Digitising Surveillance: Categorisation, Space, Inequality

Graham S; Wood D. Digitizing surveillance: Categorization, space, inequality. Critical Social Policy 2003,**23** 2 227-248.

Authors:

Stephen Graham, Professor of Urban Technology,

School of Architecture Planning and Landscape,

University of Newcastle upon Tyne, NE1 7RU.

s.d.n.graham@ncl.ac.uk

David Wood,

Earl Grey Postdoctoral Research Fellow,

School of Architecture Planning and Landscape,

University of Newcastle upon Tyne, NE1 7RU.

d.f.j.wood@ncl.ac.uk

Biographies

Stephen Graham is Professor of Urban Technology at Newcastle University'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 (1996) and Splintering Urbanism: Technological Mobilities, Networked Infrastructures and the Urban Condition (2001), both published through Routledge with Simon Marvin.
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 socio-technical 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, <www.surveillance-and-society.org> part of a project to provide online surveillance studies resources.
d.f.j.wood@ncl.ac.uk

Abstract

In this paper 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 which specifically surround digital techniques and technologies. The paper has four parts. In the first, we outline the nature of digital surveillance, and consider how digital surveillance differs from other forms of surveillance. The second part of the paper 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 privatisation, liberalisation and social polarisation. The papers third part provide 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 prioritisation 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.

Keywords

Biometrics; cities; automation; social exclusion; ICT

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 systematised through rational organisation: bureaucracy, management and policing. Now a further shift is taking place away from these 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 the monitored within particular spaces (Poster 1990; Deleuze, 1992; Gandy, 1993; Lyon, 1994, 2001; Lianos, 2001). For Gary Marx, this 'new surveillance' (Marx, 1988) is characterised by "the use of technical means to extract or create personal data… taken from individuals or contexts" (Marx, 2002: 12).

Our aim in this paper 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 has called 'digital rule' (Jones, 2000). Digitisation is significant for two reasons. Firstly, because it enables monitoring, prioritisation, and judgement to occur across widening geographical distances, and with little time delay (Lyon, 1994). Second, it allows the active sorting, identification, prioritisation, and tracking, of bodies, behaviours, and characteristics of subject populations, on a continuous, real time basis. Thus, digitisation 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).

Digitisation 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) argued, a player in social policy processes, but it is crucial not to read off 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) have demonstrated, such techniques are mediated, at all levels, by social practices, which interact with all aspects of the making and functioning of the technological system. Even apparently

automated systems, far from being inhuman domains, involve continuous complex social practices and decisions which 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 one hand, systems can be designed to socially exclude, based on automated judgements of social or economic worth. On the other, the same systems can be programmed to help overcome social barriers and processes of marginalisation. The broad social effects, and policy implications, of digital surveillance are thus contingent and, whilst flexible, are likely to be strongly biased by the political economic and social conditions which shape the principles embedded in their design and implementation.

Currently, these conditions are marked by the widespread liberalisation and privatisation of public services and spaces. This reflects a movement from free, universal public services and spaces, based on citizenship, to markets and quasi-markets based on consumerism. These markets continuously differentiate users based on ability to pay, risk, or eligibility of access. Whilst there is clearly much variation, and detail, in particular cases, this broad political economic bias means that digital surveillance is likely to be geared overwhelmingly towards supporting the processes of individualisation, commodification and consumerisation that are necessary to support broader political economic shifts towards markets, quasi-markets, and prioritised public services and spaces (see Graham and Marvin, 2001).

The paper seeks to explore the nature, scope and implications of the growth of digital surveillance techniques and technologies. It has four parts. In the first, we outline the nature of digital surveillance and consider how digital surveillance differs from earlier forms. We argue that, whilst the changes may be considered merely quantitative (size, coverage, speed etc.), 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 privatisation, liberalisation and social polarisation. 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 marginalised 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 prioritisation in transport and

communications; and, 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 retheorisation?

Michel Foucault's (1975) concept of 'panopticism'[1], the tendency towards a disciplinary state based on direct surveillance, is still a dominant metaphor. However Poster claimed that digitisation requires a re-evaluation of this concept, because Foucault failed to notice that late C20th 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 argued that information age capitalism operated through a panoptic sort – the processes by which people are categorised 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).

[1] Panopticism derives from Jeremy Bentham's reformatory design, the Panopticon, in which prisoners never know whether or not they were being watched, and would therefore modify their behaviour as if the surveillance was constant.

Digital sorting results in the creation of subjects through databases which do not replicate or imitate the original subject but create a multiplicity of selves which 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 (van der Ploeg, 1999, 2002; Lyon, 2001).

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. Digitisation 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, where 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[2]; algorithms are the foundation of mathematics and computing. However algorithms need to be translated into a form that computers have been programmed to understand, 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

[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 *et al.* (1999).

system includes software that compares the faces of people observed with those in a database of suspects, it becomes algorithmic. Patient records in a Health Service computer are digital, and 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 categorises patients automatically.

Some have claimed that algorithmic systems improve on conventional systems. Gary Marx argued that algorithmic surveillance has the potential to eliminate the potential for corruption and discrimination (Marx, 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). However algorithmic systems also pose new questions, particularly relating to the removal of human discretion. In the most extreme cases, for example the development of movement recognition linked to automatic lethal response in certain commercially available perimeter defence systems (see: Wright, 1998; Doucet and Lloyd, 2001), this can lead to death without explanation or appeal. However, even in less immediately vital situations – for example one person's Internet traffic secretly bypassing another's because of algorithmic prioritisation – the consequences can, nevertheless, be serious and exclusionary.

It is critical to stress here the subtle and stealthy quality of the on-going social prioritisations 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 prioritise certain peoples' mobilities, service quality and life chances, whilst simultaneously reducing those of those of less-favoured groups. Importantly, however, both beneficiaries and losers may, in practice, be utterly unaware digital prioritisation has actually gone on. 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 into the infrastructure of cities that even the UK Audit Commission had enormous difficulties just finding them all when trying to ensure that they would all function after Y2K. 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 means 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, 1997).

Social, commercial, and state based 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 code. So, increasingly, are stipulations and punishments (e.g.: 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 which monitor the gaze of automated cameras of electronic tags are switched to low-cost labour locations. Digital surveillance therefore promotes a new round of time-space distanciation, which moves us ever further from modern notions of discipline based on the gaze of supervisors within the same time-space 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 individual's time-space paths.

Within contemporary political economic contexts marked by privatisation and consumerisation, 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 to 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.* (1998) suggest, the problem with automated systems is that "they aim to facilitate exclusionary rather than inclusionary goals" (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 Automated Socio-Technical Environments (or (ASTEs) "*radically transform the cultural register of the societies in which they operate by introducing non-negotiable contexts of interaction*". (Lianos and Douglas 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 time-space 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 smart card based public services, all of which allow users behaviours to be closely scrutinised. Crucially, then, 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 individualised mobility and consumption, which would otherwise not be possible (Garland, 2001).

This is especially important within a context marked by the increasing privatisation 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 a 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 through three examples: algorithmic CCTV; information, communication and mobility spaces; and genetic surveillance.

Algorithmic CCTV

Many systems of sorting and analysis can be linked to video surveillance: two examples are facial recognition and movement recognition. These are both *biometric* technologies, basing their categorisation 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 US-based Identix Corporation (formerly Visionics).

FaceIt generates a 'faceprint', supposedly unique to each individual[3]. It uses a series of different algorithms. First, 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 normalised face, stripped of place and time-specific light and shade etc. 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 say that *FaceIt* maps the intrinsic shape and features of the face, and that the faceprint contains enough information to accurately distinguish an individual amongst millions of people[4]. 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

---

3 What is FaceIt? 2001 Visionics website. <http://www.visionics.com/faceit/whatis.html> Accessed 21/11/2002. Site no longer accessible.

4 FaceIt Face Recognition Software. 2002 Identix Website. <http://www.identix.com/products/pro_faceit.html> Accessed 01/11/2002.

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"[5].

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[6]. This was designed for crowd flow management, but when piloted on the London Underground, attracted attention for its potential to help reduce the numbers 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: 23, quoted in Norris, 2002). In Orlando, Florida, another experimental system in a high crime neighbourhood claims to "detect… fires, or unusual body movements" (*Economist* 2000: 16).

Gait recognition has also attracted significant media attention. Headlines like "The way you walk pins down who you are"[7] implied a reversion to Victorian notions of visible criminal character. 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 to existing images. It is perhaps even more complex than facial recognition, but according to as 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 was to counter arguments about human fallibility. But there are allegations that the technologies, and *FaceIt* in particular, 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

---

5 Verification. 2001 Visionics website. <http://www.visionics.com/faceit/tech/verif.html> Accessed 21/11/2002. Site no longer accessible.

6 Cromatica Project website. 1999. <http://www.research.eee.kcl.ac.uk/vrl/#cromatica> Accessed 21/11/2001

7 Press Reports on Gait Recognition at Southampton. 2001. ISIS website. <http://www.isis.ecs.soton.ac.uk/image/gait/press/> Accessed 01/11/2002.

used in live CCTV systems monitoring people moving freely in urban environments, by far its most common usages remain where movement is spatially restricted and a throughput of well-lit, similarly angled faces is guaranteed (entry systems; airport check-in areas etc.)[8]. However even in controlled conditions, failure rates of 53% have been identified at Palm Beach International Airport (Scheers, 2002). Justification for facial recognition has to fall back on arguments about deterrence, dominant in UK policy discourses promoting CCTV (Norris and Armstrong, 1999). However such technical arguments should not detract from fundamental questions about categorisation and bypass. As described earlier, there are significant concerns about the way in which such systems rely on and reinforce the categorisation of certain socio-spatial risk categories: high crime neighbourhoods, known criminals or dangerous socio-economic 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 communications 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 maximise the quality of service for the most profitable users. Examples include Internet prioritisation, 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 commercialised 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, whilst 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, whilst non-premium users

[8] This is changing, particularly since 9/11 (see Rosen, 2001)

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 practise 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)

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 system are emerging which can differentially queue calls according to algorithmic judgements of the profits the company makes from them. Good customers are thus answered quickly whilst bad ones are put on hold. As with Internet prioritisation, neither user is likely to know that such prioritisation and distancing is occurring.

New algorithmic techniques are also being used to reduce road congestion, whilst improving the mobilities of privileged drivers. With road space increasingly congested, electronic road pricing is an ever more popular political choice. A range of governments have brought in private or public private regimes to either electronically price entry into existing city centres (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, LA, San Diego, Melbourne and Manila).

In both cases, road space becomes a priced commodity dependent on users having appropriate onboard technology, and the 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 flow to decrease. Communicated to drivers, this reduces demand and reinstates free flowing conditions.

Whilst 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 prioritisation 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 Government of Hong Kong, for example, recently discussed implementing a city centre road pricing system like that in Singapore. This was not to reduce greenhouse gas emissions. Instead, 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 seamless door-to-door service uninhibited by traffic in Singapore's priced CBD.

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 air-side and ground-sides within major international airports (Virilio, 1991: 10). For example, hand-scans 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 smart card 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). 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[9]. ICT surveillance assemblages privilege

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

some users whilst 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, have a long history of surveillant practices, largely in the notification and monitoring of outbreaks of infectious disease (Foucault, 1973, 1975; Declich and Carter, 1994; Mooney, 1999). However, digitisation is transforming these practises. Two linked cases will be mentioned here: the first is that of the Electronic Patient Record (EPR), and the second, research into genetics.

As van der Ploeg (2002) 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 individuals 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 the 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 through law and medical ethics, but, as Mooney (1999) has shown in his analysis of debates about public health and privacy in the C18th and C19th, personal rights can lose out to what is considered to be the public good, a slippery and amorphous notion. For CCTV, the media outrage around the Jamie Bulger murder case led to a massive expansion of video surveillance without much public debate (Norris and Armstrong, 1999), and one can easily imagine outside 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 given 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, and is again complicated by digitisation. 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" (Moor, 2000: 257)

Genetic records are also so readily digitisable 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, are already well under way. For example, leaked minutes of a high-level advisory group working towards a new Health Green Paper by the UK Labour government showed that the group proposes making results of DNA sampling in NHS hospitals available to pharmaceutical companies (Barnett and Hinsliff, 2001). The state of Iceland has licensed its entire national medical database to 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 (Pokorski, 1997; Cook, 1999). Insurance has serious implications for personal well-being when individuals are increasingly forced to find private healthcare 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, mutualised life and health insurance systems, built up over centuries based on the social pooling of aggregate risks, threaten to be unbundled and individualised in the same ways that the physical infrastructures of cities. Users defined through their genetic profiles as low risk / high profit could secede from generalised 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 which continually help to determine on-going 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 embedded (unconsciously or consciously) into their algorithms years before (and thousands of miles away) from the site of application. Research is required which systematically tracks 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 decrease the ability of people to escape deemed offences in the distant past (Blanchette and Johnson, 2002).

The policy implications of such research are likely 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 which 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 discourses of individualist libertarian ‘cyber-liberties’, which renders it inadequate to dealing with complex socio-geographical 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 generalised privatisation envisaged by the proposed General Agreement on Trade in Services (GATS) – because they can allow '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 privatised, or are being remodelled through various forms of 'partnership', the automated control and sifting capabilities of digital surveillance techniques are increasingly being utilised to support differentiated service regimes. These practices closely modelled on those in the private sector ; in many cases, private sector firms are colonising public and welfare service regimes with precisely such practices..

Does this mean that the choice is for critical response to digital surveillance to be bound with either cyber-liberties, resistance to the 'war on terrorism' or with anti-globalization struggles? Not necessarily – although placing the spread of digital surveillance with 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[10], the systematic anti-panopticism of the i-SEE project in New York, calculating 'paths of least surveillance' (Schenke and the IAA, 2002)[11], 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, Steven 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).

[10] Surveillance Camera Players Website. 2002. <http://www.notbored.org/the-scp.html> Accessed 01/11/2002
[11] i-SEE website. http://www.appliedautonomy.com/isee/

Resistance varies across policy domains. In health, outside professional disquiet, it has been minimal. Whilst the Icelandic state 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. Whilst the technologies are increasing their capabilities quickly, often they are still not nearly 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 as sites of jumbled, superimposed and contested orderings and meanings ; they are "points of interconnection, not hermetically sealed objects" (Thrift, 1997: 143). Multiple 'spill-overs' 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.

References

Banisar, D. (1999) Big brother goes high tech, *Covert Action Quarterly*, 67.

Barnett, A and G. Hinsliff (2001) Fury at plan to sell off DNA secrets, *Observer*, 23rd September. <http://www.guardian.co.uk/Archive/Article/0,4273,4262710,00.html> Accessed 01/11/2002.

Blanchette, J-F., and Johnson, D. (2002) Data retention and the panoptic society: The social benefits of forgetfulness, *The Information Society*, 18: 33-45.

Brin, D. (1999) *The Transparent Society*, New York: Perseus.

Business Week (2000) Nobody's watching your every move, 3707, November 13th: 16.

Chabert, J. (ed.) (1999) *A History of Algorithms*, Berlin: Springer-Verlag.

Cook, E.D. (1999) Genetics and the British insurance industry, *Journal of Medical Ethics* 25, 157-162.

Davis, M. (1990) *City of Quartz*, London: Verso.

Declich, S. and A.O. Carter (1994) Public health surveillance: historical origins, methods and evaluation, *Bulletin of the World Health Organisation* 72: 2, 285-304.

Deleuze, G. (1992) Postscript on the societies of control, *October* 59: 3-7.

Doucet, I. and R. Lloyd (eds.) (2001) *Alternative Anti-Personnel Mines*, London / Berlin: Landmine Action / German Initiative to Ban Landmines.

Flusty, S. (1997) Building paranoia. In N. Ellin (ed.) *Architecture of Fear*, New York: Princeton Architectural Press, 47-60.

Foucault, M. (1973) *The Birth of the Clinic*, London: Tavistock.

Foucault, M. (1975) *Discipline and Punish*, New York: Vintage.

Gandy, O. H. Jr. (1993) *The Panoptic Sort*, Boulder CO: Westview Press.

Garland, D. (2001) *The Culture of Control*, Oxford: Oxford University Press.

Graham, S. (1998) Spaces of surveillant-simulation: New technologies, digital representations, and material geographies, *Environment and Planning D: Society and Space*, 16: 483-504.

Graham, S. (2000) Constructing premium networked spaces: Reflections on infrastructure networks and contemporary urban development, *International Journal of Urban and Regional Research,* 24 (1): 183-200.

Graham, S. and S. Marvin (2001) *Splintering Urbanism*, London: Routledge.

Graham-Rowe, D. (1999) Warning! Strange Behaviour, *New Scientist*, 2216, 11th December: 25-28.

Henman, P. (1997) Computer technology - a political player in social policy processes, *Journal of Social Policy* 26(3): 323-340.

Hill, R. and J. Bessant (1999) Spaced-out? Young people's agency, resistance and the public sphere, *Urban Policy and Research*, 17(1): 41-49.

Huber, P. and M.P. Mills (2002) 'How technology will defeat terrorism', *City Journal* 12(1). < http://www.city-journal.org/html/12_1_how_tech.html> Accessed 01/11/2002.

Jones, R. (2001) Digital rule: Punishment, control and technology, *Punishment and Society,* 2(1): 5-22.

Jupp, B. (2001) *Divided by Information?* London: Demos.

Lessig, L. (1999) *Code -- And Other Laws of Cyberspace*, New York: Basic Books.

Lianos, M. (2001) *Le Nouveau Contrôle Social*, Paris : L'Harmattan.

Lianos, M. and M. Douglas (2000), Dangerization and the end of deviance: the institutional environment, *British Journal of Criminology*, 40: 264-278.

Lyon, D. (1994) *The Electronic Eye*, Cambridge: Polity Press / Blackwell.

Lyon, D. (2001) *Surveillance Society*, Buckingham: Open University Press.

McCahill, M. (2002) *The Surveillance Web*, Cullompton: Willan.

Marx, G.T. (1988) *Undercover*, Berkeley: University of California Press.

Marx, G.T. (1995) The Engineering of Social Control: The Search for the Silver Bullet, in J. Hagan and R. Peterson (eds.) *Crime and Inequality*, Stanford, CA: Stanford University Press.

Marx, G.T. (2002) 'What's new about the 'new surveillance'? Classifying for change and continuity', *Surveillance & Society* 1(1): 9-29. <http://www.surveillance-and-society.org>

McKie, R. (1999) The way you walk pins down who you are, *Observer*, 12 December. <http://www.guardian.co.uk/Archive/Article/o,4273,3941021,00.html> Accessed 01/11/2002.

Meek, J. (2002) Robo-cop, *The Guardian*, 13 June. <http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html> Accessed 01/11/2002

Mooney, G. (1999) Public health versus private practice: the contested development of compulsory disease notification in Late Nineteenth Century Britain, *Bulletin of the History of Medicine* 73(2): 238-267.

Moor, J.H. (1999) Using genetic information while protecting the privacy of the soul, *Ethics and Information Technology* 1: 257-263.

Nelkin, D. and L. Andrews (1999) DNA identification and surveillance creep, *Sociology of Health and Illness* 21(5): 689-706.

Norris, C. (forthcoming 2002) From personal to digital: CCTV, the Panopticon and the technological mediation of suspicion and social control, in D. Lyon (ed.) *Surveillance as Social Sorting*, London: Routledge.

Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society*, Oxford: Berg.

Norris, C., J. Moran, and G. Armstrong (1998), Algorithmic Surveillance: the Future of Automated Visual Surveillance, in C. Norris, J. Moran and G. Armstrong (eds.), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate.

Pokorski, R.J. (1997) Insurance underwriting in the genetic era, Workshop on Heritable Cancer Syndromes and Genetic Testing, Supplement to *Cancer* 80(3): 587-599.

Pollack, A. (2000) Gene hunters say patients are a bankable asset, *Guardian*, 2nd August. <http://www.guardian.co.uk/Archive/Article/0,4273,4046698,00.html> Accessed 01/11/2002.

Poster, M. (1990) *The Mode of Information*, Cambridge: Polity Press.

Rose, H. (2001) *The Commodification of Bioinformation*, London: The Wellcome Trust. <http://www.wellcome.ac.uk/en/images/hilaryrose1_3975.PDF> Accessed 01/11/2002.

Rose, N. (2000) The biology of culpability: pathological identity and crime control in a biological culture, *Theoretical Criminology* 4:1, 5-34.

Rosen, J. (2001) A watchful state, *New York Times*, 7 October. <http://query.nytimes.com/search/article-page.html?res=9505E4DE123DF934A35753C1A9679C8B63> Accessed 01/11/2002.

Scheers, J. (2002) Airport face scanner failed, *Wired News*, 16 May. <http://www.wired.com/news/privacy/0,1848,52563,00.html> Accessed 01/11/2002.

Schiller, D. (1999), *Digital Capitalism : Networking the Global Market System,* Cambridge, MA , MIT Press.

Thrift, N. (1997), Cities without modernity, cites with magic, *Scottish Geographical Magazine,* 113(3): 138-149.

Thrift, N. and S. French (2002) The automatic production of space, *Transactions of the Institute of British Geographers*, 27(4): 309-335.

Toon, I. (2000) 'Finding a place on the street' : CCTV surveillance and young people's use of urban public space. In D. Bell, and A. Haddour (eds.) *City Visions,* London: Longman. 141-165.

Tseng, E. (2000), The geography of cyberspace. Mimeo.

Utility Week (1995), *Special Issue - IT in Utilities*, November 19th.

van der Ploeg, I. (1999) Written on the body: biometrics and identity, *Computers and Society* 29:1, 37-44.

van der Ploeg, I. (forthcoming 2002) Biometrics and the body as information: normative issues of the socio-technical coding of the body, in D. Lyon (ed.) *Surveillance as Social Sorting*, London: Routledge.

Virilio, P. (1991), *The Lost Dimension*, New York: Semiotext(e).

Wright, S. (1998) *An Appraisal of the Technologies of Political Control*, Luxembourg: European Parliament, The STOA Programme.

Young, J. (1999), *The Exclusive Society,* London: Sage.