in the modern city is leading to the automatic production of space.

This opacity and ubiquity mean that it is hard to identify how the shift to automated, digital and algorithmic surveillance practices relates to current radical shifts in the political economies of welfare states, governance, punishment and urban space. Richard Jones (2001), following Deleuze (1992), argues that, as at-a-distance monitoring systems become intelligent and immanent within the city, so notions of traditional disciplinary control are replaced by the continuous electronic disciplining of subjects against redefined norms across time and space (see Graham, 1998).

Social, commercial and state definitions of norms of behaviour within the various contexts of the city are thus increasingly automatically policed by assemblages of digital technology and software. These are less and less mediated by human discretion (Lianos and Douglas, 2000). Normative notions of good behaviour and transgression within the complex space–time fabrics of cities are embedded into software codes. So, increasingly, are stipulations and punishments (for example, electronic tagging).

Increasingly, the encoding of software to automatically stipulate eligibility of access, entitlement of service or punishment is often done far away in time and space from the point of application (see Lessig, 1999). Software is coded across the world: call centres that monitor the gaze of automated cameras of electronic tags are switched to low-cost labour locations. Digital surveillance therefore promotes a new round of space–time distanciation, which moves us ever further from modern notions of discipline based on the gaze of supervisors within the same space–time as the disciplined subject (McCahill, 2002). Efforts are then made to enforce such norms and boundaries on the ground on a continuing, real-time basis through the withdrawal of electronic or physical access privileges, the detailed stipulation and monitoring of acceptable behaviours and the automated tracking of individuals’ space–time paths.

Within contemporary political-economic contexts marked by privatization and consumerization, this proliferation of automatic systems raises clear concerns that social exclusion itself will be
automated. Rather than being based exclusively on uneven access to the Internet, the digital divide in contemporary societies is based on the broader disconnections of certain groups from IT hardware and the growing use of automated surveillance and information systems to digitally red-line their life chances within automated regimes of service provision (Jupp, 2001). Such systems actively facilitate mobility, access, services and life chances for those judged electronically to have the correct credentials and exclude or relationally push away others (Norris, 2002). They thereby accelerate the trend away from persons towards data subjects. As Norris et al. suggest, the problem with automated systems is that ‘they aim to facilitate exclusionary rather than inclusionary goals’ (1998: 271). Algorithmic systems thus have a strong potential to fix identities as deviant and criminal – what Norris calls the technological mediation of suspicion (Norris, 2002). Lianos and Douglas note that this also means that challenging these identifications becomes harder because what they term ‘Automated Socio-Technical Environments’ (ASTE) ‘radically transform the cultural register of the societies in which they operate by introducing non-negotiable contexts of interaction’ (2000: 265).

Digital surveillance techniques therefore make possible the widening commodification of urban space and the erection within cities of myriad exclusionary boundaries and access controls. These range from the electronic tagging of offenders within their defined space–time domains to gated communities with pin number entry systems and shopping malls with intense video surveillance (Davis, 1990; Flusty, 1997). Digital surveillance systems also provide essential supports to the electronically priced commodification of road spaces; to digitally mediated consumption systems; and to smartcard-based public services – all of which allow user behaviours to be closely scrutinized. Crucially, the new digital surveillance assemblage is being shaped in a biased way to neatly dovetail with and support a new political economy of consumer citizenship and individualized mobility and consumption which would otherwise not be possible (Garland, 2001).

This is especially important within a context marked by the increasing privatization of public services, infrastructures and domains (with a growing emphasis on treating users differently based on assessments of their direct profitability). Digital surveillance also provides a new range of management techniques to address the widening fear of crime and the entrenchment of entrepreneurial
efforts to make (certain parts of) towns and city spaces more competitive in attracting investors and (selected) consumers.

**Digital surveillance and the city: three examples**

After this broad examination of the connections between digital surveillance techniques and the changing political economies of cities, we are in a position to examine the links between digital surveillance, exclusion and urban space in more detail. We do this via three examples: first, algorithmic CCTV; second, information, communication and mobility spaces; and, finally, genetic surveillance.

*Algorithmic CCTV*

Many systems of sorting and analysis can be linked to video surveillance, two examples being facial recognition and movement recognition. These are both biometric technologies, basing their categorization upon human bodily characteristics or traces (van der Ploeg, 1999, 2002).

In the UK, facial recognition software is being piloted in three metropolitan areas: Newham in London, Birmingham and Manchester (Meek, 2002). This technology is designed to compare the faces of individuals on the street with those of known offenders in databases. In both cases, the system used is FaceIt ARGUS, one of the most widespread of all facial recognition systems, produced by the US-based Identix Corporation (formerly Visionics).

FaceIt generates a ‘faceprint’, supposedly unique to each individual (see: http://www.visionics.com/faceit/whatis.html; no longer accessible). Using a series of different algorithms, it draws on relatively simple pattern matching to detect whether a face-like object is present and then whether the object is actually a face. Further algorithms create a normalized face, stripped of place- and time-specific light and shade, and so on. More complex algorithmic processes known as Local Feature Analysis are then used to create the 84-bit faceprint, a set of codes that can be stored in a database or matched against existing stored codes.

Identix says that FaceIt maps the intrinsic shape and features of the face and that the faceprint contains enough information to accurately distinguish an individual among millions of people (see:
http://www.identix.com/products/pro_faceit.html). This can then be used in many ways, from simple verification (checking that an individual is who they say they are) to real-time surveillance. According to previous Visionics publicity, ‘FaceIt can find human faces anywhere in the field of view and at any distance, and it can continuously track them and crop them out of the scene, matching the face against a watch list’ (see: http://www.visionics.com/faceit/tech/verif.html; no longer accessible).

Another developing area is movement recognition. Systems in use to detect motion and movement tend to be relatively simple, based on blobs of particular colours that remain constant in sampled frames of a CCTV image, such as the EU funded Cromatica project at King’s College, London (see: http://www.research.eee.kcl.ac.uk/vrl/#cromatica). This was designed for crowd flow management but, when piloted on the London Underground, attracted attention for its potential to help reduce the number of suicides, as it had been observed that the suicidal ‘tend to wait for at least ten minutes on the platform, missing trains, before taking their last few tragic steps’ (Graham-Rowe, 1999: 25, cited in Norris, 2002). In Orlando, Florida, another experimental system in a high crime neighbourhood claims to ‘detect . . . fires, or unusual body movements’ (Business Week, 2000: 16).

Gait recognition has also attracted significant media attention. Headlines like ‘The way you walk pins down who you are’ imply a reversion to Victorian notions of a visible criminal character (see: http://www.isis.ecs.soton.ac.uk/image/gait/press/). The reality is more prosaic, if still technically impressive. Researchers at the University of Southampton have been developing algorithms for the individual human gait. These (like faceprints) have the potential to be stored as information to be compared with existing images. It is perhaps even more complex than facial recognition, but, according to group leader Mark Nixon, ‘a distant silhouette will provide enough data to make a positive recognition once we get the system working properly’ (McKie, 1999). However, despite the publicity, the systems being developed have not progressed to the point of commercial use at this stage.

Certainty about identity is crucial to the argument for algorithmic CCTV: as was argued earlier, one of the main reasons for its increasing popularity is to counter arguments about human fallibility. But there are allegations that the technologies (and FaceIt in partic-
ular) simply do not work. Research by Norris and others (cited in Rosen, 2001) and by the _Guardian_ newspaper (Meek, 2002) shows that not a single arrest has been made as a result of the use of FaceIt in Newham and that the authorities overstated both the technological capability of the system and the size of their database of suspects. Until recently, it was relatively unusual for FaceIt to be used in live CCTV systems monitoring people moving freely in urban environments. By far its most common usage remains where movement is spatially restricted and a throughput of well-lit, similarly angled faces is guaranteed (entry systems, airport check-in areas, and so on). However, even in controlled conditions, failure rates of 53 percent have been identified at Palm Beach International Airport (Scheers, 2002). Justification for facial recognition has to fall back on arguments about deterrence that are dominant in UK policy discourses promoting CCTV (Norris and Armstrong, 1999). Such technical arguments should not, however, detract from fundamental questions about categorization and bypass. As described earlier, there are significant concerns about the way in which such systems rely on and reinforce the categorization of certain sociospatial risk categories: high crime neighbourhoods, known criminals or dangerous socioeconomic groups (Lianos and Douglas, 2000).

_Information, communication and mobility services in the city_

Our second range of examples involves the use of new information and communication technologies (ICTs) and digital surveillance to subtly differentiate consumers within transport, communications or service provision. Here, algorithms are being used at the interface of databases and telecommunications networks to allocate different levels of service to different users on an increasingly automated basis. This is done to overcome problems of congestion, queuing and service quality and to maximize the quality of service for the most profitable users. Examples include Internet prioritization, electronic road pricing, call centre call queuing and the use of biometrics to bypass international passport and immigration controls (see Graham and Marvin, 2001).

When the Internet first became a mass medium in the late 1990s it was impossible to give one user a priority service over another. All packets of data on the Internet were queued when there was congestion. However, on the commercialized Internet, dominated by transnational media conglomerates, new software protocols are being
embedded into the routers that switch Internet traffic. These smart routers automatically and actively discriminate between different users’ packets, especially in times of congestion. They can sift priority packets, allowing them passage, while automatically blocking those from non-premium users (Schiller, 1999).

Thus, high quality Internet and e-commerce services can now be guaranteed to premium users irrespective of wider conditions, while non-premium users simultaneously experience ‘website not available’ signals. This further supports the unbundling of Internet and e-commerce services, as different qualities can be packaged and sold at different rates to different markets (Graham and Marvin, 2001). As Emily Tseng suggests, ‘the ability to discriminate and prioritize data traffic is now being built into the [Internet] system. Therefore economics can shape the way packets flow through the networks and therefore whose content is more important’ (2000: 12).

The integration of customer databases within call centres provides another example of digital discrimination. Initially, call centres operated through the judgement and discretion of call centre operators. One system installed at South West Water in the UK in the mid-1990s, for example, meant that:

when a customer rings, just the giving of their name and postcode to the member of staff [a practice often now automated through call-line identification] allows all account details, including records of past telephone calls, billing dates and payments, even scanned images of letters, to be displayed. This amount of information enables staff to deal with different customers in different ways. A customer who repeatedly defaults with payment will be treated completely differently from one who has only defaulted once. (Utility Week, 1995: 12)

Now that call centres are equipped with Call Line Identification (CLI) allowing operators to detect the phone numbers of incoming calls, such practices are being automated. Automated surveillance systems are emerging that can differentially queue calls according to algorithmic judgements of the profits the company makes from them. ‘Good’ customers are thus answered quickly, while ‘bad’ ones are put on hold. As with Internet prioritization, neither user is likely to know that such prioritization and distancing are occurring.

New algorithmic techniques are also being used to reduce road congestion, while improving the mobilities of privileged drivers. With road space increasingly congested, electronic road pricing is an
increasingly popular political choice. A range of governments have brought in private or public/private regimes to either electronically price entry into existing city centres (for example, Singapore and, from February 2003, London) or build new private premium highways that are only accessible to drivers with in-car electronic transponders (including Toronto, Los Angeles, San Diego, Melbourne and Manila).

In both cases, road space becomes a priced commodity dependent on users having the appropriate onboard technology and resources – and often bank accounts – to pay bills. In some cases, systems allow traffic flow to be guaranteed whatever the level of external traffic congestion. On the San Diego I-15 highway, for example, software monitoring congestion levels on the premium-priced highway can signal real-time price increases when congestion causes the flow to decrease. Communicated to drivers, this reduces demand and reestablishes free flowing conditions.

While such systems have environmental benefits, it can also be argued that their implementation is closely related to the changing political economy of cities. This is because, like Internet prioritization and call centre queuing, they facilitate the removal of what might be called cash-poor/time-rich users from the congested mobility network, in the process facilitating premium network conditions for cash-rich/time-poor users (Graham and Marvin, 2001). The Hong Kong government, for example, recently discussed implementing a city centre road pricing system like that in Singapore. This was not to reduce greenhouse gas emissions; rather, it was a direct response to the lobbying of corporate CEOs who were sick of having to walk the last half mile to meetings in hot, humid conditions because of gridlock. These executives had grown used to a seamless door-to-door service, uninhibited by traffic in Singapore’s pricey central business district.

Finally, algorithmic surveillance now allows highly mobile, affluent business travellers to directly bypass normal immigration and ticketing at major international airports. This allows them to move seamlessly and speedily through the architectural and technological systems designed to separate airsides and groundsides within major international airports (Virilio, 1991: 10). For example, handscans for the most frequent business travellers are now in operation in major airports linking the US, the Netherlands, Canada and Germany and other OECD nations under the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS). Selected
premium travellers are issued with a smartcard that records their hand geometry: ‘Each time the traveller passes through customs, they present the card and place their hand in a reader that verifies their identity and links into international databases’, allowing them instant progress (Banisar, 1999: 67). By 1999, the scheme had 70,000 participants and the INS was planning to extend the system globally. Such systems extend the infrastructure of highly luxurious airport lounges and facilities only accessible to identified elite passengers.4 ICT surveillance assemblages privilege some users, while those deemed to warrant less (or no) mobility (especially illegal immigrants and refugees) face ever increasing efforts to make international boundaries less permeable through new border control systems.

Genetics and medical surveillance

Medicine, particularly public health and epidemiology, has a long history of surveillant practices, largely in the notification and monitoring of outbreaks of infectious disease (Declich and Carter, 1994; Foucault, 1973, 1975; Mooney, 1999). However, digitization is transforming these practices. Two linked cases will be mentioned here: first, electronic patient records (EPRs); and, second, research into genetics. As van der Ploeg (2002: 62) writes:

Health care systems throughout the Western countries are moving towards on-line accessible EPRs into which all data on medical history, medication, test results from a broad variety of diagnostic (often already computer based) techniques, and therapies belonging to a particular individual’s medical biography are accumulated, and can be accessed by relevant care givers.

EPRs are convenient and contribute to quick and accurate diagnosis of illness and, therefore, patient welfare and public health. However, they also gradually accumulate a mass of personal information, most of which has no direct relevance to any particular medical condition. Such records are protected by law and medical ethics but, as Mooney (1999) has shown in his analysis of debates about public health and privacy in the 18th and 19th centuries, personal rights can lose out to what is considered to be the public good – a slippery and amorphous notion. Regarding CCTV, the media outrage around the Jamie Bulger murder case in the UK led to a massive expansion of video surveillance without much public debate (Norris and Armstrong, 1999), and
one can easily imagine external issues like international terrorism or preventative genetics forcing a reconsideration of civil rights versus the public good. The pressure to integrate, for example, medical and police databases for law enforcement purposes will become more and more intense as forensic science improves and with the increasing popularity of biocriminology and the pressure for pre-emptive law enforcement policies such as DNA screening (Rose, 2000).

But it is not 1984-style fears of state surveillance that give most cause for concern; it is the increasing influence of the private sector in health care provision. The relationship between public database holders and the private sector is a key issue, one that is again complicated by digitization. Modern medical research, and in particular genetics, depends increasingly on high-powered computing. As Moor remarks, ‘it is . . . only through the eyes of computers that we can hope to map and sequence the human genome in a practical period of time’ (1999: 257).

Genetic records are also so readily digitizable that Nelkin and Andrews (1999) can give several examples of scientists predicting that smartcards with an encoded personal genome will soon replace current methods of personal identification. Progress towards the convergence of EPRs, personal genome records and private financial interests is already well underway. For example, leaked minutes of a high-level advisory group working towards a new health Green Paper by the UK Labour government show that the group proposes making the results of DNA sampling in NHS hospitals available to pharmaceutical companies (Barnett and Hinsliff, 2001). Iceland has licensed its entire national medical database to the American genetics company deCODE for research and commercial purposes (Rose, 2001) and Estonia is also planning a genetic database of its citizens (Pollack, 2000).

Once state EPRs are commodified, so prospects for democratic control over personal information decrease and the discriminatory potential multiplies. The insurance industry is just one domain that is being transformed by this increasing commodification (Cook, 1999; Pokorski, 1997). Insurance has serious implications for personal wellbeing when individuals are increasingly forced to find private health care and retirement solutions and rely less upon decreasing state provision. Those whose genetic records make them too financially risky for insurance companies could find themselves bypassed by neoliberal health policies. Moreover, mutualized life and health insurance systems, built up over centuries and based on the social
pooling of aggregate risks, threaten to be dismantled and individualized in the same ways as are the physical infrastructures of cities. Users defined through their genetic profiles as low-risk/high-profit could secede from generalized rates and gain low-cost cover, whereas those with high risks of long-term costly illness or early death could be excluded from cover (Graham and Marvin, 2001).

Conclusions: research, policy and resistance

As digital surveillance proliferates, the politics of surveillance are increasingly the politics of code. The processes through which algorithms and software are constructed are often now the only parts of the disciplinary chain completely open to human discretion and shaping. Once switched on, many digital systems become supervised agents that continually help to determine ongoing social outcomes in space and time (Lianos and Douglas, 2000).

The research challenges raised here are clear. Software for surveillance is often bought off the shelf from transnational suppliers. Critical researchers into digital algorithmic systems practices face an imperative to ‘get inside’ the production and implementation of code (Thrift and French, 2002). This might mean switching the focus of research to the social and political assumptions that software producers embed (unconsciously or consciously) into their algorithms years before and thousands of miles away from the site of application. Research is required to systematically track the sourcing, implementation and implications of digital surveillance in practice, across multiple spaces, as the code moves from inception to application. Such research also needs to address time, as another implication of digital surveillance is its use in decreasing the ability of people to escape deemed offences in the distant past (Blanchette and Johnson, 2002).

The policy implications of such research are complex and problematic. Digital surveillance systems tend to be developed, designed and deployed in ways that hide the social judgements that such systems perpetuate. Rates of technological innovation are rapid and policy makers face serious problems in simply understanding the esoteric and technical worlds of the new surveillance. Policy makers also face geographical and jurisdictional problems. Efforts to regulate and control digital surveillance are necessarily bound by the geographical jurisdictions that give them political legitimacy and power.
But social assumptions embedded in surveillance software in one context can have major ramifications in distant times and places. The practices of digitally sorting and sifting societies occur through globally stretched sociotechnical relations (Lyon, 2001).

Another major problem concerns the dominant policy approach to surveillance: the concept of privacy. Privacy is fundamentally embedded both in the Lockean notion of property and in the patriarchal dynamics of the household (Lyon, 1994). Its current politics are also dominated by the discourse of individualist, libertarian ‘cyberliberties’, which renders it inadequate to deal with complex sociogeographical polarization.

We believe that a strong regulatory approach, based on the principle of the mutual transparency of state and individual (see Brin, 1999), could simultaneously work at the many geographical scales at which social and economic regulation occurs. However, two current trajectories make this transparent society less than likely. The first is the post-9/11 climate. Currently, many western policy makers would consider such transparency politically unacceptable, particularly as pressures increase from the Right for decreasing civil liberties in the name of security (see Huber and Mills, 2002).

The second is that the new digital surveillance systems are being used to support the dominant neoliberal economic agenda (for example, the generalized privatization envisaged by the proposed General Agreement on Trade in Services) because they can allow the ‘unbundling’ of previously public infrastructures and spaces and support ‘pay per use’ and sophisticated consumer monitoring. As public, welfare and social service regimes restructure and are privatized or remodelled through various forms of ‘partnership’, the automated control and sifting capabilities of digital surveillance techniques are increasingly being utilized to support differentiated service regimes. These practices are closely modelled on those in the private sector; in many cases, private sector firms are colonizing public and welfare service regimes with precisely such practices.

Does this mean that the choice is for a critical response to digital surveillance to be bound by either cyberliberties, resistance to the ‘war on terrorism’ or anti-globalization struggles? Not necessarily — although placing the spread of digital surveillance within a wider political-economic critique is crucial. People do ‘refuse to disappear beneath the imperatives of spatial regulation that favors select target markets’ (Flusty, 2000: 156). Resistance exists in many forms, from
the playful guerrilla art of the Surveillance Camera Players (see: http://www.notbored.org/the-scp.html), the systematic anti-panopticism of the i-SEE project in New York, calculating ‘paths of least surveillance’ (Schenke and IAA, 2002; see: http://www.appliedautonomy.com/isee/), to the everyday practices of the targeted. In British towns, young black men have been shown to develop elaborate practices to exploit CCTV system ‘blindspots’ (Norris and Armstrong, 1999; Toon, 2000). Similarly, Flusty has shown how the excluded in LA work to exploit the gaps. One busker, for example, says he ‘knows where to find every security camera on Bunker Hill’ (Flusty, 2000: 152).

Resistance varies across policy domains; in health, outside professional disquiet, it has been minimal. While Iceland has at least provided mechanisms for public consultation on the role of deCODE (Rose, 2001), the UK government has shown no such inclination. The practices of insurance companies and health providers are similarly opaque, and, unlike the case of CCTV, there seems little space for individual acts of subversion.

Finally, we must stress that digital surveillance systems do have real limits. While the technologies are rapidly increasing their capabilities, they are often still not as reliable as their proponents claim. For example, facial recognition is still prone to misidentification, although the nature of these errors is in itself a matter of concern. In addition, the sheer diversity of identities, social worlds and political pressures in contemporary cities can quickly swamp crude efforts to impose simplistic notions of exclusion and purified urban order. Contemporary cities remain sites of jumbled, superimposed and contested orderings and meanings; they are ‘points of interconnection, not hermetically sealed objects’ (Thrift, 1997: 143). Multiple ‘spillovers’ can easily saturate and overwhelm simple attempts at establishing and maintaining ‘hard’ disciplinary boundaries. Virtually all boundaries remain to some extent porous and perfect control strategies are never possible.

Notes

1. Panopticism derives from Jeremy Bentham’s reformatory design, the panopticon, in which prisoners never knew whether or not they were being watched and would therefore modify their behaviour as if the surveillance was constant.
2. The word algorithm derives from the 9th-century Muslim mathematician Muhammed ibn Mūsā al-Khwārizmī. 12th-century Christian scholars used al-Khwārizmī’s name, latinized as Algorismus, to differentiate his method of calculation from commonly used methods like the abacus or counting tables. For more on the history of algorithms, see Chabert (1999).

3. This is changing, particularly since 9/11 (see Rosen, 2001).

4. As with facial recognition, such schemes are proliferating in the wake of 9/11, despite having no direct connection with the prevention of terrorism.

References


Stephen Graham is professor of urban technology at the University of Newcastle’s school of architecture, planning and landscape (SAPL) in the UK. His research interests centre on: the relationships between society and new technologies; urban and social theory; telecommunications and information technologies and cities; surveillance and the city; networked infrastructure, mobility and urban change; urban planning and strategy making; and the links between cities and warfare. His books include Telecommunications and the City: Electronic Spaces, Urban Places (with Simon Marvin; Routledge, 1996) and Splintering Urbanism: Technological Mobilities, Networked Infrastructures and the Urban Condition (with Simon Marvin; Routledge, 2001). Address: School of Architecture Planning and Landscape, University of Newcastle, Newcastle-upon-Tyne NE1 7RU, UK. email: s.d.n.graham@ncl.ac.uk

David Wood is Earl Grey postdoctoral research fellow at the University of Newcastle’s school of architecture, planning and landscape (SAPL) in the UK. His current project, ‘The Evolution of Algorithmic Surveillance and the Potential for Social Exclusion’, looks at the sociotechnical history and development of computer-mediated surveillance technologies. His other research interests include: geographies of military intelligence and orbital space; virtual spaces; and social theory. He is also the founder and managing editor of the new international journal of surveillance studies, Surveillance & Society (see: http://www.surveillance-and-society.org), part of a project to provide online surveillance studies resources. email: d.f.j.wood@ncl.ac.uk