Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example

David Murakami Wood
Queen's University, Ontario

C. William R. Webster
University of Stirling

Abstract

This article argues that surveillance is becoming increasingly normalised across Europe and that this is altering the landscape of liberty and security. It identifies this normalisation as a product of the globalisation of surveillance, the domestication of security, the desire of the European Union (EU) to create a distinct leading role in security, and the influence of the 'bad example' of the United Kingdom (UK). The article uses the two very different examples of video-surveillance and electronic public services in the UK to make this case and to argue for both stronger resistance to calls to make human rights more flexible in a risk and security-driven age and more detailed research into the differences between emerging surveillance societies in Europe.

Keywords

CCTV; Security; Surveillance; Surveillance Society

IT IS COMMONLY HELD THAT CONTEMPORARY CAPITALIST NATION-STATES ARE 'surveillance societies' (Lyon 1994, 2001, 2007). This usually refers to the fact that surveillance is a key mode, if not the principle mode, of organisation in those nation-states. It is no longer remarkable that this is so, and the naive phase of surveillance studies, in which we were 'surprised' by evidence of surveillance, is long past. But what does it mean to live in surveillance societies and what economic, political and social relations are produced? These are the key questions of a new pan-European research network called Living in Surveillance Societies (LiSS),[1] and this article will outline some of the background and reasoning behind it.

The key argument made in this article is that while it makes sense in academic terms to have abandoned any notion that we are still 'discovering' surveillance, the normalisation of

[1] Living in Surveillance Societies COST Action ISO807, funded by the ESF and the EU Framework programme and administered by COST (European Cooperation in the field of Scientific and Technical Research). Available at: http://www.cost.esf.org/domains_actions/isch/Actions/liss, last accessed 9 July 2009.

Murakami Wood, D. and Webster, C.W.R. (2009). 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example', *Journal of Contemporary European Research*. 5 (2), pp. 259-273.

Available at: http://www.jcer.net/ojs/index.php/jcer/article/view/159/144/

surveillance in social life has important ethical and political consequences which, although inevitable for everyday life, have to be called into question. The role of surveillance studies then, is both to detail the ways in which everyday life in surveillance societies occurs, but also to continually reopen the 'black-box' into which surveillance is vanishing, and to critically examine the increasingly coherent and stable surveillant assemblage (Haggerty and Ericson 2000). We need to make surveillance strange again, and therefore open to rigorous examination and possibly change.

Underpinning our argument is the simple proposition that technologically mediated surveillance practices raise significant questions about modern society, the nature of liberty and its relationship to security, and about relations between citizens, businesses and the state. Furthermore, a closer examination of the 'new normality' of everyday surveillance highlights the differentiated and diverse application of surveillance in modern European society. We argue that in the United Kingdom (UK), processes of normalisation of surveillance have gone much further than elsewhere, and with the UK currently considered a 'model' to be aspired to by security professionals, the 'threat of a bad example' to other European nation-states is real. Consequently, our view is that a better understanding, and enhanced societal awareness, of surveillance can lead to better informed public policy and practice.

This short article has three main parts. The first part looks at the ways in which surveillance has become a key part of the 'organisational package' that accompanies late or advanced capitalism. Contemporary globalisation involves the simultaneous spread and intensification of this particular mode of capitalism, but also forms of governmentality, state, social and personal organisation that accompany it and are held to flow 'naturally' from the adoption of these new relations of production and consumption. The second part will consider the ways in which this new normality is in no way 'natural' even within late capitalism, and in fact continually reinforced through the work of state and private sector actors and this always incomplete process is contested by others. It looks in particular at the example of video-surveillance in the UK as an area where the normalisation of surveillance has gone further than in most other countries. Part three considers the nature of modern surveillance for those living in surveillance societies. This is achieved by exploring dimensions of modern technologically mediated surveillance, dimensions which show that surveillance is not just ubiquitous; it is also subtle, deep, unobtrusive and selective. The concluding discussion pulls the cores themes of the article together around an agenda for research into living in surveillance societies.

The Globalisation of Surveillance and the Domestication of Security

Modes of production and consumption have their own accompanying modes of ordering (Law 1992). Surveillance has become a key mode of ordering in late capitalism (Lyon 2007) largely through the affordances of particular sociotechnical developments: telecommunications, computing and the new verticality offered by access to orbital space. The organisational rationale for this has been the rise of risk-thinking (Beck 1992) and the spread of risk-management as being the predominant perceived job of any organisation, both internally and externally (Ericson and Haggerty 1997). The new technologies are placed in the service of this agenda: collecting and sorting data on people, things and events in order to produce categories of risk and profitability, which will enable foresight and anticipation of future risks and profits (Graham and Wood 2003). Many of these developments have taken place initially within military arenas; however, the globalisation of surveillance has also been accompanied by the domestication of security. As the 'risk-surveillance society' (Murakami Wood *et al*. 2006) has become the 'ideal-type' state of the Twenty-First Century, so its aims - anticipated and pre-managed risk, safety, control, security – are increasingly permeating policy and practice at every level. The relationship of globalization and militarism has become an important area of research and polemic recently (see e.g. Hardt and Negri 2000), indeed Naomi Klein (2008) has controversially characterized the contemporary economy as one of 'disaster capitalism', in a post-modern and critical variation on Schumpterian creative destruction. Regardless of whether one would go as far as Klein, it is rather less controversial that there is a military character to the forms of surveillance that are currently being globalized. One of us has elsewhere used the language of 'securitization' (Coaffee *et al.* 2009) but this should not obscure the fact that the flows go both ways. Militaries are increasingly influenced by models originating from outside the military. Mick Dillon (2002) has noted the influence of new biological and bioinformatic research on US military strategic thinking, and business style and discourse increasingly penetrate military style.

In the immediate post-Cold War period, there was a diversification of production in the military security sector, which led to large companies that had previously been almost exclusively military contractors adapting products for civilian markets (Coaffee *et al*. 2009). For example, as Jon Coaffee (2001) has noted, the Automatic Numberplate Recognition (ANPR) system installed in London in the early 1990s relied on technologies tested in the invasion of Iraq in 1991. Whilst this militarism may seen to have a strongly 'American' flavour, just as the current wave of capitalism does, the new mixed military-civil security and surveillance economy is not exclusively an American or Anglo-American development. Large companies all over Europe and the world maintain such diverse portfolios, for example, the French group Sagem, which makes everything from mobile telephones to Unmanned Aerial Vehicles (UAVs) - flying surveillance drones; or Nokia which has moved into collaboration with Siemens on the manufacture of new Intelligent Surveillance Platforms (ISPs) - off-the-shelf dataveillance systems able to handle everything from telecommunications capture to video images. However it is certainly the case that the surveillance surge that has overtaken the UK since the early 1990s has made Britain a lucrative marketplace for surveillance equipment.

The new surveillance economy has of course profited from the renewed hostilities that have gradually come to fill the perceived military vacuum left by the end of the Soviet Union and its satellite states. Indeed, along with the creation of new civilian markets for military surveillance equipment, the language of combat also became part of the lexicon of politics: wars on drugs; wars on crime; wars, as Ericson (2006) put it, on everything. However, with the war on terror(ism), and the invasions of Iraq and Afghanistan, there has been a renewed surge of military surveillance development. The new 'war' does not involved the massive, lumbering, 'baroque arsenal' (Kaldor 1981) but is a series of asymmetric conflicts seen as being fought much more much through information and intelligence than through the threat of total annihilation (Metz 2000; see also Graham 2004). The transformation of crime and policing has been similar with information-led (and surveillance-saturated) policing to deal with flexible forms of crime that are not limited by traditional borders. The new forms of war and crime are also at once international, transnational and intranational; they do not fit either the old order of discrete nation-states connected by bilateral or international agreements and institutions, such as the United Nations or Interpol, and thus are seen to call into question the capacity of both those existing global institutions and individual states to deal with these issues internationally or within their own jurisdictions (Loader and Walker 2007). Hence the secret EU-FBI policing deals in the 1990s that have led to the opening of databases and the flow of personal information between a whole variety of US and European agencies[2] or the rise of the G7/8 as a place for the creation of new security and surveillance initiatives, as for example, with

[2] See the collection of documents accumulated by Statewatch on 'the EU-FBI telecommunications surveillance system' available at: http://www.statewatch.org/eufbi/,last accessed 10 July 2009; and the subsequent expansion of EU-US agreements on data-sharing available at: http://www.statewatch.org/soseurope.htm, last accessed 10 July 2009.

the new international passport standards, despite its relative lack of formal competence in this area (see: G8 2003, 2004; Statewatch 2004). The globalisation of surveillance depends to some extent on the spread of standards to allow interoperability of systems, which in itself is part of a globalization of governance, but this globalization is not based on the institutions of previous waves of internationalization but on a more exclusive, closed and secretive set of organisations.

It would be easy to put this down to a new American 'empire' in the manner of Hardt and Negri (2000) but, as with the economic expansion, this is too convenient and simple an explanation. The form of the globalization of surveillance and the new political economy that is evolving around it is as much a product of the practices of the European Union (EU). As the work of organisations like Statewatch[3] and the CHALLENGE network[4] have demonstrated, the new forms of international security co-operation, and the setting of surveillance standards are as much a product of the EU's experience of the creation and operation of its 'Fortress Europe' Schengen immigration controls (see Bigo and Guild 2005) and the way in which these agreements occur largely in secret and at an elite level, as much 'European' in character as American. It does not mean either that the EU is 'under the thumb' of the USA: the EU is quite capable, when it wishes, of carrying out development independent of or even in direct opposition to, the USA – as with the Galileo satellite project, which will create a direct rival for the US Global Positioning System (Lembke 2002; McDonald 2007). Frequently, the EU has also gone beyond the standards required by international agreements on surveillance and security as was the case with the new biometric passports (Bunyan 2005).

The creation of new modes of surveillant organisation and the expansion of military technologies into civilian markets has also led to a redefinition of the concept of security. It is undoubtedly the case that for many forms of surveillance, especially those associated with crime control and policing; one can see a domestication of military security rationality alongside the use, in many cases, of military technologies. As Coaffee and Murakami Wood (2006: 503) argued, "security is coming home". This domestication of surveillance technology occurs not just in the arena of urban security and surveillance but also in the practices of government. There has been a migration of technologies from military settings to civil settings driven by the expansion of e-government services and the need for more effective and efficient public services. The use of new ICTs has led to the emergence of large state databases, utilised for processing public service information, and the emergence of new transactional electronic public services, using a range of electronic service delivery mechanisms including, significantly, the Internet (Bellamy and Taylor 1998). The growth of computing power and indeed the new networked infrastructure that can join them together were both initially products of the US Cold War military research and development, and the attempt to create a 'closed world' over which the US military could exercise control (Edwards 1996).

Normalising Surveillance Society

The domestication of security and the globalisation of surveillance would be limited processes if their results did not become increasingly 'normal' and part of the experience of everyday life. In his ongoing expansion and critique of Foucault, Giorgio Agamben (2005) has described the way in which 'states of exception' spread and come to be expected forms of governmentality. What would in the previous mode of ordering be

[3] Statewatch, the independent observatory of civil liberties in Europe. Available at: http://www.statewatch.org/, last accessed 9 July 2009.
[4] CHALLENGE, EU Framework Program 6-funded research network on liberty and security. Available at: http://www.libertysecurity.org/, last accessed 9 July 2009.

regarded as temporary or even entirely unacceptable becomes unremarkable, mundane, normal and consequently may not even be challenged.

A key example is that of the spread of Closed Circuit Television (CCTV), or video-surveillance, in the UK (Webster 1996, 2004). Despite the existence of earlier experiments (Williams 2003, 2009), the history of state video-surveillance in the UK began in the late 1980s and went through a massive period of expansion from the mid-1990s and again in the early years if the 2000s (Webster 2009). However what is remarkable about this is the distinct lack of non-academic opposition to this spread, and indeed the popular enthusiasm for surveillance cameras and the demand for their installation in more and more places. This is all the more remarkable as independent and state assessments have repeatedly revealed that CCTV is extremely limited in its effectiveness in preventing crime (see Gill and Spriggs 2005; Welsh and Farrington 2002, 2008) and even solving crime (ACPO 2007). It has thus been criticised as an extremely inefficient use of public funds (Groombridge 2008) regardless of its effects on liberty and social trust (see Murakami Wood *et al.* 2006).

So why the lack of opposition to, or even enthusiasm for CCTV? There are several reasons. Firstly, it is about what they represent rather than what they do. We would argue that CCTV cameras are a visible manifestation of the state's concern about crime and security. They show 'something is being done'. This 'stage-set security' (Murakami Wood and Coaffee 2006) or ‘security theatre’ (Schneier 2008) gives us symbols of safety in a society in which everything is seen as a potential source of risk, and where fear dominates. It assuages our fear of the dangerous other and society as a space of negative possibilities in a risk society (De Cauter 2004). Theatrical security is to be found everywhere from the airport to the high street, from the demands to remove shoes for inspection to the increasing numbers of uniformed 'plastic police': Police Community Support Officers (PCSOs, in the UK), city centre and neighbourhood wardens, ‘mall cops’, private security and so on, who look like the 'real' police and may even have some direct connection to the police, but lack either their training or powers. They are simply symbols: performers in the ‘security theatre’.

Secondly, there is a perception of the purposes and practice of surveillance that is not wrong as such but may not necessarily appropriate in this case. David Lyon (2001) argued that the motivations for surveillance are usually as much about care as about control, and if CCTV cameras imply the idea of someone watching, for many people this means watching out for them. Of course we know that in practice those working in control rooms are as good or bad at their jobs as anyone else: there are examples of care, but there are also examples of bad practice that range from simple boredom and laziness to active abuse of the role, for example in the compilation of sexual images of women from recordings by male operatives (Norris and Armstrong 1999; Smith 2004, 2005).

Thirdly, CCTV very rapidly became part of the cultural landscape of Britain (Groombridge 2002). CCTV images were used right from the start in a new generation of television shows that used extreme examples of activities captured on CCTV for entertainment. Ostensibly about the police, many were even initiated by police forces, they were actually simply vicarious pleasures in the manner of short movies but with a greater feeling of immediacy and therefore more 'real' (Jermyn 2003). This kind of reality TV soon gave way to the next generation in which the set-up was far more artificial – a group of young people in an expensive studio apartment, or on a deserted island - but surveillance cameras allowed the viewing of these artificial set-ups not just in short segments now but potentially 24/7 (see Holmes and Jermyn 2003). Much like the operators in a CCTV control room, the millions of viewers in this 'synopticon' (Mattiessen 1997) watched these small groups of voluntarily incarcerated individuals in the generally frustrated expectation that *something* might happen. It was banal, boring, normal, but utterly addictive: soporific even. However, there are more productive governmental aspects to this watching of surveillance images and both Gareth Palmer (2003) and Mark Andrejevic (2003) have drawn attention to different aspects of its political economy. Palmer describes this as a process of governance, Andrejevic as a kind of labour or at least a form of training for both participants and watchers. It is both. It is effectively helping us all to become not only used to surveillance, to experience it as an expected part of everyday life, but to enjoy it and to watch its products in a certain way: to train our eyes for surveillance. In this sense through reality TV, as much as through government exhortations to look out for suspicious activity, we all become potential agents of surveillance and spies (Coaffee *et al.* 2009). However this 'responsibilization' of citizens (Rose 2000) has its limits: although after the terrorist attacks of the early twenty-first century in Europe, governments at first encouraged citizens to take an active part in watching for signs of terrorism, there seems to be a limiting of such responsibilization now, at least in Britain. In the 2008 Counter-Terrorism Act, which came into force in February 2009[5], there are powers available to the police to limit the ability of citizens to take photographs or video footage in public places. Taken along with the expansion of CCTV, it could be argued that there is a totalitarian direction emerging in particular groups within the British state to regulate the production of visual information *altogether*. This foregrounds the incompleteness of normalization processes and the conscious or subconscious anxiety that their potential failure generates in government. As Rose (2000) has argued, there is never a clear division between the three forms of governmentality set out by Foucault: moral regulation, surveillance and sovereign power, rather there is a constant movement between them akin to the 'modulation' identified by Deleuze (1990) as a key characteristic of the postmodern 'control society' (Coaffee *et al.* 2009).

Fourthly, and connected to this, is that CCTV gives a visual narrative to the incomprehensible. This is perhaps why the state has no objection to the public having access to the products of CCTV. People watch CCTV like a TV soap opera or a Hollywood movie, and whether there is narrative or not, they impose their own story complete with characters, settings and plot, as Gavin Smith (2008) has shown with regard to CCTV operators. More broadly, watchers invest what are often only retrospectively meaningful images with emotional content and personalise it. This of course can have a negative effect on critical judgement and politics. As Norris and Armstrong (1999) argued of the notorious James Bulger case in the UK, the CCTV images of a child being taken away by his killers helped create a demand for cameras even though what was being seen was a failure of CCTV: the presence of video-surveillance did not prevent the crime, and the analysis of the images for some time led the police to erroneous conclusions about the age of his abductors.

The important thing about this discussion is that none of these arguments have anything to do with either the technological properties of the cameras or the actual functioning of the systems *per se*. They are not about the exact number of cameras, their capabilities or, fundamentally, about whether the cameras *work*. Our argument instead is about how surveillance works at the level of emotion, symbolism and culture. The normalisation of surveillance can occur, then, when surveillance colonises these domains. The normalisation of surveillance is therefore also about far more than just the proliferation of a range of surveillance artefacts and technologies; it is about how these are embedded in the norms and institutions of society and how they are reflective of other aspects of modern society.

[5] Counter-Terrorism Act 2008 (UK). Available at: http://www.opsi.gov.uk/acts/acts2008/ukpga_20080028_en_1, last accessed 10 July 2009.

There are other kinds of 'normalization' however, which are equally important. Perhaps the most significant are the alteration to routines of work practice and management, particularly in government bureaucracies and service delivery. The movement to the kind of computerised, networked, electronic public services, to which we made reference in the previous section, has been driven by cost cutting and efficiency agendas, partly because new informated services are replacing old paper-based manual services and partly because new electronic services allow citizens to access services from multiple locations at their own convenience. The potential to extend this form of service delivery is recognised in the UK with the Varney report (2006) which calls for greater information sharing and the development of extensive networked databases. A further aspect of electronic provision of public and democratic services is the emergence of citizen-centric or citizen-focussed services - i.e. where new technologies tailor information specifically for citizen clients. So, services are supposedly personalised around the discreet information and needs of individuals. Surveillance – or more accurately in this case, dataveillance, the management and categorisation of data derived from surveillance – is seen to be working to provide what citizens want – the efficient and convenient delivery of public services from health to education – and without it, these services would be put at risk. The functioning of the services they provide again reinforces the normality of the collection, storage and sorting of large amounts of personal data, and the privileged or protected access or even 'ownership' of personal data by the state or, increasingly, its private partners or subcontractors. The assumption of ownership of private data is certainly not normal across Europe, but is another 'bad example' from Britain, which can be seen in the proposal to fine or even imprison those who do not provide up-to-date information for the proposed new British National Identity Register (NIR).[6] Other models exist in Europe, both of the greater assumption of 'data protection' for the citizen (*not* privacy) in Germany, and its opposite in the 'state-generated data is everyone's data' of Sweden, which allows even personal tax returns to be scrutinized by anyone who wishes (for a survey, see Bennett and Raab 2006).

So, electronic public services are key to developing a surveillance infrastructure, to populating it with information, and in addition, because of the universal and information-intensive nature of public services, bureaucrats, citizens and service users are all exposed to subtle surveillance practices through the everyday interactions that occur around information giving and service provision. It is not so much that social negotiations tend to be reduced to a series of binary possibilities as Michalis Lianos (2001) has suggested, however the range of possibilities are certainly reduced: interactions certainly become structured around surveillance relationships, and the new forms of social negotiation that emerge are no longer about what information one chooses to give but how that information is to be given (or taken).

Everyday Living in Surveillance Societies

Global surveillance, the domestication of surveillance and the normalisation of surveillance activity has led a number of authors to explicitly consider 'life' and everyday living in the emergent surveillance society (Aas 2008; Lyon 2002; Monahan 2006). The term 'surveillance society' is a term that has widespread recognition and which in recent years has gained considerable currency. However, it is also a bland term, which although recognises the widespread usage of surveillance technologies in society tells us little about how these technologies are felt, experienced or the different dimensions and deviations in surveillance practice. Surveillance in the most basic surveillance society perspective is seen to be ubiquitous and universal - everywhere - and mediated by new

[6] Home Office ID Cards site, available at: http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/, last accessed 9 July 2009.

sophisticated ICTs. Such a position masks the subtleties of modern surveillance and the different ways in which we experience everyday life under the scrutiny of surveillance. This line of argument is explored further in this section of the article through the identification and exploration of three dimensions of everyday surveillance, dimensions which reflect upon: firstly, our perceptions of surveillance, secondly, the 'depth' of surveillance and thirdly, our exposure to surveillance. We then problematize the term further with consideration of the very different national settings of surveillance activity in Europe.

Dimension 1: Contrasting perceptions of surveillance

The first dimension relates to the different ways in which surveillance technologies are perceived, both in their usefulness and their desirability. The term 'surveillance society' has embedded within it a sense of negativity, it is very subjective term and conjures up images of the Big Brother state of George Orwell's *Nineteen Eighty-Four* (1949) and constant threats to privacy and liberty (Garfinkel 2000). This is reflected in the discourses of anti-surveillance groups, for example No2ID[7] in the UK, and also in official reports, for example, the European Parliament Scientific and Technological Options Assessment Committee Report on 'Technologies of Political Control' (STOA 1999) or the UK Information Commissioner's Office report on the surveillance society (Murakami Wood *et al* 2006). However, the deployment of surveillance technologies divides opinion and for many their introduction is heralded as valuable in delivering national security and in the 'fight against crime' and terrorism. An example of this is the support for CCTV mentioned above and demonstrated in public perception surveys (see Honess and Charman 1992). Additionally, vast quantities of personal information are collected, stored and exchanged by public services in e-government initiatives designed to make public services more efficient, accessible and effective (Cabinet Office 2005; Varney 2006). In this respect, technologies, like CCTV, ID Cards, offender tags, mobile phones, databases, the internet and satellite navigation (etc.) represent technologies for enhanced surveillance on one hand *and* technologies of efficiency, enhanced services and a better, safer society on the other. Taylor *et al.* (2009) go so far as to argue that these two positions, that is 'information capture' for enhanced services and 'information capture' for surveillance, are diametrically opposed perspectives on the same phenomenon - they call these two perspective the 'surveillance state' and 'service state' perspectives. This dichotomy raises questions about the intentions of technological uptake and about our perceptions of these intentions. So, following on from the argument brought forward by Taylor *et al.* (2009), the integration and networking of government databases could be seen as either effective 'joined-up' government or 'surveillance creep', depending upon which perspective you subscribe to. Although, these perspectives may seem diametrically opposed we would argue that they are in fact interlinked and interdependent, and that not only is it possible to deliver public service efficiencies, enhanced security and increased surveillance simultaneously, but this is what is happening in practice (when the technology 'works' which it frequently does not). Following this line of argument the adoption of sophisticated new technology does not imply a choice between the surveillance society *or* a safe efficient society, because both are perceived to be, or promoted as, happening at the same time.

Dimension 2: Depth of surveillance

The second dimension relates to the depth and intensity of modern surveillance. In the surveillance society perspective surveillance is seen as ubiquitous, it is everywhere and we are all subject to it on an ever increasing scale. However, we would argue that to merely

[7] NO2ID, campaign against ID cards and the 'database state'. Available at: http://www.no2id.net/, last accessed 9 July 2009.

say surveillance is everywhere masks the extent and depth of surveillance that can be realised through new technology. Furthermore, surveillance is more subtle than this. More often than not we are not aware that surveillance is taking place and consequently the scope or scale of surveillance we participate in. Consider, for example, the spread of biometric ID cards or CCTV systems with facial recognition, both offer systems for electronic citizen identification, which can be networked to further databases to access a range of information about the citizen, potentially including information about their criminal, health, educational financial and/or employment histories. If the necessary political will is present (and this is certainly not a given), such information could be extended beyond public records to include intimate information relating to personal relations, political affiliations, travel history and sexual preferences (etc.) – as indeed was the case with the 'EDVIGE' database in France (see below). It is not what information is accessed, but our knowledge of the information sharing possibilities supported by discreet electronic interactions. Despite the apparently successful attempts of many European regulatory bodies to raise awareness of information rights (Kantor Management Consultants 2009), most people only become aware of the information held about them, or what information is shared between agencies, when media-publicised breaches or losses occur, as happened with some regularity in the UK in 2007 and 2008 (Poynter 2008). The scenario described here is only feasible with the emergence of large databases of personal information, and these databases exist in the public and private sectors. In addition to the records held by public service agencies the private sector keeps records about our credit history, our travel patterns (via GPS and mobile phones), telephone and email usage and our purchase patterns (via shop loyalty cards, 'air miles' schemes, and so on). Increasingly, this information can be used to 'profile' individuals so that products can be selected and tailored to their personal requirements. Participation in modern society necessitates a series of activities which leave a data shadow, trail, or electronic 'footprints', as we go about our everyday existence (Lace 2005). Many of these electronic interactions go unnoticed and are/seem perfectly normal. But they initiate the exchange of vast quantities of personal information, much of which we are oblivious to. In this respect surveillance is not just ubiquitous it is deep, unobtrusive and sophisticated.

Dimension 3: Exposure to surveillance

The third dimension relates to the extent to which we as individuals are the discreet targets of surveillance activity, in other words, the extent to which we are exposed to intense technologically mediated surveillance. Although the surveillance society perspective would suggest we are all exposed to increasing levels of surveillance much of our exposure is usually benign and unobtrusive. This is because the majority of our electronic interactions, when considered on their own, are relatively insignificant (beyond the initial transaction or purpose of the interaction) and consequently do not warrant further surveillance attention. For example, travel cards, such as the 'Oyster' card in London, may record our personal travel details but they also provide important information about general travel patterns, such as passenger numbers on a particular route, peak periods, typical journey length, and so on. For the latter our personal details are not of interest, the value of the information gained relates to a bigger picture, and in particular, how this information can be 'reflected back' and utilised to make adjustments to service provision in order to provide better more efficient services. Public administration e-government theorists refer to this as processes of 'informatization' (Frissen and Snellen 1990). In this scenario citizens and service users remain relatively anonymous, although they are surveyed, their personal details are not really utilised in any meaningful way. This may be the case for the majority, but there will be instances where the same technologies will be utilised to conduct intensive targeted personally focused surveillance. A case in point is the general use of CCTV in public spaces. Although such systems are commonplace in towns and cities across Europe (Webster 1996, 2004), their deployment has led to diverse surveillance practices and differentiated levels of surveillance (Webster 2009). Most citizens will pass through CCTV surveyed areas relatively anonymously, unidentified and ignored. However, certain individuals will attract further attention, scrutiny and surveillance. They may be exhibiting suspicious behaviour, be known to the CCTV operatives, or just seem somehow different (Smith 2008). Such individuals may be surveyed more closely, their movements and activities more closely monitored and information cross-referenced and recoded for future use. They are not anonymous; rather they are being subject to targeted intense surveillance. It is relatively easy to see how such arrangements could be expanded to perpetually and intensively survey those in society who are perceived to be a 'risk' or 'at risk'. The key feature of this dimension then is that our expose to surveillance is differentiated by who we are, or who we are perceived to be. Surveillance for one person may be unobtrusive, perhaps even key to helping them get access to the goods and services they need, yet for others it will be intense and pervasive. A further aspect of this argument relates to the vast quantities of personal data held. Individuals may not be 'live' surveillance targets but the trail of electronic interactions stored on databases mean that activities can be recalled at a later date if necessary. So, in time, given the right (or wrong) circumstances we can all retrospectively become suspects - which means that we are actually always already potential suspects. The movement of responsibilization identified above is almost always accompanied by a concomitant 'deresponsibilization' (Hunt 2003).

A surveillance society or surveillance societies?

The final point to make is that we very deliberately in this article and in the title of the COST action used the term 'surveillance society' in the plural. This is to emphasise something that is still under-emphasised in the literature (Murakami Wood 2009), which is the way that surveillance, despite its spread as a key mode of ordering in late capitalism, is always situated and varied depending on its application in different places - regions, states, cities (etc) - and in the responses and challenges posed to it by different cultures, constitutions, legal systems and institutional settings (etc.). For example, as Marianne Gras (2004) pointed out, the varying nature of constitutional protections for privacy across Europe has meant very different responses to surveillance. Bennett and Raab (2006) further develop a comparative perspectives in their exploration of the emergence of multiple privacy 'regimes', each embedded in its own national setting and history. A case in point is the divergent ways in which European countries have responded to the emergence of CCTV. The trans-European comparative *UrbanEye* study of city-centre CCTV showed remarkable differences in the implementation of, and both state and public attitudes to surveillance (Hempel and Toepfer 2004). For example, the German Federal Constitutional Court's decision of 1983 on the extent of privacy in Article 10 of the Basic Law has hindered the spread of open-street CCTV (Gras 2004) and allowed a campaign of opposition to build up against security rhetoric. However, in the UK, the lack of any real constitution, and the only recent incorporation of the European Convention of Human Rights in British law, has meant that attempts to challenge open-street CCTV on privacy grounds are already confounded by the 'facts on the ground' of millions of existing cameras. Germany also has the recent past of totalitarian rule and, for the former German Democratic Republic the experience of the intense attention to personal lives of the Stasi and their legions of informers. Britain never had this experience and perhaps there is a certain smugness about the impossibility of fascism in the United Kingdom ('it couldn't happen here'), which when examined is based simply in contingency rather than any supposed 'national characteristics' and is increasingly being undermined by laws like the Counter-Terrorism Act 2008 (mentioned above). This has lead the ex-Head of the Security Service, MI5, Stella Rimington, who can hardly be dismissed as an alarmist or a radical, to claim that Britain is heading towards a police state (Whitehead 2009). This does not mean that Germany is by definition not a surveillance society and Britain certainly is, but it does mean that they exhibit different surveillance characteristics; they are different kinds of surveillance societies. Experience of totalitarianism does not lead the same way in every European country either: whilst the Greek population generally appears strongly resistant to contemporary surveillance (Samatas 2004), the Poles and the Russians do not draw the same lessons.

However there are connections, even as there are differences. Britain has come to be regarded by those making security-based arguments for more surveillance anywhere in Europe, as an 'example' or a model to be aspired to. This will inevitably bring conflicts with the very different traditions of liberty. President Sarkozy of France was one of those who expressed admiration for Britain's CCTV networks, yet in the reaction to the 'Exploitation documentaire et valorisation de l'information générale' (EDVIGE) database[8] of all those in positions of responsibility in organisations, clubs and societies, which included demonstrations and a fierce opposition campaign shows a rather stronger culture of defence of liberty than has yet been demonstrated in the UK. However with the Convention on Modern Liberty held across the UK in March 2009, a fragmented and still small but increasingly determined opposition is emerging.[9]

Concluding Discussion: Understanding and Challenging Surveillance Societies

The landscape of security and liberty in Europe is changing. Developments resulting from the simultaneous globalization of surveillance and domestication of security (Coaffee and Murakami Wood 2006), the creation of a distinctive security agenda and institutional landscape at the EU level (Bigo and Bonditti 2009) and the emergence of different surveillance societies in nation-states across Europe are leading to a variety of possibilities. It is certain that in contemporary European society surveillance is increasingly embedded in everyday life. We participate, often willingly, in surveillance and it is a lucrative business at a time when business in many other sectors is difficult, perhaps even because of economic pressures. The future of liberty and security in Europe is closely intertwined with the deployment of sophisticated technologically mediated surveillance technologies, which are introduced for a variety of purposes, many associated with enhancing the efficiency of public services, but which nevertheless implicitly result in more sophisticated ways of collecting and sharing personal data.

It could be argued, from a perspective of efficient government, that surveillance is a central part of modern society and intrinsic to ideas about delivering a secure, stable and competitive Europe. It is evident from the arguments brought forward in this article that a key feature of the emergent surveillance society is the centrality of the role played by government and public services. Information-intensive state activity has led to the development of large networked state databases, essential to the effective delivery of information age democracy and public services. Further to this, public policy has played a central role in bringing forward such systems in order to deliver internal and external security. Public policy and services are therefore inherently intertwined with modern surveillance practices. We would suggest that it is the information intensity of our relations with the state, embedded in and reflected by, the provision of new 'surveillance' technologies that determines and characterises the nature of modern society and the extent to which this society is dominated by surveillance relations.

[8] Ministere de L'Interior, Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE » JORF n°0152 du 1 juillet 2008, texte n° 3. Available at: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019103207&dateTexte=&oldAction=rechJO&categorieLien=id, last accessed 9 July 2009.
[9] Convention on Modern Liberty. Available at: http://www.modernliberty.net/, last accessed 10 July 2009.

However, this article has also gone further and in noting the differences between European surveillance societies, we have posited the United Kingdom as a 'bad example' in several regards, and one whose replication represents a particular 'threat' to the constitutional, legal, and everyday concepts of liberty understood elsewhere in Europe: the most exceptional should not come to be seen as the most normal. At the same time, however, the EU itself in its enthusiasm to create internal 'social inclusion' and coherence is also in danger of embedding naive, security-driven and exclusionary policies into the heart of its project.

The changes must come from the demands of citizens and the work of those researchers and activists. We need to increase and deepen knowledge about living and working in European surveillance societies, to better understand the consequences of technologically enhanced surveillance for social questions, such as equity, cohesion and trust, so that surveillance theorists can better inform citizens and government, and influence future governance and practice, not to mention control and limitation of surveillance. We need to know far more about how surveillance is understood, lived with and resisted in the different countries of Europe, and to spread those lessons so that where surveillance has become normal, it can be made strange and questionable again, and where it remains unusual to keep it the subject of active political debate. Liberties must not be a matter for state manipulation and a constant shifting of the ground under our feet in the name of security. We need to demarcate limits and to resist the idea that living in a world of changing and flexible threats to security means that human rights are equally mutable and ephemeral.

***

References

Aas, K., Gundhus, H. and Lomell, H. (eds.) (2008). *Technologies of InSecurity: The Surveillance of Everyday Life*. London: Routledge.

Association of Chief Police Officers (ACPO) (2007). *The National CCTV Strategy*. London: Home Office (UK).

Agamben, G. (2005). *State of Exception*. Chicago, IL: University of Chicago Press.

Andrejevic (2003). *Reality TV: the Work of Being Watched*. Lanham, MD: Rowman & Littlefield.

Beck (1992). *Risk Society: Towards a New Modernity*. London: Sage.

Bellamy, C. and Taylor, J. A. (1998). *Governing in the Information Age*. Milton Keynes: Open University Press.

Bennett, C. and Raab, C. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Bigo, D. and Bonditti, P. (2009). 'Mapping the field of EU Internal Security Agencies', Report to the *The Changing Landscape of European Liberty and Security*, CHALLENGE Project Final Conference,18 -19 May 2009, Brussels.

Bigo, D. and E. Guild (eds.) (2005). *Controlling Frontiers: Free Movement Into and Within Europe*. Aldershot: Ashgate.

Bunyan, T. (2005). *Unaccountable Europe*. Index on Censorship 2005 (3).

Cabinet Office. (2005) *Transformational Government: Enabled by Technology* (cm.6683). London: HMSO.

Coaffee, J. and Murakami Wood, D. (2006). 'Security is Coming Home: Rethinking Scale and Constructing Resilience in the Global Urban Response to Terrorist Risk', *International Relations* 20(4), pp. 503-517.

Coaffee, J., Murakami Wood, D. and Rogers, P. (2009). *The Everyday Resilience of the City*. Basingstoke: Palgrave.

De Cauter, L (2004). *The Capsular Civilization*. Rotterdam: NAI Publishers.

Deleuze, G. (1990). 'Post-scriptum sur les sociétés de contrôle., *L'autre journal*, 1.

Dillon, M. (2002). 'Network Society, Network-centric Warfare and the State of Emergency', *Theory, Culture & Society* 19(4), pp. 71-79.

Edwards, P. (1996). *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.

Ericson, R.V. (2006). *Crime in an Insecure World*. Cambridge: Polity.

Ericson, R.V. and K.D. Haggerty (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.

Frissen, P. H. A. and Snellen, I. Th. M. (1990). *Informatization Strategies in Public Administration*. Amsterdam: Elsevier Science.

G8 (2003). Presidents' Summary. 'G8 Meeting Of the Ministers of Justice and Home Affairs', Paris, 5 May 2003. Available at: http://www.statewatch.org/news/2003/may/09g8.htm, last accessed 9 July 2009.

G8 (2004). 'G8 Secure and Facilitated International Travel Initiative (SAFTI)'. Available at: http://www.statewatch.org/news/2004/jun/g8-sec.pdf, last accessed 9 July 2009.

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol, CA: O'Reilly.

Gill, M. and Spiggs, A. (2002). *Assessing the Impacts of CCTV*. Home Office Research Study 292. London: Home Office (UK).

Graham, S. (ed.) (2004). *Cities, War and Terrorism: Towards an Urban Geopolitics*. Oxford: Blackwell.

Graham, S. and Wood, D. (2003). 'Digitising Surveillance: categorisation, space and inequality', *Critical Social Policy*, 23, pp. 227-248.

Gras, M. (2004). 'The Legal Regulation of CCTV in Europe', *Surveillance & Society*, 2(2/3), pp. 216-229.

Groombridge (2002). 'Crime Control or Crime Culture TV?', *Surveillance & Society*, 1(1), pp.30-46.

Groombridge, N. (2008). 'Stars of CCTV? How the Home Office Wasted Millions – A Radical Treasury / Audit Commission View', *Surveillance & Society*, 5(1), pp. 73-80.

Hardt, M. and Negri, A. (2000). *Empire*. Cambridge, MA: Harvard University Press.

Haggerty, K. and Ericson, R. (2000). 'The Surveillant Assemblage', *British Journal of Sociology*, 51(4), pp. 605-622.

Hempel, L. and Toepfer, E. (2004). *CCTV in Europe: Final Report (UrbanEye Working Paper 15)*. Centre for Technology and Society, Technical University of Berlin.

Holmes, S. and Jermyn, D. (eds) (2003). *Understanding Reality Television*. London: Routledge.

Honess, T. and Charman, E. (1992). *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*. Home Office Police Research Group, Crime Prevention Unit (paper 35). London: Home Office.

Hunt, A. (2003). 'Risk and moralization in everyday life', in R.V. Ericson and A.Doyle (eds), *Risk and Morality*. Toronto: University of Toronto Press. pp.165-191.

Jermyn, D. (2003). '"This is about real people!" Video technologies, actuality and affect in television crime appeal', in S. Holmes and D. Jermyn (eds) *Understanding Reality Television*. London: Routledge. pp. 71-90.

Kaldor, M. (1981). *The Baroque Arsenal*. New York: Hill & Wang.

Kantor Management Consultants S.A. (2009). *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection. FINAL REPORT*. JLS/2007/C4/040: 30-CE-0185875/00-79, European Commission Directorate-General Justice, Freedom and Security.

Klein, N. (2008). *The Shock Doctrine: The Rise of Disaster Capitalism*. New York, NY: Henry Holt & Co.

Lace, S. (ed.) (2005). *The Glass Consumer*. Bristol: Policy Press.

Law, J. (1994). *Organizing Modernity: Social Order and Social Theory*. Oxford: Blackwell.

Lembke, J. (2002). *Competition for Technology Leadership: EU Policy for High Technology*. Cheltenham: Edward Elgar.

Lianos, M. (2001). *Le nouveau contrôle social : toile institutionnelle, normativité et lien social*. Paris: L'Harmattan.

Lyon, D (1994). *The Electronic Eye: The Rise of the Surveillance Society*. Cambridge: Polity Press.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham and Philadelphia: Open University Press.

Lyon, D. (ed.) (2003). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Loader, I., and Walker, N. (2007). *Civilizing Security*. Cambridge: Cambridge University Press.

MacDonald, F. (2007). 'Anti-Astropolitik: outer space and the orbit of geography', *Progress in Human Geography,* 31(5), pp.592-615.

Matthiessen, T. (1997). 'The Viewer Society: Michel Foucault's "Panopticon" revisited', *Theoretical Criminology*, 1(2), pp.215-33.

Metz, S. (2000). *Armed Conflict in the 21st Century: The Information Revolution and Postmodern Warfare*. Carlisle, PA: Strategic Studies Institute.

Monahan, T. (ed.) (2006). *Surveillance and Security: Technological Politics and Power in Everyday Life*. Routledge.

Murakami Wood, D. (ed.), Ball, K., Lyon, D., Norris, C. and Raab, C. (2006). *A Report on the Surveillance Society*. Information Commissioner's Office (ICO) (UK).

Murakami Wood. (2009). 'The Surveillance Society: Questions of History, Place and Culture', *European Journal of Criminology*, 6(2) pp.179-194.

Murakami Wood, D. and Coaffee, J. (2007). 'Lockdown! Resilience Resurgence and the Stage-set City', in R. Atkinson and G. Helms (eds) *Securing an Urban Renaissance*. Bristol: Policy Press. pp. 91-106.

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

Orwell, G. (1949). *Nineteen Eighty-Four*. London: Martin, Secker and Warburg.

Palmer, G. (2003). *Discipline and Liberty*. Manchester: Manchester University Press.

Poynter, K. (2008). *Review of information security at HM Revenue and Customs. Final report*. London: HMSO.

Rose, N. (2000). 'Government and Control', *British Journal of Criminology* 40, pp 321-339.

Samatas, M. (2004). *Surveillance in Greece: From anti-communism to Consumer Surveillance*. New York, NY: Pella.

Schneier, B. (2008). *Schneier On Security*. Indianapolis, IN: Wiley.

Smith, G.J.D. (2004). 'Behind the Screens: examining constructions of deviance and informal practices among CCTV control room operators in the UK', *Surveillance & Society,* 2(2/3), pp.376-395.

Smith, G.J.D. (2007). 'Exploring Relations Between Watchers and Watched in Control(led) Systems: Strategies and Tactics', *Surveillance & Society*, 4(4), pp.280-313.

Scientific and Technological Options Assessment Sub-Committee (STOA) (1998). *An Appraisal of Technologies of Political Control*. Directorate General of Research: Brussels: European Parliament.

Statewatch (2004). G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel. Available at: http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm, last accessed 9 July 2009.

Taylor, J. A., Lips, M. and Organ, J. (2009). Identification Practices in Government: Citizen Surveillance and the Quest for Public Service Improvement, *Identity in the Information Society* (forthcoming).

Varney, S. D. (2006). *Service Transformation: A Better Service for Citizens and Businesses, a Better Deal for the Tax Payer*. Norwich: The Stationary Office.

Webster, C.W.R. (2009). 'CCTV Policy in the UK: Reconsidering the Evidence Base', *Surveillance & Society*, 6(1), pp. 10-22.

Webster, C.W.R. (2004). 'The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK', *Surveillance & Society*, 2(2/3), pp. 230-250.

Webster, C.W.R. (1996). 'Closed Circuit Television and Governance: The Eve of a Surveillance Age', *Information Infrastructure and Policy*, 5(4), pp. 253-263.

Welsh, B.C. and Farrington, D.P. (2002). *Crime Prevention Effects of CCTV: A Systematic Review*. Home Office Research Study 252. Home Office (UK).

Welsh, B.C. and Farrington, D.P. (2008). *Effects of Closed Circuit Television Surveillance on Crime*. Campbell Systematic Reviews 2008:17. Oslo: The Campbell Collaboration.

Whitehead, T. (2009). Spy Chief: 'We risk a police state', *The Daily Telegraph* (London), 17th February. Available at: http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/4643415/Spy-chief-We-risk-a-police-state.html, last accessed 9 July 2009.

Williams, C.A. (2003). 'Police Surveillance and the Emergence of CCTV in the 1960s', *Crime Prevention and Community Safety,* 5(3), pp. 27–37.

Williams, C.A. (2009). 'Police filming English streets in 1935: the limits of mediated identification'. *Surveillance & Society,* 6(1) pp.3-9.

***