Welcome to the Software-Sorted Society

Professor Stephen Graham, *of Durham University, analyses the extent to which society has become subject to visible and invisible surveillance, tracking, and sorting technologies. He draws attention to the radical and divisive social consequences of 'software-sorting' and calls for public regulation of the systems that are coming to pervade so many aspects of our lives.*

Introduction: cities of passage points

Our cities and infrastructures are rapidly becoming sentient. Infused with a wide range of digital sensors and surveillance systems, the built environments and infrastructures of cities are being produced and managed in ways which were unthinkable only a few years ago. Organised through millions of electronic tags, cards, transponders, mobile phones, computers and CCTV cameras, the movements and interactions that constitute urban life are now tracked and monitored like never before. In many ways, city spaces and infrastructures can now be thought of as structures of pervasive and continuous surveillance. These are widely being used not just to keep an eye out for threats and risks, but automatically to sort and prioritise the life chances of people based on judgements embedded in computer software.

In a typical day, the average Briton must now negotiate a seemingly endless series of high-tech systems which are sunk into the wider environment. Even the most banal communication, transaction or even physical movement now requires use of a whole list of passwords, PIN numbers or electronic cards to be successfully completed.

Such systems act as a myriad of electronic and physical passage points strung out across Britain's geographical landscapes. Through the inputting of a code, or the automatic scanning of a person, vehicle, card or tag, these systems try to separate people deemed legitimate from those deemed irregular or risky. They are also the basis for allocating rights and privileges to some, whilst witholding them from others.[1] It's no wonder that, in a recent book, the social critic Jeremy Rifkin argued that we live in what he called an 'age of access', where computerised systems continually mediate access to essential services, infrastructures and spaces through increasingly intense surveillance.[2]

Understanding passage points

Such passage points vary considerably. They do so in three main ways.

Visibility. Some passage points are highly visible and obvious, and must be negotiated willingly and knowingly by users. The PIN credit card machine or airport passport control are examples here. Others are more stealthy and covert (as with the widespread sorting of traffic to ease congestion on the internet or at call centres). Stealthy passage points force users to negotiate surveillance unknowingly, as a hidden background to their everyday life and movement.

On still other occasions, the presence of some form of passage point is clear to those who look for it — as with a CCTV camera on a street or a speed camera on a motorway. But it is impossible to know in practice if one's face or car number plate has actually been scanned, or if the legality or legitimacy of one's movement has been assessed.

Automation. Whilst most passage points are now fully automated, and involve little immediate human supervision, some have so far managed to resist full automation and still involve human discretion. Traditional CCTV control rooms, with the human operator using their 'Mk1 eyeball' to scan for misdemeanours or suspects, are a good example here. (But, as we shall see, digital CCTV that uses software to select the 'targets' of surveillance is emerging fast.)

Effectiveness. This depends largely on how difficult it is comprehensively to control access to the service, infrastructure, or city space in question without the controls being challenged, resisted, or swamped by unwieldy amounts of traffic. Generally, electronic services and realms are relatively easy to control compared to physical urban streets. (Of course, in software-sorted cities, most passage points now involve both electronic and physical parts working closely together.)

Within these differences, all passage point systems also have key similarities.

- Direct human operation is diminishing rapidly as they become increasingly automatic. This occurs because computer software actually does the day-to-day work scanning and sifting people and their traffic.
- They all more or less work 24 hours a day.
- They operate in real time (i.e. the decision by the software to allow access to the space, service or infrastructure is made with very little delay).

Given the proliferation of electronic passage points, and the way in which they increasingly mediate access to the crucial services people now need to lead their lives, the simple question arises: what is going on here? How has our society been remodelled in the last decade or so that everyday life emerges as an endless series of high-tech passage points, scrutinised by unseen databases, and disciplined through computers whose actual location is usually impossible to know? And what does it mean for social and geographical inequality in our society that our lives are mediated by computer software which stipulates automatically who is allowed access to the services, transport and communication networks, and urban spaces necessary to sustain a meaningful life in today's society, and, of course, who is not?

In a recent project, supported by a British Academy Research Readership, I sought to

start to uncover the largely invisible world through which British society is being sorted by software. The project had two starting points.

Beyond the glitz: rethinking the 'digital divide'

New Information and Communications Technologies (ICTs), like mobile phones, the internet and e-commerce systems, are almost always portrayed in the media and popular press as magical means of overcoming the barriers of time and space that shape urban life. The dominant depiction of the so-called 'information society' portrays such technologies as new, friction-free means of connecting people, institutions and spaces, which speed up and improve the functionality of all manner of services in the process. Bill Gates talks about 'friction-free' capitalism. Frances Cairncross announces 'the death of distance'. And Charles Leadbetter argues that we are now 'living on thin air' in a society where the incredible ease of electronic interaction and communication contrasts all too starkly with our increasingly congested physical world.[3]

And yet, when one studies the remaking of society through electronic passage points, one comes to a decidedly different view of new technologies. Here, it emerges that electronic and 'virtual' technologies are not separated off from the 'real' world in a simple, binary way. Nor are they closed off in a purely immaterial domain of cyberspace, with its perfect and friction-free mobilities and infinite possibilities. Instead, new technologies are very definitely diffusing into the material world of cities and infrastructures, allowing them to be radically remade in the process.

Such a view also reveals that, beneath the seductive glitz and glamour of high-technologies, in many cases their proliferation is actually being widely used to create disconnections as much as connections, as they are used to set up new passage point systems. Rather than a utopian world of ubiquitous electronic freedom, such systems are being used to slow down and add friction to certain peoples lives, making them logistically more difficult. And in some cases they are actually being used to facilitate the withdrawal of services from people and communities and the worsening of some people's opportunities.

Consequently, the so-called 'digital divide' which characterise high-tech societies are not just about the usual focus of debate – uneven access to the internet. Perhaps even more important, but almost completely unnoticed, are the powerful and often invisible processes of prioritisation and marginalisation that emerge as computer software is used in electronic and physical passage points to judge people's worth, eligibility and levels of access to a whole range of essential urban spaces, infrastructures and services.

Above all, the shift to a society of electronic passage points sorted by computer software means that people are continually having to justify passage or access, or have electronic codes do this for them. For generally powerful and privileged people or places, this access tends to open up a world of rapid communication, premium transport, and privileged service. Such offerings, however, are being made through the way these very same systems simultaneously inhibit or undermine the services and life chances of more marginalised people and places in our society. Quite literally, their traffic is electronically held up, or even stopped altogether, to allow service providers to concentrate on meeting the needs and desires of the powerful, privileged and profitable parts of our society.

'The most profound technologies are those that disappear'

The second starting point for the project was that the technologies that use software to sort British society remain largely invisible, mysterious, and unnoticed. Increasingly, they are literally sunk into the wider environment of our cities, homes, neighbourhoods, transport systems, vehicles, and digital appliances, whilst connecting all of these together and linking them to the far-off places that life in the UK now connects to through intensified globalisation (call centres are a good example here).

This invisibility of electronic passage points is partly physical, i.e. the systems are very small in scale and blend into the wider environment. But it is also cultural: once people get used to all aspects of their lives operating through electronic and physical passage points of various kinds, they start to take very little notice of these systems. This invisibility is especially pronounced for the computer software that continually sorts people's life chances and access to vital spaces and services. Where is it made? How does it work? What does it consist of? And what are its geographies?

In a sense, then, these technologies form a largely invisible 'background' to our society. They disappear from our radar screens at the very moment when they become most important in deciding who gets access to what in our society. As the computer scientist, Mark Weiser, argued in 1981, 'the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.'[4]

The time is therefore ripe to consider how the proliferation of electronic and physical passage points is helping to reorganise the ways in which cities and infrastructures work. To understand the challenges here, I want to briefly explore three key areas: computerised visual surveillance; access-controlled infrastructures; and geolocation.

Towards computerised visual surveillance and tracking

Whole city districts and infrastructure systems are being subject to remote, visual electronic scrutiny for the first time. The several million CCTV cameras currently installed in the UK still rely overwhelmingly on the discretion of human operators to function. However, following early experiments of face recognition software in Newham, Birmingham, Tameside, Manchester, and other locations, a shift towards digital CCTV, which uses computer software to search automatically for stipulated people or behaviours, is rapidly gaining momentum.

Face recognition and other so-called biometric CCTV systems still face major technical obstacles in operating on city streets. However, considerable research and development investment is rapidly addressing these. This is part of a much broader exploration, often funded with support from the US/UK governments as part of the 'war on terror,' of the use of interconnected 'smart' CCTV systems to track movements and behaviours of millions of people both in time and across geographical space.

Although only in its infancy, the combination of biometric tracking – based on scans of people's faces, retinas, irises or even

facial expressions and walking styles – may allow the many current 'islands' of CCTV in cities to be quickly joined up into an integrated whole. This is because software can automatically monitor very large camera networks in a way that traditional, human operators can never hope to match.

Such a shift would prefigure a comprehensive collapse in the age-old notion of anonymity on city streets. Using computer databases or biometric signatures remotely, security and law enforcement personnel may soon be able to identify people without their knowledge, and continuously track them on an individual basis as they move about within a city, or even within whole national or international systems of cities.

To computer ethics specialist, Phil Agre, such a shift to widescale social tracking using face recognition CCTV would usher in a 'tremendous change in our society's conception of the human person. It would mean that people would find strangers addressing them by name' in previously anonymised encounters in city streets and commercial spaces.[5] More worrying still, commercial judgements, based on continuous connections to credit registers and the like, could lead to the regular exclusion and targeting of people deemed to be commercially marginal within increasingly commercialised and gentrified town and city centres.

Two particular challenges present themselves here. First, there is a danger that digital CCTV systems, which continuously search for people and behaviours using computer software, will embed social prejudice deep into the very software that makes them work. With the discretion of camera operators increasingly removed, the software that decides which behaviours, appearances, faces and identifiers require further scrutiny or action becomes both the key site for regulation and the key agent of potential exclusion. The difficult challenge here is for regulators to make transparent the types of faces, behaviours and movements that systems are designed to track as supposedly risky, threatening or abnormal within cities, whilst ignoring the rest of the population and their behaviours which they deem 'normal'.

Pressing questions arise here. Are such systems likely to rely on crude racial profiling as bases for their operation (especially in the context of the 'war on terror')? Will facial recognition databases be interoperable, allowing the possibility of individual tracking across cities, regions, countries, or even internationally? Will such systems be used to police the boundaries of commercialised, gentrified or strategic city spaces, allowing those deemed to be failed consumers within regenerated cities to be tracked and even excluded? Finally, how can codes of practice and accountability be established to prevent abuse when the key algorithms that make face recognition work are themselves so difficult to scrutinise and make transparent, trapped as they are within what social scientists often call the metaphorical 'black boxes' which tend to surround automated technologies?

Second, there is evidence that facial recognition systems will inevitably have inbuilt social and ethnic biases. Evidence for this comes from a major test of emerging systems, the Facial Recognition Vendor Tests of 2000 and 2002.[6] Facial recognition rates were higher for males than for females, and for older people than for younger people. More troubling still, groups classified as Asians and African Americans were easier to recognise than Caucasians because the facial recognition software was programmed to search for the supposedly distinct physical characteristics of such populations.

Clearly, installing widespread face recognition systems whose inbuilt performance biases them to recognise and track particular age and ethnic groups more effectively than others raises major questions about how to regulate these emerging technologies. This is a particular risk with Western security rhetoric focusing over-whelmingly on monitoring and scrutinising people of 'Arab appearance' in the post 9/11 context.

Software-sorted infrastructures

The public spaces and the physical and electronic infrastructures of cities are rapidly being restructured in ways that directly exploit the capabilities of new surveillance passage points. Universal and standardised provisions of access to services, spaces and infrastructures – based on notions of democratic citizenship, open access and public service – are on the wane. Replacing them are notions of targeted services, infrastructures and spaces, available only to these who are allowed access, and priced very differently to different people.

Such shifts are often based on commercial judgements and profiles of the ability of people to pay for increasingly commercialised services, spaces and infrastructures. There is a widespread tendency to apply market principles, and differential pricing, to people at different ends of the social spectrum.

On other occasions, such softwaresorting reflects a desire to allow certain privileged social groups to bypass the congestion presented by the mass of the population in increasingly crowded cities. Such an approach is encouraged because, in a globalised network-based society, the ability to connect and move reliably is of paramount importance for social and economic elites. In line with the varying visibility of passage points, software-sorted infrasructures have very widely varied levels of salience to their users. All users of an airport or congestion-charge system can see whose mobility is being privileged and who is impeded by such systems. But, interestingly, people using call centres on the internet have no idea whatsoever who are the winners and losers of the introduction of software-sorting techniques to manage these increasingly vital domains.

Let's look at the three main emerging types of software-sorted infrastructure in a little more detail.

Road congestion charging and 'intelligent' public transportation

Growing parts of the UK road network are now being splintered off from the main public network, to be allocated on a pay-per-use basis for drivers who choose to pay money for the improved journey times that come with charged access. The London congestion charge, which commenced in 2003, and the Birmingham Northern relief road, are the first examples. Both use Automatic Number Plate Recognition (ANPR) systems to track cars entering charged road space and use this to act against non-payers. But the UK and EU Governments are exploring the possibility of using GPS navigation systems to charge for all road use everywhere within UK and EU territory.

There are major concerns here that the comprehensive electronic movement records inevitably generated by such systems will be used as a social tracking system and that function creep will occur through which law enforcement and security agencies gain access to tracking records. Already, the London system has been enrolled as part of an anti-terrorist initiative proactively searching for suspect and stolen cars. In a similar development, the tracking databases generated by the new 'Oyster' smart card, used by 5 million Londoners to access London's public transport system, are now regularly accessed by the Metropolitan Police for criminal investigations.

Differential call centre queuing

Following widespread practice in the USA, UK-based call centres now routinely use software programmes known as Customer Relations Management (CRM) systems to queue incoming calls differently based on sensing the numbers of incoming calls. This is done by linking to customer databases. Automatic judgements are then made about the quality, worth, or profitability of calling customers. This allows efforts to concentrate on the most profitable premium customers, who are given tailored services, individual attention, and the best promotions and deals. Meanwhile, people from marginalised backgrounds, called 'pond life' recently by one IT executive,* are forced to wait longer periods for inferior or automated service.

'It's all about finding out who the customer is, and putting them in the correct bucket,' explains Ian Davis, a customer relations manager at the IT company ATG. 'This way, the unprofitable customers never hear about the discounts and promotions.'[7] Different service packages, prices and promotions — even for previously nationally standard services like rail fares — can be offered to different individuals, organisations and even localities. The phone company Orange allows immediate access to a human being only to those users who sign up for a premium panther service. The Virgin call centre, thetrainline, deters first time callers with lengthy interactive voice response menus whilst prioritising regular, business, train users for tailored, human, support.[8]

A two-tier software-sorted internet

Similar techniques are also now being used to sort the flows of electronic traffic on the internet. Originally developed to accord all the packets of information that flowed within it equal status, the internet was originally configured by the so-called 'best effort' model of switching packets of information. Here, equal efforts were made to allow all packets to flow to desired destinations at all times. Now, complex surveillance techniques are being used to sift and prioritise each of the billions of data packets that flow over the internet at any one time. The world's biggest manufacturer of internet routers, Cisco, now sifts packet flows on the internet to allow them to offer premium services to what they call the 'transactional/interactive data class' of users. The document also outlines how the electronic mobility of what they term the 'scavenger class' will now be actively impeded based on software-sorting of every single internet packet. 'The Scavenger class [categorisation] is intended to provide differential services, or "less-than-Best-Effort" services, to certain applications,' the document suggests.[9]

Plans to charge a 'congestion charge' to low-grade internet users, announced by the US telecommunications group AT&T in July 2006, look set to exacerbate the reconfiguration of the internet into a two-tier system, which works to reinforce social and economic gaps between privileged and marginal users and places though the sorting of packets flows.

The geolocation and pervasive computing booms

Befitting their role as a means to organise and co-ordinate the everyday life of cities, surveillance practices are increasingly referenced geographically. Most systems of electronic surveillance are now actually organised geographically and are integrated with computerised maps known as Geographical Information Systems (GISs). Many actually track the geographical movements of people, vehicles or commodities using radio frequency identification tags (RFIDs), Global Positioning Systems (GPS), smart ID cards, transponders or the radio signals given off by mobile phones or portable computers.

Whilst opening up the potential to improve logistics management, to learn more about the make-up of neighbourhoods, or to track one's friends as they move around cities, this 'geo-referencing' of surveillance brings with it major risks. Services and advertising can be targeted only at those deemed more profitable as they move about the city, as sensors automatically detect their presence. Computerised mapping systems can exacerbate the gaps between rich and poor neighbourhoods and ossify prejudice into urban geographies through the electronic red lining of areas and people deemed unprofitable or problematic in some way. And people's movements might be continually tracked for the purposes of commercial or social control, with such highly valuable information also traded at great profit on the burgeoning marketplace for geographical data.

The rapid diffusion of tiny Radio Frequency Identifier Tags (RFIDs) – tiny electronic tags that can be scanned by radio systems – raises a series of key challenges to the regulation of geographical surveillance. Computers blur invisibly into the background of the material city, underpinning new smart means of continually tracking goods and people wirelessly as they move. RFIDs are being installed in everything from razor blades and animals, to vehicles, passports and even human skin. The continual assembly of tracking data enables the emergence of city environments that are constantly aware of who and what is moving around within them, along with their recent movements, associations and consumption habits.

RFID and other so-called 'pervasive computing' technologies raise a host of crucial questions. How can principles of transparency and accountability be implemented when cities, streets, rooms and infrastructures literally become sentient, and continually and covertly track who and what

goes on within them? How can the principles of the free and democratic public realm in cities be maintained when those managing malls and increasingly privatised public spaces have the possibility of secretly identifying each individual who enters their realm automatically, as well as their tastes, wealth and potential profitability? How can regulators respond to the dangers that such operators will use RFID to link with profiling databases to sort users, offering incentives,

extra services and benefits to these deemed most desirable, whilst attempting to remove those deemed to be problematic, unprofitable, or irregular in some way? With Amazon.com already shown to be selling DVDs to different customers at different prices, based on computer assessments of their value as customers, is regulatory intervention necessary to ensure that mass commercial price-fixing does not emerge based on the operation of automated RFID surveillance? How can the covert scanning of people's private realms for consumption data best be regulated, and how can the use of such data to identify risky individuals be controlled? In short, how can the freedom of movement and assembly in cities be protected in a world of ubiquitous and continuous tracking where such technologies are being widely invested with the power to improve security and fight terrorism? The clear danger is that pervasive computing and RFID revolutions will work to 'chill [the] irregular, deviant or unpopular speech and actions'[10] that are ultimately essential to the maintenance of a democratic society.

Conclusion

It is clear that the largely invisible and esoteric world of software-sorting urgently needs to be exposed and robustly regulated. In particular, privacy regulators, Information Commissioners, and all those addressing the challenges of social exclusion in today's society need to become rapidly aware of how cities and infrastructures are being rebuilt as systems of continuous surveillance, tracking and social-sorting. With these systems already at the point where they are 'disappearing' from view, to become the taken-for-granted background to the functioning of our society, the policy and research challenges here are both urgent and, it must be said, somewhat daunting.

The key challenge is to try and expose the computer software that directly operates in software-sorted systems to favour certain people at the direct expense of others. For it is in the shaping and writing of computer software itself where real power now lies. What social judgements, prejudices and problematic biases go into such software? How is such software diffused and sold around the world? And do the organisations shaping it even have any idea themselves about how its exclusionary 'decisions' might operate in practice?

To prevent all aspects of life being secretly and continually sifted by new, often highly commercialised, software-sorting, public regulation of these systems is vital. Without it, there will be little to stop the emergence of a hyper-consumerised and hyper-individualised society where rights, services and social status are starkly segmented and packaged up on a completely customised basis using judgements of potential profitability, riskiness or regularity. To avoid this, three principles of accountability, transparency and proportionality must be the keystones for a robust programme of regulation and supportive research.

Accountability is necessary so that those organisations practising software-sorting are made to justify their actions as part of the principle of democratic regulation, at the most appropriate geographical scale.

Transparency is required to make software-sorting visible. It is necessary so that the contents of the software that actually does the social and geographical sorting are made as public as possible — within the obvious constraints of commercial propriety — along with an assessment of the effects.

And an assessment of *Proportionality* is vital to prevent the shift towards ever-extending and integrated surveillance systems which work to track and monitor greater and greater portions of public and private life, for the purposes of social control, the supposed imperatives of the market, or simply profit. Once societies are organised around the tracking and sorting possibilities of computerised databases, there will be a logic of extending the reach and range of those systems. This is especially so as the mantra of 'security' creeps over all walks of public life, as part of the 'war on terror'.

The software-sorted society is here. It is rapidly intensifying and extending its powers. And it is about time that regulators, policy makers and governments realised that fact.

Notes

[1] See Stephen Graham (2004) (Ed.), *The Cybercities Reader*, Routledge; Stephen Graham (2005), 'Software-sorted geographies', *Progress in Human Geography*, 29(5), 1–19.

[2] Jeremy Rifkin (2000) *The Age of Access: The New Culture of Hypercapitalism, Where All of Life Is a Paid-for Experience*, Tarcher.

[3] Bill Gates (1995), *The Road Ahead*, London: Hodder and Stoughton; Frances Cairncross (2001), The Death of Distance, Texare Publishing; Leadbetter, C. (2000), *Living on Thin Air: The New Economy*, London : Penguin.

[4] Marc Weiser (1991), 'The computer for the 21st century,' *Scientific American*, 265, September, 94–104.

[5] Phil Agre 2001: 'Your face is not a bar code: Arguments against automatic face recognition in public places', *Whole Earth*, 106, 74–77.

[6] Phillips, P. et al (2002), Face Recognition Vendor Test, 2002: Overview and Summary, Biometric Institute. See Introna, L. and Wood, D. (2004), 'Picturing algorithmic surveillance: The politics of facial recognition systems', *Surveillance and Society*, 2, 177–198.

[7] Quoted in Booth, N. (2006), Press 1 if you're poor, 2 if you're loaded..., Technology Guardian, March 2nd, pp.3.

[8] Booth, N. (2006), Press 1 if you're poor, 2 if you're loaded..., Technology Guardian, March 2nd, pp.3.

[9] Cisco (2002): Service provider quality of service – Design guide, Washington DC: Cisco Inc.

[10] Kang, J. and Cuff, D. (2005), Pervasive Computing: Embedded in the Public Sphere, available from dcuff@ucla.edu. pp. 33.

Stephen Graham is Professor of Human Geography at the University of Durham, and Deputy Director of the Centre for the Study of Cities and Regions (www.dur.ac.uk/cscr/). He is also Associate Director of the International Boundaries Research Unit (www.dur.ac.uk/ibru/). He held a British Academy Research Readership, funding two year's replacement teaching to allow him to concentrate on his research on the 'software-sorted society'.