*Information & Communications Technology Law*
Vol. 17, No. 1, March 2008, 25–35

Routledge
Taylor & Francis Group

# Law, privacy and information technology: a sleepwalk through the surveillance society?

Mark O'Brien*

*School of Law, University of the West of England, Bristol, UK*

The Surveillance Studies Network report of 2006 on the 'surveillance society', highlighting the omnipresence of information technology in British society, once again brought into sharp focus concerns about the types and levels of technological surveillance to which the public are subjected. This article seeks to explore the opportunities for surveillance presented by recent developments, and suggests a number of privacy and civil liberties concerns.

**Keywords:** privacy; society; surveillance; technology

## Introduction

The continued development of information technology has had a huge impact upon many aspects of our lives in the last quarter century, changing much of what we do in our personal and professional existences, and also how we do it. One of the many consequences of the near-ubiquity of information technology in modern-day society is the potential now afforded for the surveillance of individuals and the storage and dissemination of such information about a huge number of the – often seemingly unremarkable – day-to-day activities that we undertake. Public, academic, governmental and media concern frequently is focused on the impact of the 'information revolution' upon our lives, in particular where this interface impacts upon our ability to lead a *private* life.

The aims of this article are to seek to examine the nature of the technical developments that have resulted in a more 'surveilled' society, exploring how these technical changes have led not only to an ability to allow observation to take place with greater frequency (but not always necessarily accuracy) in a multiplicity of ways, but have also led to the development of new, hitherto unknown modes of surveillance, the development of which would not have been possible without the impact of advancing technology. To illustrate this, this article will focus upon the surveillance of data in the context of combating crime, specifically including the detection and deterrence of the viewing and proliferation of illegal Internet pornography, and the detection and prevention of certain instances of serious public disorder. As will be seen, I will contend that recent developments in this sphere can result, in both predicable and unpredictable ways, in an inappropriate imbalance between the societal need for surveillance and the concomitant individual need for privacy.

*Email: mark.o'brien@uwe.ac.uk

ISSN 1360-0834 print/ISSN 1469-8404 online

DOI: 10.1080/13600830801887214
http://www.informaworld.com

## Concepts of privacy

In order to give meaning and context to a discussion on surveillance, and to explore why too much surveillance is regarded as undesirable, it is first necessary to examine the development of, and differing notions within, the privacy debate and the relationship of that debate with surveillance. As many commentators recognise, despite the nebulous nature of the concept, with the literature, according to Wacks, lacking a 'lucid or consistent meaning of privacy' (Wacks 1993: xi; Fenwick 2000: 338), and with debates regarding to what degree rights and privacy have value in different types of societies (Dembour 2001), the links between surveillance and privacy generally are seen as competitive with each other (Bloss 2007: 208) and deep-rooted, particularly in the culture of Western liberal democracies. It is, therefore, useful to begin this analysis with an exposition of the development of privacy, and why we give it value.

### *Historical development of privacy*

Meaningful, recorded references to privacy-based ideas stretch back to the work of Aristotle and his bifurcation of the private or the family from the political and the public. This public-private divide concept was developed, post-Enlightenment, by the liberal theorists. John Locke advanced arguments that in nature, all the world's goods are common to all, but that property could be acquired and thus became private by the mixing of the public property with the person's own (private) labour, rendering the end product private property. Similarly, in *On Liberty* (Mill 1994), John Stuart Mill argued for a realm for self-regulation and a separate, narrowly-defined area for government responsibility.

Moreover, the intervening period has seen different emphases being applied to the factors that are considered as constituting privacy 'rights', with some commentators asserting that privacy in relation to information about the individual, or *informational* privacy is of primary concern (Warren & Brandeis 1890; Westin 1967; Fried 1970); that privacy is important for the development of the individual capable of the relationships of love, trust and friendship (the notion of *intimate* privacy) (Fried 1970). There is also a notable body of work that seeks to critique the burgeoning arguments pertaining to privacy rights that emerged during the late 19th and 20th centuries; broadly speaking, the critics of those that elevate privacy rights question whether a set of concerns that can be labelled 'privacy rights' actually exist, alternatively contending that the so-called 'privacy issues' can be 'defended ... in terms of standard moral and legal categories' (Schoman 1984: 5). The proponents of this approach – the reductionists – therefore reconsider 'privacy' issues as part of other interests, such as proprietorial rights (see Thompson 1975; Posner 1981).

There also exist a number of feminist critiques of traditionally-conceived privacy debates, which highlight the perceived dangers accorded by the absence of the public realm from private situations when women may need the assistance of the State to combat harm (MacKinnon 1989).

### *Reasons for 'valuing' privacy*

The development of the modern ideas of privacy relevant to the development of this article, however, are those widely ascribed to the body of academic literature that advances what Fenwick (2000: 338) broadly describes as 'informational autonomy' – that is the right to control the information about ourselves – as the central privacy value, for reasons that shortly will be explained. The catalyst for, in particular, United States

common law development along these lines, and the more sustained exploration of the concept of privacy generally, including international human rights measures, is often attributed to the 'seminal' (Feldman 2002: 156) 1890 Harvard Law Review article 'The Right to Privacy', written by Samuel Warren and Louis Brandeis (Warren & Brandeis 1890). This essay argued that, due to a combination of 'the right to be let alone' and a range of political, social and economic changes in the late 19th century, which included the advancement of technology, contemporaneous law could be employed to protect individual privacy, of interest in the face of then-new technological developments such as photography (McRobb & Stahl 2007).

Moreover, to justify their privacy argument, Warren and Brandeis advanced the concept of the 'inviolate personality' (Warren & Brandeis 1890: 215), which in essence meant that people required a 'protected field of decision making', for happiness and in order to conduct their own affairs as best as they could (Feldman 2002: 516). This broad view of the role served by privacy is advanced by numerous later academics and theorists (Bloustein 1964; Westin 1967; Fried 1970; Gerstein 1978; Lustgarten & Leigh 1994), with emphasis upon links between the individual's control of information about themselves, but also links on to outcomes that protect the importance of human dignity – those goals 'which may be seen as essential to human flourishing' (Fenwick 2000: 339).

These essentially instrumentalist arguments for privacy rights can and have been advanced in conjunction with arguments for privacy rights that have an intrinsic base; this is, the right to privacy is advanced for its own sake as a self-evident 'good' or a 'human right', rather than being viewed solely or in part as a tool to facilitate the advancement of other goals that are seen as being of value (McRobb & Stahl 2007: 234). The most significant instance of this, as will be discussed below, being the incorporation of the Art 8 right to privacy enshrined in the European Convention on Human Rights (ECHR) into United Kingdom domestic law by the Human Rights Act 1998.

### *Concepts of privacy in law*

Despite some early scepticism, practical developments in jurisprudence followed the initial embrace by the US legal community of Warren and Brandeis's arguments for privacy to be assigned a legal value, with Judge Thomas Cooley arguing for a right to be 'let alone' (Cooley 1888: 29), and the concept being embraced by the United States Supreme Court in *Union Pacific Railway Co v Botsford* (1891) 141 US 250 at 251.

Practical developments regarding privacy in UK law were, for a considerable period however, less significant. Despite the concept of the 'peace' gaining an early importance in the early stages of English law, alongside the principle that a person's home and family life were to be free from intrusion (Feldman 2002: 542), this concept does not appear to have developed in an all-encompassing way, rather attaching itself solely to property rights, leaving the equity system to deal with quasi-'privacy' rights. Nor did this situation improve throughout the late 19th century nor most of the 20th century; in 1972, the Report of the Younger Committee on Privacy highlighted the difficulty associated with the actual definition of a privacy right, and in the case of *Malone v Metropolitan Police Commissioner (No.2)* [1979], Megarry VC explicitly ruled out a privacy right based either on US common law or derived from the ECHR – a position in contravention of Art 8 of the at-the-time unincorporated ECHR to which the United Kingdom was a signatory.

The position of privacy in the law of the UK was definitively changed not, as indicated by the above case, by the UK being signatory to the various international instruments pertaining to the protection of human rights, but by the incorporation of the Art 8 privacy

provisions of the ECHR into UK domestic law by virtue of the Human Rights Act 1998. There does remain some debate, however, about the impact of the nuances of language between the different conceptions of privacy. Feldman (2002) highlights that the Art 8 right denotes *respect for* 'private and family life, home and correspondence', rather than a right to be *free* from privacy interference, and contends that this could lead to the possibility of an interference – for example, paternalistic – with privacy that would be consistent with the European Convention provision, though he concedes that the right does represent a 'considerable' extension (Feldman 2002: 524).

## The development of surveillance

It is against this backdrop of developments in privacy, and their interaction with surveillance, therefore, that this article explores the role that surveillance has played and is continuing to develop in society, particularly as a consequence of developments in information technology.

The concept of surveillance has in itself existed for hundreds of years (Foucault 1977; Bentham 1996; Fenwick 2000), has been widely employed throughout that time by countries and organisations with varying degrees of success, and its periodic use is regularly and relatively uncontroversially characterised as a necessary part of a democratic society. States and their governments usually do retain a right to utilise surveillance techniques in legally ascribed circumstances to protect their legitimate interests – for example, the reaction against persons or groups that seek to overthrow democratic government, or those who seek to indulge in terrorist acts – and in such circumstances an 'approach which succeeds in preserving respect for democracy and for ... individual privacy, as a hallmark of democracy, while affording respect to state interests' (Fenwick 2000: 339) is one that is valued.

The development of the information society and its attendant technological advances, however, has placed into focus both the development in the extent and nature of the surveillance that can and does take place in society and how traditional understanding of these concepts has changed.

### *Definitions of surveillance*

Until the information revolution, surveillance predominantly had consisted largely of 'physical surveillance'; that is, the act of physically listening to or watching the actions of a person. In the course of the past three decades, however, society's understanding of surveillance and the extent of its operation significantly have expanded. Several different categorisations of surveillance have resulted from this, including (but not limited to) 'personal surveillance' versus 'mass surveillance' (Clarke 1997) and Alan Westin's early model of characterising surveillance as 'physical surveillance', 'psychological surveillance' (i.e. psychometric testing, interrogation and the triangulation of data), and 'data surveillance' (Westin 1971).

The sphere of data surveillance (or 'dataveillance' (Clarke 1997)) is one area where, due to computerisation and networking, especial change has taken place. By focusing at this stage, by way of example, upon merely non-governmental surveillance (as distinct from State surveillance, which is the main focus of this article), considerable changes in terms of data surveillance and the ready availability of everyday information about the individual (and thus the consequent impact upon the private/public divide in relation to conceptions of privacy) are evident. A shift from payments for goods and services with (anonymous)

cash to (identifiable) electronic funds transfer (EFT) transactions, store loyalty cards, electronic withdrawal of funds from bank automatic transaction machines (ATM) (which also note the time and location of withdrawal) rather than traditional over-the-counter transactions are just limited examples of the multiplicity of complex ways that illustrate that citizens automatically are subject to a 'passive' (Lloyd 2003) process of data surveillance. Similarly, the consumer can be rendered the subject of marketing (whether by email, telephone or other means) campaigns on the basis of information held on the databases of companies and traded between companies. Subject to the limitations of the legal protection to privacy and identity afforded by measures such as the Data Protection Act 1998, such as the requirement for an individual to have their information held securely, or the legal right to prevent personal details being utilised for the purposes of marketing or associated activities, this information can easily be bought, sold and utilised in relation to actual and projected customers.

Another example of non-governmental surveillance exists in the workplace, with the potential for computer keystroke speed to be automatically measured, emails to be monitored for personal use or for what an employer deems inappropriate language, telephone conversations, call data and other communications to be recorded, and computer file caches automatically monitored for web-browsing habits, unauthorised behaviour, or any illegal activity (O'Brien 2005).

**Surveillance and crime**

Despite the all-pervasive impact both of physical and data surveillance in the contexts of business and e-commerce, with a concomitant impact upon the 'protected field of decision making' identified within the concepts of privacy rights, some of the most significant developments in relation to technological advancement and surveillance have occurred in relation to attempts to utilise the developing technologies to combat crime. Prior to the onset of the information revolution, a panoply of physical surveillance accompanied by some data surveillance techniques were widely employed; these included 'traditional' modes of physical surveillance – such as the interception and opening of letters, scrutinising relevant documents, and once the relevant technologies had sufficiently developed, the application of a range of aural surveillance techniques to private telephone lines to hear what was being said in a particular location.

The considerable developments in technology over the last 30 years, however, have greatly expanded the possibility of an increased level of existing types of surveillance, as well as the instigation of different types of surveillance, including the harnessing of technology to combat crime, employing new methods to augment existing physical surveillance and also adding a portfolio of data surveillance tactics.

At the same time as – and at least partly as a consequence of – the increased prevalence and application of technology, the UK also developed new, so-called 'proactive' models of policing. Prior to the adoption of the 'proactive' policing model in the UK, police forces mainly operated in a way, according to Newburn (2003), which was 'opportunistic and responsive ... dealing with individual offences reactively and trying to solve them one at a time as evidence happens to be available'.

However, the reputation and effectiveness of this familiar approach to policing was brought into question by inner-city riots in 1981 in Toxteth in Liverpool, Handsworth in Birmingham, St Paul's in Bristol and in Brixton in London, the growth in football hooliganism of the period, the year-long miners' strike and several instances of mass trespass involving counter-cultural groups (O'Brien & Ashford 2002–03), and which all

lead to the adoption of the 'proactive' model of policing, focusing upon a prevention of criminality and police intelligence-gathering activities. The rapid development in and increased potential for the application of information technology has meant that technology is now capable of playing a significant role in fulfilling many of the UK's goals in respect of a proactive policing policy. This includes the use of a variety of computer software as part of the Police National Computer for the analysis and the mapping of crime patterns, the use of technology to identify crime patterns across the boundaries between different forces to aid crime detection at regional or national levels, and also (as part of the 'proactive' agenda) to help predict what sort of crime is likely to committed, and where that crime is likely to be committed, in order to police different districts or implement effective crime-prevention strategies.

In relation to 'traditional' manifestations of physical surveillance, electronic developments and improvements in the technical process have resulted in the physical interception of calls becoming easier (Fenwick 2000: 341), with the equipment needed for aural surveillance being compact, easily accessible and cheap (Taylor & Walker 1996). Recording and storage media, and the surveillance devices also, have been improved. In addition, new forms of physical surveillance have become common. The closed-circuit television (CCTV) device, although first employed in a criminal law capacity in 1956 when police in selected forces began to use this 'proto'-red light camera to film drivers ignoring red lights at traffic signals, was increasingly used by the retail sector from the 1970s onwards, and has been extensively employed for surveillance within the public sphere – public spaces, streets, town centres, and places where the possibility of attacks are of concern – for the last 15 years. As a consequence, one estimate is that the UK has five million CCTV cameras, with it being mooted that there is the potential for some citizens to have their movements closed-circuit television recorded up to 300 times in a given day (O'Neill 2006).

Fundamental changes have taken place, however, in the utilisation of data surveillance techniques in the enforcement of the criminal law. A wide range of new or relatively new modes of data surveillance (or tactics that combine physical surveillance with data surveillance to achieve an outcome) have been developed. A non-exhaustive list includes:

(1) *changes relating to road traffic law enforcement* – using automatic number plate recognition systems (ANPR), road-safety cameras, red-light cameras, mobile enforcement cameras, all of which employ an approach that combines physical surveillance (the camera) with data surveillance (comparing the offending photographic evidence with the electronic version of registration document held on the Driver and Vehicle Licensing Agency's database);
(2) *predicting, preventing and quelling serious civil disturbances, possibly linked to public order offences* – utilising closed-circuit television cameras, electronic and physical surveillance; and
(3) *preventing certain serious crimes or terrorist and potential terror-related activities* (a particular preoccupation in relation to surveillance post-2001) – adopting electronic surveillance tactics, DNA sampling and the DNA database, forensic examination of evidence, surveillance of email communications, and obtaining evidence of deleted and undeleted computer material held in computer caches or on computer storage media. Additionally, wider array of tools employed include monitoring so-called email 'chatter' – the prevalence of email communications from sources previously identified as in some way 'suspect' – and the interception of communications and counter-espionage.

### *The legal framework*

There is, as has previously been discussed, a legal framework within which both physical surveillance and data surveillance are regulated, whether the surveillance be in the course of e-commerce and associated matters, or in relation to surveillance undertaken with the view of combating some form of crime. The Data Protection Act 1998, in conjunction with European Union measures, provides a statutory framework in relation to the use of personal information, whereas the UK's traditional approach to surveillance relating to state activities, sometimes regarded as limited, fragmentary and devoid of substantive rights for the individual (Feldman 2002; Mirfield 2001), was bolstered by the incorporation of the ECHR into domestic law by virtue of the Human Rights Act 1998 and the passage of the Regulation of Investigatory Powers Act 2000.

This latter measure, introduced as a 'codifying' measure (Feldman 2002) to regulate instances of directed surveillance, intrusive surveillance and covert intelligence, provides for the first time a comprehensive framework for surveillance regulation, but has received a mixed reception from academics. Whilst it does provide a framework for the regulation of such activities, and the opportunity for review via the Surveillance Commissioners (whose positions were created by the legislation), commentators have expressed concerns about the processes by which the government has extended powers in this sphere (Feldman) and about how some measures, whilst legal, lack moral acceptability (Mirfield 2001).

## Data surveillance problems

Of particular interest to this article, however, are aspects of the recently developed methods of data surveillance that have become prevalent. Some aspects of these methods, although ostensibly compliant with the relevant legal frameworks, are flawed, with the consequences that personal privacy is invaded to a degree that, in terms of rights protection, can be regarded as excessive, and also that the privacy invasion is not recognised as such, with potentially a consequent subversion of the interests of justice.

A definitive study of all aspects of all flaws, potential and actual, relating to the many aspects of surveillance found in society today clearly is beyond the scope of an article such as this, if indeed all such flaws could easily or exhaustively be identified, so I shall adopt a thematic approach, exploring problems that can be demonstrated to have emerged from technology used for the specific purpose of data surveillance with the goal of combating criminal activity in the UK. The purpose, therefore, is to provide salient examples of particular problems, not to formulate a rigorous critique of the use of data surveillance techniques, but rather to highlight the potential for wider problems and counsel for the need to be more cautious in the employment and interpretation of the relevant methods.

### *(i) Function creep*

The potential for function creep has long been recognised as an issue in relation to data gathering and data retention generally, and pre-empts the advent of the information revolution. Function creep occurs when data gathered by surveillance methods for a defined, specific purpose, and recognised as being gathered for that specific purpose, is subsequently used to provide information pertaining to different objectives. Notable examples of this, prior to technological advancement, include the use by Artur Seyss-Inquart's World War II administration of Nazi-occupied Holland of the Dutch census records to identify citizens of Jewish origin for deportation to the concentration camps

(Lloyd 2003). Another was the US government's use of lists held by an ice-cream company that the company utilised in order to provide promotional ice cream to each American on their 18th birthday; the government used this list to enhance the information that it already held in order successfully to identify so-called Vietnam war 'draft dodgers.'

The reasons for function creep can be argued to include value-for-money considerations – that the considerable money often invested in relevant technologies can or should be recouped by their wider application (Ponder 2007) – and for the protection of the citizen, and one situation where a 'joined-up' approach to existing data was identified as potentially being of use was in relation to information held by various social services agencies on the mistreatment and ultimate death of the eight-year old Victoria Climbie in February 2000, when Lord Laming, the Chairman of the Inquiry into her death, suggested that a National Children's Database be established for the efficient interchange of information (Laming 2003).

Despite some initial reluctance by the courts to allow function creep in relation to data surveillance, with Sir Nicolas Browne-Wilkinson, in *Marcel v Metropolitan Police Commissioner* [1991], expressly forbidding multi-agency access to documentation and describing 'the dossier of private information' as 'the badge of the totalitarian state', there have been a number of moves towards permitting function creep. In July 2007, the Home Secretary Jacqui Smith signed an order allowing an exemption from the provisions of the Data Protection Act 1998 in relation to data held by Transport for London, the body that administers the capital's road-congestion charge. This was to allow the data, collected for administering the fees system in relation to the congestion charge, to be utilised by the Metropolitan Police when investigating threats to national security. Information emerged in the same month regarding police wishes to obtain such congestion charge data for 'all crime fighting purposes' (Travis 2007) – a rather open-ended notion. Further development seems likely. In May 2006, the then UK Constitutional Affairs Minister Harriet Harman told a meeting of the policy group Progress that the National Identity Register (NIR), which was under development in connection with ID cards, could be used for correcting errors in the electoral roll, despite the Identity Cards Act 2006 expressly providing that information on the NIR could only be used in connection with detecting or preventing terrorism, identity fraud, social security fraud and organised crime (Taylor 2006.)

### *(ii) Complexity and error*

The increased sophistication of the technology employed in order to undertake new forms of data surveillance and the resultant complexity of the evidence-gathering and forensic processes necessary to support such data surveillance introduce into the equation a range of new problems; for example, the increasingly technically complex evidence-gathering processes, and the linked but separate need to introduce more forensic, physical and administrative processes into the *interpretative* processes necessary to give this evidence readily-understandable meaning, both for investigators and for later stages in the criminal justice process such as jury trials, means that the various levels of greater complexity give rise to the potential for greater procedural and interpretive error.

A number of examples of the potential for greater procedural and interpretive error above exist. One such issue manifested itself during the course of Operation Ore, one of the major worldwide inquiries that have taken place in recent years into the distribution of child pornography via the Internet (O'Brien 2005). Here, worldwide investigations were triggered by a raid by US federal authorities on a US company, Landslide, the owners of which were successfully prosecuted for distributing child pornography. What was novel

about this case was that the investigation concentrated upon the fact that rather than offering the relevant illegal pornographic material itself, the company provided a portal through which customers could obtain pornographic material from external, independent sites. The situation in terms of the detection and identification of *offending* customers via data surveillance of the company's lists of the names and addresses of subscribers appears to have been further complicated by Landslide also offering a range of legal material via their portal service. Consequently, instead of there being a straightforward, easily provable 'real world' connection between the illegal material and the customer, the evidence consisted of lists of names and addresses, forensically obtained from seized computers, and derived from credit card details that had been used to purchase material from the company. Therefore, in order to identify those that potentially had committed criminal acts: (i) the forensic examination of the seized computers' storage media and subsequent conversion of the data into a meaningful and readable form had to be without technical flaw or human error, especially given the level of trust that would be placed in this evidence by (possibly technically unversed) judges and juries (O'Brien 2005: 159); (ii) those undertaking the extraction of data forensically needed to be suitably qualified and competent to undertake the task; (iii) the data obtained, if accurate, had to be transcribed properly for dissemination to and amongst the investigative authorities worldwide; (iv) in the circumstances, as posited here, of the details of purchasers of legal material being mixed with the purchasers of illegal material, appropriate examination of the data source should take place to prevent infringement of the rights of those demonstrably innocent of the alleged activity; and (v) if this information was derived from credit card details, then due consideration needed to be given to the possibility of credit card fraud, especially given the illegal nature of the activities either by the unauthorised use of a card or by the fraudulent opening of an account in another person's name.

However, in the above instance, the likelihood of flaws in the processes adopted was been identified (Bates 2004). Even assuming that all personal details related to those who accessed illegal material (in this scenario highly unlikely), the *full* list of names and addresses provided to law enforcement agencies in the UK appears not to have been the actual list of 'raw data' as obtained by the Federal Bureau of Investigation (FBI), rather a list prepared by a firm of forensic specialists in the UK (Hamilton 2004); therefore there was the attendant possibility of transcription and other errors, both in the raw and interpreted data.

In relation to the issue of which 'list names' (though at this stage not considering the attendant issue of whether the 'name' and the person were one and the same) had accessed legal material, and which has accessed illegal, the technical arrangements caused further complexity. It was suggested by investigators that the (KEYS) portal (rather than the (AVS) portal) provided access to the illegal, child pornography, material; thus it was assumed that if a 'name' was registered with the KEYS portal, then that was for the purpose of downloading illegal material. However, it has been noted that this was a flawed argument – solicitors acting for accused persons highlighted evidence that the relevant KEYS portal also provided legal, adult pornography, and that, therefore, the *technical* evidence of accessing the relevant portal does not *of itself* necessarily provide evidence of commission of a criminal act (Hamilton 2004.) Moreover, the point regarding credit card fraud appears to have been little considered by the investigative authorities, with warrants for raids being issued by magistrates in the UK on the basis of 'reasonable suspicion' derived the (interpreted) data initially obtained from the FBI.

Similar issues increasingly are being identified in relation to other complex analyses of material obtained by data surveillance. The interpretive processes implicit in the use of

DNA evidence, and particularly the matching of DNA samples from scenes of crime with the UK's burgeoning DNA database has raised concerns. These include different and potentially inconsistent procedural processes being adopted by different teams of forensic investigators; in February 2007 it was announced that there would be case reviews where examinations involved a procedure known as Low-Copy Number DNA sampling (utilised where only very small quantity or minimal traces of DNA are present) as it transpired that the Home Office Forensic Science Service analyses of such samples differed from those adopted by external scientists and laboratories, with the obvious potential for differing results (Holden 2007).

### *(iii) Contextual issues*

A further issue manifests itself in relation to 'cause-and-effect' arguments *per se* in this sphere, both generally and more specifically in relation to the impact of these issues upon the administration of justice.

Wood et al. (2006) argue that the skewed nature of contextual issues is impacting upon how data surveillance policy has evolved and is evolving, with a consequent impact upon privacy. They suggest that a presentation of arguments in this sphere as simple 'cause-and-effect' (for example assertions that 'More CCTV cameras lead to less crime' (Wood 2006) or perhaps 'DNA samples are a foolproof way of accurately identifying the perpetrator of a crime', or even 'People whose name is on our list are paedophiles who will be punished') ignores the complex reality implicit in each area, and potentially impacts upon both development of policy and also public perception and understanding of the issues involved. This demonstrably has a practical impact: a Home Office study led by Professor Martin Gill of Leicester University examined the impact of CCTV systems in 14 areas in the UK and found that a drop in levels of crime could be linked to CCTV in only one of those locations.

However, it is the extremities of these (headline-grabbing) wider debates, rather than the nuances of technical or academic argument, that drive public and media perception (Wood et al. 2006). By way of example, on 26 April 2002, *The Sunday Times* newspaper presented information on the seized lists of names from the Landslide company discussed above, described as ' ... voyeurs in a cyber-world of depravity', whilst conceding in the same article that some of the names were 'demonstrably false'. Such approaches, when linked to an understandable and entirely justifiable ignorance of obtuse technical detail, have a possible impact in the court room. Recorded instances of 'cause-and-effect'-style arguments employed in cases include evidence of attempts to present a possibly automatically-generated computer username with an attached numerical suffix, e.g. 'JoeBloggs14', as evidence that points to attempts to masquerade as a child (Bates 2003), and one instance where an advocate said that a computer 'contained images of children' (that is, not necessarily *indecent* images of children.)

## Conclusion

The concept of privacy, and how we undertake the balancing of privacy protections with the other justifiable goals of a society, especially issues such as preventing crime and ensuring national security, has long been a contentious issue, and is rendered more so by current concerns regarding issues such as Internet pornography and 'global terrorism' in the post-9/11 environment, with what has been described as a 'progressive shift between police surveillance authority and individual privacy' (Posner 2003; Chang 2003;

Bloss 2007). Pressure from governments can be demonstrated to exist, including the UK government, in relation to the issues explored within this article, for a heightened – or even an overriding – importance to be attached to issues of security. However, the importance of privacy rights in a democratic society demands that the privacy/security tension is fully debated in an open and rational way, devoid insofar as is possible of rhetoric and sensationalism, with an assessment of some of the difficulties.

As a consequence of the above issues, therefore, it can be seen that via a range of technical and contextual means, including the issues of appropriate and inappropriate function creep, the increasingly complex nature of the technical processes and attendant issues associated with forensic examination techniques, and issues regarding the wider arguments in society in relation to data surveillance, its usefulness and how those debates are presented, in combination have an impact upon current debates justifying greater surveillance. This has a consequent direct (and as have been seen, perhaps unnecessary) impact upon our collective ability to lead our individual, private lives. As Lustgarten and Leigh (1994) argue in the wider context of this debate, 'in attempting to protect democracy from threats [...] there is an ever-present risk that ... that which was to be preserved has been lost'.

## References


Bloustein, C (1964) Privacy as an aspect of human dignity, in Schoman F (ed), *Philosophical Dimensions of Privacy*, New York: Cambridge University Press.

Bloss, W (2007) Escalating U.S. police surveillance after 9/11: an examination of causes and effects, *Surveillance and Society*, *4*(3), Part 1, 208.

Dembour, M-B (2001) Following the movement of a pendulum: between universalism and relativism, in J Cowan, M-B Dembour and R Wilson (eds), *Culture and Rights*, Cambridge: Cambridge University Press.

Feldman, D (2002) *Civil Liberties and Human Rights in England and Wales*, Cambridge: Cambridge University Press.

Fenwick, H (2000) *New Labour, Freedom and the Human Rights Act*, Harlow: Longman.

Fried, C (1970) *An Anatomy of Values*, Cambridge: Harvard University Press.

Gerstein, (1978) Intimacy and Privacy, *Ethics 89*(1), 76–89.

Hamilton, A (2004) *Recent Developments in the Law Regulating Child Pornography on the Internet*. Available at: <http://www.hamiltons-solicitors.co.uk/archive-docs/operation-ore.htm>. Accessed 21 December 2006.

Holden, (2007 December 21) Court cases to be reviewed over DNA concerns, Reuters.

Lustgarten, L and Leigh, I (1994) *In From the Cold: National Security and Parliamentary Democracy*, Oxford: Clarendon.

MacKinnon, C (1989) *Toward a Feminist Theory of the State*, Cambridge: Harvard University Press.

McRobb, S and Stahl, B (2007) Privacy as a shared feature of the e-phenomenon: a comparison of privacy policies in e-government, e-commerce and e-teaching, *International Journal of Information Technology and Management*, Nos 2-4, 232.

Schoman, F (ed) (1984) *Philosophical Dimensions of Privacy: An Anthology*, New York: Cambridge University Press.

Stahl, B (2002) The moral and business value of information technology: what to do in case of a conflict?, in N Shin (ed), *Creating Business Value with Information Technology: Challenges and Solutions*, Hershey, PA: Idea-Group Publishing.

Taylor, (2006) Anger AS Harman electoral role for ID database, *The Guardian*, 11/5/2006.

Wacks, R (ed) (1993) *Privacy*, New York: NYU Press.

Westin, A (1967) *Privacy and Freedom*, Atheneum: New York.