Article

A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance Systems

Nick Taylor

School of Law, University of Leeds, UK. N.W.Taylor@Leeds.ac.uk

Abstract

The United Kingdom uses visual surveillance techniques on a huge scale, but its regulation of those techniques has been sadly lacking. This paper seeks to consider the extent to which the European Convention on Human Rights (ECHR) provides an overarching framework for the regulation of visual surveillance practices, both overt and covert, thereby bringing about the conditions for accountability and transparency, and to critically analyse the extent to which UK law operates within that framework so far as it applies to video surveillance.

Introduction

In the context of regulation in the use of surveillance systems the United Kingdom has rarely been seen as an exemplar. Throughout the 1980's and 1990's the UK government lost a series of cases in the European Court of Human Rights concerning the unlawful use of different state surveillance practices. At the same time, the use of video surveillance grew exponentially in the absence of legal regulation. This paper seeks to consider the extent to which the European Convention on Human Rights (ECHR) provides an overarching framework for the regulation of visual surveillance practices, both overt and covert, thereby bringing about the conditions for accountability and transparency, and to critically analyse the extent to which UK law operates within that framework so far as it applies to video surveillance.

The Framework

The framework for the regulation of surveillance in the UK is multi-layered. It is well recognised that the law in books is not the same as law in action (Dixon, 1989) and therefore when considering regulation both the principle and the practice have to be considered. In addition, domestic law in the UK also operates within an overarching European framework, and this too must be considered in order to understand how domestic law ought to be interpreted and practiced. McKay has considered a similar approach in the context of covert police work (McKay, 2006), seeing the need to consider the conceptual, substantive and practical issues. Conceptual issues, in the context of this piece, are provided by the ECHR and the standards it sets for the ethical operation of state surveillance. Substantive issues relate to domestic law, its objectives, meaning and standards. Finally, the practical perspective looks at the implementation of the law at operational level and whether this reflects the ethical standards envisaged in the conceptual framework.

Taylor, Nick. 2011. A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance Systems. *Surveillance & Society* 8(4): 455-470.

<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author, 2011 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

The Conceptual Context

The ECHR, given ‘further effect’ by the Human Rights Act 1998 provides a legal framework within which the UK, as a signatory state, must operate. In the context of surveillance operations, it can bring with it two clear ethical demands: namely, issues of due process and substantive standards. However, these demands are only required if the Convention is ‘engaged’, more specifically, if the rights it provides are ‘interfered with’ by the particular surveillance operation. Surveillance activity may affect a number of different rights. The way a surveillance operation is effected could impact upon an individual’s right to a fair trial through the way in which evidence is gathered and subsequently used, or may have a chilling impact upon an individual’s right to assemble or their right of free expression (Slobogin, 2002). However, the right most obviously affected by surveillance and the most pertinent for the purposes of this piece, is the right to privacy, or its near equivalent in the ECHR, the right to respect for private life. As the Supreme Court of Canada has observed, “One can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance” (*R v Duarte* (1990) at 249).

Privacy: underlying values.

In order to consider the extent to which surveillance practices infringe upon privacy and therefore what policies for protecting privacy may be necessary, it is important to consider the values which might underpin the somewhat nebulous concept.

It is argued that whenever ‘privacy’ is invaded it is, in truth, the violation of some more specific interest that comes under the privacy ‘umbrella’. Further, it is recognised that the specific interests, or values, underpinning privacy are in many ways dependent upon cultural tradition. Therefore, despite many official pronouncements of the position of privacy as a fundamental right, there is less of a consensus as to what values are actually being protected. Some consider that the core value of privacy is perhaps limited to ‘secrecy’ (Jourard, 1996); the withholding of information from others or non-disclosure. Others, however, argue that ‘secrecy’ does not engage privacy at all, suggesting that individuals are not so interested in non-disclosure of information about themselves, but selective disclosure. Westin’s influential account suggested that “privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967: 7). Others argue that such a concept might be too narrow however as it fails to account for those aspects of privacy which are not informational, such as the right to make fundamental decisions about the rearing of one’s children (Solove, 2002). It is also vague in that it fails to account for the type of information over which individuals should have control.

Informational privacy, it is argued, leaves privacy at the discretion of the individual. Arguably, if privacy has the significance of a right it is because it is a value that *society* should protect. Going beyond simply informational selective disclosure, Gavison’s ‘limited access’ is very closely linked to the idea of autonomy (Gavison, 1980). If privacy is intuitively seen as some kind of boundary that surrounds an individual and protects them from outside interference, then this automatically fosters the conditions conducive to the exercise of autonomy. In this sense, privacy is of teleological benefit, though still appears clearly individualistic. A lack of privacy also leads to the loss of aspects of individuality and dignity. Gavison emphasises the point by commenting that the individual need for privacy is sufficiently strong that even individuals in so-called ‘total institutions’ develop some way to achieve intimacy despite near constant surveillance. It is argued that privacy is necessary for mental well-being (Lustgarten and Leigh, 1994: 40). Certainly, the idea that autonomy and dignity underpin a western European concept of privacy is widely accepted (Whitman, 2004). In the House of Lords case, *Campbell v Mirror Group Newspapers* (2004), a case concerning informational privacy, Lord Hoffman commented that “what human rights law has done is to identify private information as something worth protecting as an aspect of human autonomy and dignity” (para. 50). The House also stated that “an individual’s privacy can be invaded in ways not involving the publication of information” (para. 15). Indeed, the scope of cases that the European Court

has found to fall within the definition of ‘private life’ is huge and varied (Moreham, 2008). The Court has stated that private life is a broad term not susceptible to definition. Without a definition, identification of the underlying value(s) becomes of genuine practical importance if both domestic law and practice is to attempt to give respect to the right.

The idea that privacy is based very centrally upon autonomy, and therefore its protection serves to ensure that people can make their own life choices, is not the whole picture however, as recognised above. Being individualistic means it is inevitably problematic to those who feel that its strength as a protected right is ‘anti-social’. This approach is in accordance with the idea that rights bring responsibilities (Etzioni, 1999). Raz (1986) has persuasively argued that individual freedom and self fulfilment requires the cooperation of others, therefore an entirely negative conception of privacy would be inappropriate. Feldman adds that “any attempt to identify a single interest at the core of privacy is doomed to failure, because privacy derives its weight and importance from its capacity to foster the conditions for a wide range of other aspects of human flourishing.” (Feldman, 1997: 21). A loss of privacy is recognised as undesirable and such losses should therefore be minimised, but if the law is to be the instrument to protect privacy, then we need to know when a privacy-related interest is so substantial as to demand not merely state neutrality but positive state action to defend it. So, it follows, we need to recognise when an interest is actually privacy related, and once it is recognised as such, it must be balanced against other competing claims.

Feldman (1994) contends that the current social meaning of privacy within the liberal tradition is perceived as an actor’s ability to determine their level of intimacy with others by demarcating their life into a series of interlaced social spheres. A sphere itself is formed by a gathering of individuals who have a requisite degree of intimacy with each other to realise a purpose. Every individual will be part of a multitude of different social spheres, such as their workplace, social gatherings, family unit and so forth. The level of intimacy will necessarily vary between each sphere. For example, an individual within the social sphere of his or her workplace will typically have fairly formal inter-relationships and little intimacy. The family sphere on the other hand would have a far greater level of intimacy and familiarity. Within each sphere there is communal privacy, claimed on the part of the whole group, and enforced against outsiders to that social strata. This is similar to what Nissenbaum (1998) would term ‘contextual integrity’. We would not be concerned with providing a doctor with intimate details about our health, but would be concerned if such information was disseminated more widely. What Feldman’s communal privacy protects is a notion of privacy divided into four dimensions, namely, space, time, action and information. Which of these dimensions is affected and the subsequent manner in which privacy is impinged upon depends on the individual’s social value that is encroached. These values are categorised as secrecy, dignity and autonomy. Secrecy, Feldman contends, is the maintenance of the confidentiality of personal information. The ability to control the flow of information about oneself within the social sphere can be seen as an important ‘privacy related’ interest. In the social circles in which one chooses to live we should be free to divulge only that information that is necessary to live in those circles. Being able to control the boundaries of the social spheres in which we participate is significant for fostering autonomy and dignity – the promotion of an agent’s ability for self determined action, guided by reasoned principles, and self respect and respect for the moral rights of others.

Given then that privacy may be viewed as a bundle of interests or values which relate to the different social spheres in which an individual participates it is possible that some aspects can be over-ridden whilst maintaining others. Equally, whilst the values are inherent within the individual, their extent depends partly upon the social sphere in which they are in; therefore they are affected by space but not determined by space. To this end it must follow that privacy related interests can operate when an individual is in the public domain. This latter point is especially important when considering the relationship between overt visual surveillance and privacy. This bundle of privacy related interests, secrecy (of personal information), autonomy and dignity sits neatly with that suggested by the House of Lords in *Campbell*, a case which

sought to give effect to the values of the ECHR. It is to the ECHR we must now turn. With the values of privacy in mind, what does the Convention demand?

The European Convention on Human Rights.

Article 8 of the European Convention on Human Rights provides:

8(1). Everyone has the right to respect for his private and family life, his home and his correspondence.

8(2). There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Described as “ill defined and amorphous” (Moreham, 2008: 45) Art.8 provides “one of the most dynamically interpreted provisions of the Convention” (Feldman, 2007: 265). Given that the European Court has intentionally sought not to define its parameters there is a degree of uncertainty as to its scope. However, there is a good deal of jurisprudence on which to draw to establish the applicability of Art.8 to overt and covert surveillance and therefore the overarching ethical standards that then follow.

In *PG and JH v. UK* (1998) the European suggested that in considering the extent of ‘private life’, “a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor” (para.57). In *Niemietz v Germany* (1992) the Court did not consider it possible to attempt an exhaustive definition of ‘private life’, though it is worth quoting at length their thoughts that: “it would be too restrictive to limit the notion to an ‘inner circle’ in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of ‘private life’ should be taken to exclude activities of a professional or business nature...” (para.29). It can reasonably be assumed that, for example, surveillance of an individual in their home will engage Art.8 as it is a place that is in fact an ‘inner circle’ and where there would be a reasonable expectation of privacy. This clearly accords with the inner core of Feldman’s social spheres analysis. When an individual leaves a traditionally ‘private zone’ however the problem is more nuanced. Clearly the European Court has recognised that private life includes the developing of relationships which must take place beyond the ‘inner circle’ (the outer spheres). In *P.G.* the Court expressly stated that there is “a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life” ... (para.56). This has been given more clarity in the context of surveillance in *Perry v UK* (2004). “The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life (at para.38; see also *Herbecq v. Belgium*, 1996). These interpretations are entirely consistent with the themes of autonomy and secrecy considered earlier. When in a traditionally private setting there is a clear expectation of privacy and therefore any form of surveillance will interfere with that expectation. When in a public setting the expectation of privacy would be consequently reduced, but it is not eradicated. In *P.G.* the Court explained:

There are a number of elements relevant to a consideration of whether a person’s private life is concerned by measures effected outside a person’s home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to

any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. (see, for example, *Rotaru v. Romania*, 1995).

Therefore, though the recording of *P.G.*'s voice was made while he answered questions in a public area of a police station, the use of the recording for further analysis was regarded as the processing of personal data amounting to an interference with his privacy. Further, in *Friedl v Austria* (1989) taking photographs of someone at a public demonstration did not of itself constitute an interference with Art.8 provided that the photographs were not entered into a data processing system and stored together with the name of the person.

This approach to Art.8 has been echoed in the UK courts. In the wider context of the civil law claim for 'misuse of personal information' developed in response to the demands of Art.8, domestic courts have stated that a key factor in determining whether, for example, the taking of photographs in public engages Art.8 is the individual's reasonable expectation of privacy (*Campbell v MGN* (2004)). The House of Lords stated that, "We have not so far held that the mere fact of covert photography is sufficient to make the information contained in the photograph confidential. The activity itself must be private" (para.154). However, to this one must note the European Court's discussion of a "systematic and permanent record". It is argued that covert photography of itself *may* not be sufficient to create a privacy claim but its *use* to create a record would. The nature of overt video surveillance may be for crime prevention or public safety purposes rather than for reasons of creating a permanent record, however, it is inevitable that recorded material will become a systematic record once an event occurs in which the data is analysed and processed according to the individual's personal details.

Therefore, though attention must be paid to the individual facts of each case, it is safe to assume that Art.8 will be engaged by covert video surveillance in most instances as the very nature of covert monitoring is that the individual cannot monitor his behaviour to maintain contextual integrity of the situation. Overt video surveillance is less straightforward, though the *use* made of any recording rather than the fact of the recording is where Art.8 would most obviously 'bite'.

Nonetheless, Art.8 is not an absolute right which acts as a trump to any competing claim but recognises that the right to private life must, on occasion, give way. Art.8(2) provides a framework for accountability and transparency where private life is the subject of state interference. It demands that any surveillance that interferes with private life must have a legal basis; must be in pursuit of a legitimate objective; must be necessary and proportionate. These require closer scrutiny in order to see what demands they place on domestic law.

The Legal Basis

ECHR jurisprudence has interpreted Art.8(2) to mean that, regardless of the end to be achieved, no right guaranteed by the Convention should be interfered with unless a citizen knows the basis for the interference through an ascertainable national law (*Malone v United Kingdom*, 1984); *Leander v Sweden*, 1987). This demand for transparency requires that the law should be sufficiently clear and accessible to ensure that people can adequately determine with some degree of certainty when and how their rights might be affected. In *Kruslin v France*, (1990) a case concerning covert surveillance techniques, the European Court commented, "it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" and further added a demand for accountability in stating that "there must be a measure of legal protection in domestic law against arbitrary interferences... especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident" (para.30). In the context of surveillance being used for crime prevention and detection it is

apparent that the European Court is demanding increasingly rigorous legal provisions (*Valenzuela v Spain* (1998)). In short, where an individual's private life is engaged, domestic law must be transparent and provide mechanisms of accountability.

The Legitimate Objectives

Interference with Art.8(1) must be directed towards a legitimate aim, and these are found in Art.8(2). The restrictions on the primary right are numerous and widely drawn and it could be argued that it is not overly burdensome to require state conduct to remain within such boundaries. The restrictions are for the purposes of national security; public safety; the economic well being of the country; the prevention of disorder or crime; for the protection of health or morals; and the protection of the rights and freedoms of others. However, the list is intended to be exhaustive and there should be no capacity for the State to add to those grounds. In the context of overt or covert surveillance operations, the vast majority will fall clearly within the scope of being for "the prevention of disorder or crime" or "public safety".

The Requirement of Necessity.

The words of Art.8 require that the restriction must also be 'necessary in a democratic society'. 'Necessity' has been interpreted by the European Court as not synonymous with 'indispensable' but not as flexible as 'ordinary, useful, reasonable' or 'desirable' (*Silver v UK*, 1983: para.97). The interference with the primary right should be in response to 'a pressing social need'. Intrinsic within this idea is the notion of proportionality. It is this aspect of Art.8 to which particular emphasis should be drawn. It demands that in each and every case when surveillance by the state will impinge upon Art.8, attention is given to the proportionality of that response. It brings about a need to be accountable for the way in which the surveillance operation was designed and carried out in practice. Therefore, in identifying the demands that the overarching framework places on domestic law it is essential to develop an understanding of what proportionality demands.

The Principle of Proportionality

In many ways this concept is the key to the exercise of surveillance that is ethical, in the sense that it respects the right to private life. It is the concept that provides some guidance as to how surveillance should be carried out in a practical situation, thereby maintaining the contextual integrity of privacy. In *Brown v Stott* (2001) Lord Steyn recognised that "... a single-minded concentration on the pursuit of fundamental rights of individuals to the exclusion of the interests of the wider public might be subversive of the ideal of tolerant European liberal democracies. The fundamental rights of individuals are of supreme importance but those rights are not unlimited: we live in communities of individuals who also have rights". Privacy cannot be a cloak for illegal conduct but further, it must give way to the rights of others in certain contexts.

Proportionality was succinctly defined by Lord Bingham in *R. v. Shayler* (2002) wherein he stated that the test was whether, in all the circumstances, the interference with the right was greater than was required to meet the legitimate object which the state sought to achieve (para.26; see also *Jersild v Denmark*, 1995). The jurisprudence of the European Court has identified various factors to be taken into account when considering the issue of whether the interference is proportionate to the aim, and these centre upon accountability and transparency. For example, a need to have relevant and sufficient reasons based on reliable information provided in support of the particular measure has been emphasised. The reasons provided for the particular surveillance operation should not be arbitrary but should be based on relevant considerations (*W v UK*, 1988). Crucially, consideration should also be given to whether there is a less restrictive alternative (*Campbell v UK*, 1993). There also must be sufficient safeguards against abuse. In *Klass v Germany*, 1980) the European Court stated that, "One of the fundamental principles of a democratic society is the rule of law... (which) implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control... . (para.55).

In summary, what is required is a consideration of whether the interference with the right is greater than is necessary to achieve the aim. This is not an exercise in balancing the right against the interference, but instead balances the nature and extent of the interference against the reasons for interfering: crucially, it is not the *right* itself that is the subject of a balancing exercise.

Therefore, it can be seen that the width of Art.8 is considerable. Its scope, whilst undefined, sits comfortably with the idea of Feldman's social spheres in which privacy related interests are protected to differing degrees. It ensures that visual surveillance operations may, depending upon each particular set of circumstances, interfere with private life and therefore domestic law and practice must operate within the overarching conceptual framework it provides.

The Substantive Context: Domestic Law

Prior to the Human Rights Act 1998 the UK's response to the regulation of surveillance was in many instances nonexistent (Walker, 1980). However, whilst surveillance had been 'acceptable' on a domestic level where its use was otherwise not unlawful (for example, by amounting to a trespass) the passage of the Human Rights Act 1998 brought the principles of the ECHR to the fore in domestic law. As such, where surveillance might breach individual private life, legal regulation was necessary. The first comprehensive attempt at the regulation of covert surveillance was the Regulation of Investigatory Powers Act 2000 (RIPA). During the passage of the Act through Parliament, the Home Secretary assured the public that it would ensure that covert techniques "will be properly regulated by law and externally supervised, not least to ensure that law enforcement operations are consistent with the duties imposed on public authorities by the European Convention on Human Rights" (H.C. Debs, vol. 345, col. 677). No similar tailored legal regime was developed for overt surveillance, though the regime designed to protect the processing of personal data, enhanced during the same period, did provide a measure of regulation.

Covert Visual Surveillance

RIPA draws a distinction between 'directed' and 'intrusive' surveillance, with consequently different levels of authorisation and accountability (Akdeniz, 2002). Intrusive surveillance is essentially covert surveillance carried out on residential premises or a private vehicle. It clearly will always have implications for privacy and consequently has a relatively robust process of authorisation. Directed surveillance is covert surveillance outside of such areas, as part of a planned operation, which is likely to impact upon privacy. It consequently has a less rigorous authorisation procedure. The Act recognises that privacy can extend beyond the traditional spatial interpretations of public and private, but arguably the categories of surveillance still appear to protect places rather than people, with 'intrusion' only occurring if the target is situated in his or her property or vehicle. This fails to recognise that surveillance that is intrusive might occur outside of these places through, for example, prolonged surveillance, or in a place in which the target would legitimately expect to enjoy 'inner core' privacy.

Given that the home is given specific protection through RIPA, this paper will concentrate upon the use of visual surveillance in traditionally more public arenas: what the legislation defines as 'directed surveillance'.

RIPA states that surveillance is directed if it is covert but not intrusive and is undertaken (a) for the purposes of a specific operation; (b) in such a manner as is likely to result in the obtaining of private information about a person; and (c) is otherwise than by way of an immediate response to events such that it would not be reasonably practicable for an authorisation to be sought.

The reference to 'private information' should be interpreted to be compatible with Art.8. If private life is affected then one would anticipate that the ECHR requirements of necessity and proportionality would then follow. However, the legal regime applies only to 'covert' surveillance, and this is not interpreted

broadly. Covert surveillance is defined as that carried out in a ‘manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place’. This would not encompass public space visual surveillance typically used. For example, video surveillance cameras used on public streets and clearly signed. However, the definition does leave a question about whether overt video cameras used in a manner that is not anticipated effectively become covert.

An example of this problem is provided in *Rosenberg* (2006). The defendant and her neighbour had had a long-running dispute, and the neighbour set up video-recording equipment in order to record the activities of the defendant in and around her premises. The defendant was fully aware of this but treated it simply as part of their ongoing antagonism toward each other. The neighbour submitted video footage to the police which showed the defendant apparently unwrapping packages of drugs. Officers subsequently found drugs at the address, and the defendant was tried. The prosecution sought to use the neighbour’s visual recordings in evidence. The defendant claimed that the evidence should be excluded from court as being obtained in breach of the legal regime in RIPA (and, as such, had not been subjected to the requirements of necessity and proportionality). She argued that the police had encouraged the neighbour’s surveillance of and into her home, and that the court should regard that conduct as amounting to surveillance by the police for which no authorisation had been given (under RIPA). However, only if the surveillance was covert would the authorisation process ‘bite’. Given that the defendant was aware of the existence of the ongoing video observation by her neighbour it seems difficult to argue that the surveillance could be considered ‘covert’. The court was of the same opinion and determined that RIPA had no application to these circumstances. Nonetheless, interpreting the need to respect private life broadly, as one should when dealing with minimum standards of rights, it is argued that ‘covert’ has a broader meaning than simply that a person is unaware of *any* surveillance. Whilst the defendant saw the neighbour’s video camera trained on her property, she viewed it in the context of their continuing poor relationship, but arguably, were the police to assume responsibility for the use of the camera this would change its nature considerably. Such action would amount to a planned covert operation. Though the surveillance device itself might be visible, the manner of the operation could be considered to be ‘calculated to ensure’ the subject was unaware that it was taking place. Therefore, merely because a surveillance device is overt, that may not of itself take a subsequent surveillance operation outside of the boundaries of the RIPA regime. Such an interpretation is not to use the scope of privacy to mask criminal conduct but simply to ensure that when the state is involved in visual surveillance affecting privacy rights it ought to be accountable for doing so, such that any operation can be seen to be proportionate in the circumstances.

The same argument would apply if, for example, overt video surveillance cameras operated by the local authority for the purposes of public safety were appropriated by the police with a view to tracking the movements of a particular individual. If a systematic record of such an individual’s movements, contacts and suchlike were made then this would amount to an interference with private life, yet the definition of ‘covert’ as currently applied would mean that such an operation would not be subject to a pre-authorisation regime and therefore no prior consideration of the necessity or proportionality of the operation would take place. Any regulation of overt surveillance would apply but this is considerably less robust. In terms of protecting privacy through mechanisms of accountability and transparency, it is argued that the scope of the regulation covering covert video surveillance is too narrow.

For pre-planned operations which do fall within the definition of ‘covert surveillance’, RIPA provides a regulatory system that seeks compatibility with the demands of Art.8 and the conceptual framework highlighted above. Firstly, RIPA provides the requisite legal regime. A directed surveillance operation requires prior authorisation though it is somewhat disappointing that this amounts only to internal albeit higher level authorisation. For criminal investigations it is argued that an element of judicial supervision should have been provided, as recommended by the Royal Commission on Criminal Procedure in 1981 (para.3.57). The judiciary have the necessary expertise to scrutinise the suspicion which supports a case for surveillance and they provide an element of objectivity and independence. Further the range of state

bodies able to carry out directed surveillance is huge, and consistency and objectivity in authorisation should be paramount. Secondly, a system of accountability is provided by way of oversight by a Surveillance Commissioner and a complaints tribunal. However, the major flaw in this system of accountability is that the target of any surveillance operation need not be informed that it has taken place and therefore will be in no position to ensure that the reasons for the operation could be justified.

Overt Visual Surveillance

The use of overt video surveillance is considerable and its growth was attributed in part to the fact that it was largely unfettered by legal regulation. Since 1998 however, the Data Protection Act has incrementally developed a regulatory framework that now applies to most public space visual surveillance systems which record 'personal data'. Such data is that which relates to a living individual who can be identified from those data, or from the data and other information which is in the possession or likely to come into possession of the data controller. This can be seen to equate to the 'systematic and permanent' record described above. The legislation requires that data controllers (those who control the video surveillance system) register with the Information Commissioner. This process ensures that a publicly accessible database is kept on who is collecting personal data and their reasons for so doing, though it does not equate to compliance with other aspects of the Act. The backbone of the Act is the list of eight data protection principles. In essence they seek to bring about a framework of accountability, transparency and proportionality for the legitimate infringement of privacy that seeks compatibility with the demands of Art.8. In response to a Parliamentary question in 1999 about the potential effect of the Human Rights Act and the use of CCTV, Mr. George Haworth M.P. commented that, "CCTV schemes funded by the Home Office are governed by codes of practice and data protection legislation to ensure that the systems are operated fairly and lawfully, and with due regard to individual rights to privacy..." (House of Commons, Written Answers, (1999) July 2).

The first principle requires that data be processed fairly and lawfully, and shall not be considered to be so unless it is processed for a 'legitimate reason'. As far as the general monitoring of public spaces is concerned, justification may be found in Schedule 2, which states that the 'processing is necessary for the exercise of any ... functions of a public nature exercised in the public interest ...'. Though broad in its terms, this ought to be interpreted to be compatible with Art.8(2).

In order to process images fairly the data controller should also provide individuals with information at the point of obtaining the image as to the identity of the data controller and the purpose for which the data is processed. In practical terms this is a demand for adequate signage which would not only inform the data subject that he is in an area in which surveillance cameras might be operational, but also will provide the contact details of the operator and the reason behind the surveillance. This demand for a degree of accountability and transparency provides the subject of the surveillance with knowledge of the context within which he or she is operating whereupon the integrity of that social sphere can be gauged effectively.

The Act requires that data should be obtained only for specified and lawful purposes, and should not be processed in any manner incompatible with that purpose. This reflects the need for a legitimate reason for the interference with private life. Further, data should be adequate, relevant and not excessive. This has implications for issues such as the positioning of cameras and whether the surveillance needs to be constant. That the surveillance be proportionate is also evident in the following two requirements: that personal data should be accurate and, where necessary, kept up to date; and that personal data should not be kept longer than is necessary for that purpose. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Again, the intent to protect the privacy and integrity of the data is clear. Accountability and transparency is further enhanced by 'subject access' rights. An individual has the right to see surveillance images relating to them and to obtain a copy of them. Furthermore,

surveillance operators should not disclose images of identifiable people to the media for entertainment, which sits comfortably with the reasonable expectation of privacy the target has in regard to the use of the images (*Peck v UK*, 2003).

In addition to the DPA, the Private Security Industry Act 2001 provides a criminal offence for staff to be contracted as video surveillance operatives without a licence, and a further requirement is that front line staff must have a degree of training to attain certain minimum standards.

Whilst legislation regulating the use of both covert and overt video regulation seeks to give substance to the conceptual principles outlined earlier it is well recognised that the law in books and the law in action are not the same thing. Therefore, it is necessary to consider some of the issues of operational practice.

Operational Issues: Surveillance in practice

Covert Surveillance

RIPA has been described by the judiciary as “a particularly puzzling statute” (*R v W*, 2003: para.98) that is “not easy to understand” (*AG Reference (No.5 2002)*, 2004: para.29). Its complexities have not made the task of transferring concepts into practice particularly straightforward. A further drawback in the legislation is that without the requirement to notify a person that they have been the subject of surveillance, the ability to see the state held accountable for its use is severely restricted. There have been few cases before the courts that have tested the boundaries of the legislation. The main source of accountability therefore comes by way of the Surveillance Commissioner and the Annual Reports he prepares for Parliament on, inter alia, the powers and duties conferred by RIPA.

From March 2008 to April 2009 a total of 16,118 directed surveillance authorisations were granted to the law enforcement agencies. A further 9,894 were granted to public authorities (Office of the Surveillance Commissioner: 2009: 4.7). In general terms, the Commissioner found the use made of the legislation to be “proper and of good standard”. However, a number of errors were detected in relation to all types of public authority use. For example, there was a continuing failure to demonstrate that less intrusive methods had been considered and discounted before the particular surveillance method had been adopted. This is a key failure of proportionality. Further, there was a continued misunderstanding of private life to refer only to biographical data and not the wider definition adopted by the European Court and explored earlier in this piece. The Commissioner confirmed that overt or covert video surveillance should not be determined by the positioning of the camera but by the use to which it is put. This flexible interpretation is clearly failing to reach the users. Authorising officers have displayed a lack of knowledge about the capabilities of the equipment being authorised. Again, this demonstrates a lack of proportionality as such a lack of knowledge cannot ensure the least intrusive means possible have been adopted. Poor internal auditing procedures were also highlighted, detracting from the necessary degree of accountability required by the Act. Relatively rare but recurrent themes in previous years include: poor training. (“Inadequately trained and ignorant staff often rely on templates to compile applications or authorisations. This leads to a lack of proper consideration, and nearly always produces an unsatisfactory result.” Office of the Surveillance Commissioner, 2006 para.8.3); failure to adequately record and retain authorisations; ineffective oversight (“Senior executives must ensure that ...the Authorising Officer is senior enough to challenge as well as listen to operational practitioners.” Office of the Surveillance Commissioner, 2007 para.10.8); a lack of centralised records (“A poor central record is usually an indicator of ineffective oversight...” (para.10.7)); lack of knowledge of the demands of the legislation; inadequate applications; errors of detail; failure to utilise technical feasibility reports leading to inappropriate use of equipment and the authorisation of more than was sought (without good reason). In addition to these problems, the police in particular have taken a risk-averse approach to using their powers in a bid not to fall foul of the regulations. However, this in itself displays a lack of attention to relevant factors. To seek authorisation for a surveillance operation where it is not required illustrates a failure or reluctance to grapple with the

question of proportionality. It further results in a widely held perception that the authorisation process is overly bureaucratic though a clear audit trail represents a key feature of the demands of accountability and transparency. In his 2008 Review of Policing Sir Ronnie Flanagan noted that “in some instances excessive bureaucracy is created by a combination of misunderstanding and sometimes over-interpretation of the relevant rules” (Flanagan Report, 2008: para.5.55).

The apparent disproportionate use of covert surveillance by local authorities in particular has also caused a degree of public dissatisfaction. Particularly widely reported was the decision by a local council to mount a covert surveillance operation on a family who had been wrongly accused of breaking rules on school catchment areas. Recognising the damage that such unnecessary and disproportionate incidents can cause to public confidence in surveillance more generally, a Minister of State in the Home Office in 2009 announced a consultation process which would lead to the development of legislation and accompanying codes which would limit the number of public bodies who could carry out covert surveillance and more clearly articulate what the principles of necessity and proportionality demanded.

Overt Surveillance

Though the DPA regime represents an attempt to protect private life in the face of overt video surveillance, as with covert surveillance, there are some serious flaws. The first concerns registration. In order to demonstrate that the necessity and proportionality of a system that might breach private life have been considered, some form of licensing ought to take place. Post establishment registration cannot ensure that these essential pre-requisites for surveillance, a fundamental feature of the conceptual framework, have taken place.

Further, it has been argued that the Information Commissioner’s Office lacks teeth (Davies, 1996). Perhaps this lies in the fact that it is a regulatory body. Academic literature emphasises that whilst regulatory bodies can take many different forms, their specific form depends upon their internal and external pressures, their aims and objectives, and the context within which they must carry out their task. The link between the ability of state bodies to enforce the law and the amount of information that is forthcoming from the public has been stressed. The difficulty with the DPA is the apparent lack of public knowledge of the boundaries of (or even the existence of) the DPA in relation to data protection issues generally. The lack of an obvious link between data collection and the recording of images via surveillance cameras reduces the knowledge of the boundaries of the DPA in this context still further. Allied to a lack of knowledge as to when surveillance might be taking place, and the extent of ‘public privacy’ combine to reduce the knowledge that rights might be being infringed and therefore what standards need to be imposed to ensure the use of surveillance is legitimate.

Cotterill continues this theme in his discussion of various factors that might inhibit the effective voicing of grievances (Cotterill: 1992). To set the law in motion it is recognised that invariably an individual will have to draw the authorities’ attention to a particular breach of the law. This obviously becomes more difficult where the nature of the legal regulation is complex. This can certainly be said of the DPA, which has been described as “inelegant and cumbersome” (PDP editorial: 2004). In effect, the combination of the surveillance users’ lack of knowledge of the conceptual underpinning to the legislation, and the public’s lack of knowledge or understanding of the legislation itself combines to condone a surveillance network that fails to give effect to the overarching conceptual framework.

The National CCTV Strategy consultation document (Home Office, 2007) recognised that the growth and diversity of public space video surveillance systems had resulted in a number of problems affecting future development. These problems highlight clear difficulties in relation to accountability, transparency and the protection of privacy such that existing legislation was clearly inadequate. For example, the lack of compatibility between the technologies employed meant that the process of retrieving surveillance data affected the quality and integrity of the images (para.2.2.2). Though Home Office guidance was available

on minimum performance requirements, many users found this difficult to understand. The consultation found that many new surveillance systems had failed to give consideration as to how the surveillance would be used from “camera to archive” (para.2.2.7). Such a lack of attention must inevitably illustrate a lack of proportionality. Recommendations in the document for the setting of standards across operators suggest a clear gap between the substantive law and the operational practice. Similarly, a recommendation that “owners of systems should undertake a review of all the CCTV cameras in public space use, detailing their purpose and establishing if they are fit for that purpose” (p.16) is a welcome move but a clear recognition that the technology has been developed and utilised with little regard to conceptual or substantive standards to date. The Information Commissioner’s lack of resources and powers to enforce standards and his restrictions on dealing with the ‘processing’ of data rather than on the use of video surveillance itself were also highlighted (para.3.3). The recommendation that “there needs to be greater understanding by all about the issues around public protection in the context of the DPA and the Human Rights Act” is a clear indication that the conceptual principles have not filtered down, through education, into working operational standards.

The SIA licensing regime has brought about a degree of minimum standards across surveillance operatives, but gaps in the training requirements (for example, they don’t apply to the police) mean that not all involved in the ‘processing’ of the data are familiar with the conceptual or substantive standards. Whilst the DPA requires that data is kept for no longer than necessary, and attention to this issue serves to demonstrate the exercise of proportionality, the consultation document noted that retention periods had reduced following the introduction of digital systems (para.6.1). However, the clear indication was that the technology was driving the retention question rather than the demands of the particular surveillance operation – a clear lack of proportionality.

Ultimately, without a licensing scheme which demands attention to the conceptual and substantive standards, the operation of overt video surveillance systems will continue to lack respect for the fundamental right to private life in that interferences with the right fail to be legitimised by a proportionate response which reflects the values of accountability and transparency.

Future Developments

There are current developments in both areas of covert and overt surveillance directed towards the development of more open and accountable frameworks. In 2009 the Home Office announced a consultation process on the codes of practice accompanying RIPA for the regime for covert surveillance on the ground that there was public unease at the inappropriate use by public authorities of directed surveillance. The thrust of the questions the Home Office sought answers to were whether the range of bodies that could use covert surveillance was too broad and whether the authorisation process needed to be at a more senior level. However, rather more disconcerting was the query about how bureaucracy could be reduced “for the police so they can use RIPA more easily to protect the public against criminals” (p.4). In the words of the Surveillance Commissioner: “It should not be acceptable that the use of covert powers is made “easy” for any public authority. The fundamental purpose of the legislation is to ensure that covert surveillance is necessary, proportionate and carried out in a way which is compliant with human rights...” (para.5.32). The Home Office did question whether the codes offered sufficient guidance on the demands of necessity and proportionality. In 2008 the Surveillance Commissioner produced a procedures and guidance document to promote consistency in the authorisation and use of covert surveillance and to help raise the standards of compliance (para.3.13), and it is perhaps in the area of consistency that guidance is appropriate. However it should be recognized that by its very nature proportionality is case specific. General guidance can be problematic when what is required is a close attention to the individual scenario faced by the authorizing officer. Whilst the code of practice can provide some limited guidance, and the dissemination of good practice throughout criminal justice agencies and public authorities can be helpful, it is of considerable importance that standardised formats are avoided.

There have also been developments in overt surveillance. In December 2009 the Home Office announced the appointment of an interim CCTV regulator to “advise the government on matters surrounding the use of CCTV in public places, including the need for a regulatory framework overseen by a permanent CCTV regulator, which enables the police, local authorities and other agencies to help deliver safer neighbourhoods while ensuring that personal privacy considerations are appropriately taken into account” (David Hanson, House of Commons Written Answers, 15 December, 2009). The regulator will still have no responsibility for the appropriate positioning of cameras or how they are used. However, the development of the National CCTV Strategy Board is designed to develop national standards for installation and use of video surveillance; determine training requirements; engage with the public to determine regulatory standards and promote public awareness of the mechanisms for accountability. Laudable standards no doubt, but these will be unlikely to affect the current disproportionate use of overt surveillance unless a broad and expansive audit of existing schemes is to take place.

Conclusion

Developments in both fields that are designed to bring about greater protection for privacy through enhanced accountability, transparency and proportionality must be welcomed. In 2007 the European Commission for Democracy Through Law (Venice Commission, 2007) “recommended that specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy” (para.81). The independent human rights organisations JUSTICE and Liberty have both expressed concern about the lack of effective regulation (Select Committee, 2009); the former arguing that “it is a mistake to suppose that existing privacy safeguards – such as the DPA or RIPA – are capable of providing effective protection” (para.215).

One clear problem is that the law or extra-legal policies are inevitably seeking to catch up years of surveillance operation and practice. In such circumstances policies developed to protect privacy are viewed suspiciously; that in some way any call for privacy is merely to act as a cloak for illegal or anti social behaviour, or is in some way designed to blunt to drive for crime prevention or detection. However, it is important to make the point that the use of surveillance tactics and privacy rights do not and should not represent a conflict. Crucially, ‘policing’, in a broad sense, that maintains moral authority and community support is that which is carried out according to transparent ethical standards. It is essential that those employing surveillance are able to demonstrate that they work within an ethical framework and this can be found within the ECHR which seeks to guarantee a set of *minimum* standards below which public bodies should not fall. The ECHR and the flexibility of the overarching concepts in Article 8 can and do provide the valuable conceptual framework that can both shape domestic law and, equally importantly, can provide both a barometer against which domestic law can be measured. It can also act as a valuable interpretative tool. RIPA, with its concentration on covert surveillance, does represent an effort to get to grips with the demands of Article 8 but the safety first approach currently adopted arguably fails to give significant or indeed sufficient attention to the key concept of proportionality. In terms of overt surveillance the lack of any dedicated law represents a significant gap in the legal framework for surveillance generally. Reliance on the data protection legislation is ill-directed and its lack of an obvious connection to the use of public space video surveillance is arguably partly responsible for its relative lack of influence on users/practitioners. It is clear that reform of both covert and overt surveillance regulation is required.

The Government, certainly in the short term, is placing its trust in Codes of Practice – enforceable in the case of covert surveillance, voluntary in the case of overt video surveillance. Both have a role to play in shaping behaviour but whatever policies or laws are developed, the key for those using surveillance techniques is to understand the conceptual framework because it is the demands of those overarching

principles that the substantive policies and operational practices are seeking to satisfy. There is enough evidence to suggest that merely reproducing ‘core principles’ in codes of practice itself does not affect behaviour (Norris, 1999; Goold 2004; Taylor, 2005) but genuine knowledge of the principles has a better chance of affecting working practices. The conceptual standards will not change despite laws and policies regularly changing, and a greater knowledge of those standards can and should influence outcomes both nationally and internationally (Gras, 2004).

Postscript

In May 2010 the new coalition Government announced that it intended to bring forward a Freedom (Great Repeal) Bill which would cover a range of areas, including the regulation of CCTV with the aim of protecting individual privacy. A very welcome move without doubt and in March 2011 the Home Office produced a consultation paper on a code of practice to regulate CCTV (Home Office, 2011). The stated aims of any new legislation directed at CCTV are to ensure “that there is proper transparency and proper proportionality in their use” (p.3). These are key aspects of the conceptual framework discussed above and, more importantly, the consultation paper also speaks of potentially introducing operational standards in the use of overt video surveillance and highlighting core training issues. These are essential. The conceptual standards have to be translated into substantive policies and operational practice if they are to have meaningful value.

Initially, whilst the code of practice will be applicable to all overt surveillance schemes (above small, private schemes, e.g. on a private residence) only local authorities and police forces will have a statutory duty to have regard to it. Whilst an incremental approach which gradually encompasses more CCTV users has the advantage of providing a firm foundation for a consistent and workable regime, arguably it is local authorities and the police who largely adhere to the current DPA code (Taylor, 2005). The problem in lack of accountability lies rather more clearly *outside* the public sector, though from earlier in this paper it can be seen that the public sector’s safety first approach brings problems of its own in an operational sense. The consultation paper does envisage that if insufficient progress is being made towards the aims of the code then further regulation will be sought, or aspects of the code will be made mandatory. One might question why aspects of the code will not be mandatory from the outset rather than that users should ‘have regard’ to it. In this sense it might fall foul of the same problems as the current DPA code in that a lack of teeth results in widespread ignorance or apathy about the relevant standards.

The extent to which the regime will affect existing users is also open to debate. There is a useful ‘proportionality checklist’ envisaged for “anyone considering the use of such technology” (p.13), though it has to be explicit that because proportionality is case specific a ‘proforma’ checklist is only a guide. Whilst this practical application of proportionality is a useful way of giving substance to a seemingly complex concept, if such questions are not also required to be asked of existing users then it might be a case of closing the stable door after the horse has bolted.

A Surveillance Commissioner is envisaged whose role will be not one of enforcement but to promote the code. This has echoes of the role of the Information Commissioner and though the latter has had a limited impact in the field of video surveillance it is to be hoped that a commissioner with a more dedicated brief can have a wider impact. Nonetheless, the clear drive to “minimise new regulatory burdens” (p.3) must be interpreted appropriately. The need to regulate video surveillance is premised on the need to protect personal privacy, a fundamental right, and a certain degree of bureaucracy will be essential to achieve that aim.

In sum, that dedicated regulation is forthcoming is welcome though long overdue and the impact of regulation in giving effective meaning to the conceptual standards to the hundreds of thousands of existing schemes in addition to new users will be the real key to success.

Bibliography

- Akdeniz, Y., Taylor, N., and Walker, C. 2001. 'The Regulation of Investigatory Powers Act 2000: Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights' *Criminal Law Review* 73.
- Cotterill, R. 1992. *The Sociology of Law*, 2nd. Ed. London: Butterworths.
- Davies, S. 1996. *Big Brother: Britain's Web of Surveillance and the New Technological Order*. London: Pan.
- Dixon, D. Bottomley, A.K., Coleman, C.A., Gill, M. and Wall, D. 1989. 'Reality and Rules in the Construction and Regulation of Police Suspicion', *Int. Jo. Sociology of Law* 17: 185
- Etzioni, A. 1999. *The Limits of Privacy*. New York: Basic Books.
- Feldman, D. 1994. 'Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty', *Current Legal Problems* 47(2): 41
- Feldman, D. 1999. 'The Human Rights Act 1998 and Constitutional Principles', *Legal Studies* 2: 165
- Feldman, D. 1997. 'Privacy-related Rights and their Social Value', in Birks, P. (ed.) *Privacy and Loyalty* Oxford: Oxford University Press.
- Feldman, D. 1997. 'The Developing Scope of Art.8 of the European Convention on Human Rights', *EHRLR* 3: 265.
- Flanagan Report. 2008. *The Review of Policing*.
- Gavison, R. 1980. 'Privacy and the Limits of the Law', *Yale Law Journal*, 89(3): 421
- Goold, B.J. 2004. *CCTV and Policing: Public Area Surveillance and Police Practices in Britain* Oxford University Press.
- Gras, M. 2004. 'The Legal Regulation of CCTV in Europe', *Surveillance and Society* 2(3): 216
- Home Office, UK. 2007. National CCTV Strategy.
- Home Office, UK. 2009. Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice: A Discussion Paper.
- Home Office, UK. 2011. Consultation on a Code of Practice Relating to Surveillance Cameras.
- Jourard, S.M. 1996. Some Psychological Aspects of Privacy, *Law and Contemporary Problems*, 31: 307.
- Lustgarten, L. and Leigh, I., 1994. *In From the Cold: National Security and Parliamentary Democracy*. Clarendon Press, Oxford.
- Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- McKay, S. 2006. 'Approaching the Regulation of Investigatory Powers Act 2000', *Covert Policing Review* 1: 46.
- Moreham, N. 2008. 'The Right to Respect for Private Life in the European Convention on Human Rights: a re-examination', *European Human Rights Law Review*, 44.
- Nissenbaum, H. 1998. 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', *Law and Philosophy* 17: 559
- Norris, C., and Armstrong, G. 1999. *The Maximum Surveillance Society: The Rise of CCTV* Berg: Oxford.
- Office of the Surveillance Commissioner, UK. 2006. Annual Report 2005-6
- PDP Editorial 2004. 'Bad Data Protection Publicity – Commissioner fights back', *Privacy and Data Protection* 4.4(1)
- Raz, J. 1986. *The Morality of Freedom* Oxford: Clarendon.
- Royal Commission on Criminal Procedure, UK. 1981. Cmnd. 8092, 1981
- House of Lords Select Committee on the Constitution, UK. 2009. Surveillance: Citizens and the State, 2nd Report of 2008-9, HL 18-1
- Slobogin, C. 2002. 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity', *Mississippi Law Journal* 72(1): 214
- Solove, D.J. 2002. 'Conceptualising Privacy', *California Law Review* 90: 1088
- Taylor, N. 2002. 'State Surveillance and the Right to Privacy', 1(1) *Surveillance and Society* 1(1)
- Taylor, N. 2002. 'You've Been Framed: The Legal Regulation of CCTV', *Journal of Civil Liberties* 7(2): 83
- Taylor, N. 2003. 'Policing, Privacy and Proportionality', *European Human Rights Law Review Special Issue* 86
- Taylor, N. 2005. 'The Legal Regulation of CCTV', Unpublished M.Phil., University of Hull.
- Taylor, N. and Walker, C. 1996. 'Bugs in the System', *Journal of Civil Liberties* 1
- Venice Commission 2007. European Commission for Democracy Through Law: *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights*, Study No. 404/2006
- Von Hirsch, A. 2000. 'The Ethics of Public Television Surveillance', in Von Hirsch, A. Garland, D. and Wakefield, K., (eds.) *Ethical and Social Perspectives on Situational Crime Prevention*. Oxford: Hart.
- Wacks, R. 1980. *The Protection of Privacy*. London: Sweet and Maxwell.
- Wacks, R. 1980. 'The Poverty of Privacy', *Law Quarterly Review* 96: 73
- Walker, C. 1980. 'Police Surveillance by Technical Devices', *Public Law* 184
- Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum.
- Whitman, J.Q. 2004. 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *Yale L.J* 113:1151
- Younger Committee, 1972. *Report of the Committee on Privacy*, Cmnd 5012

Table of Cases

- AG Reference (No.5 2002)* (2004) UKHL 40
- Brown v. Stott* (2001) 2 WLR 817
- Campbell v. MGN* (2004) 2 AC 457
- Campbell v. United Kingdom* (1993) 15 EHRR 137

Friedl v. Austria App. No. 15225/89
Herbecq v. Belgium App. No. 32200/96
Jersild v. Denmark (1995) 19 EHRR 1
Klass v. Germany ((1979-80) 2 EHRR 214
Kruslin v. France (1990) 12 EHRR 547
Leander v. Sweden (1987) 9 EHRR 433
Malone v. United Kingdom (1984) 7 EHRR 14
Malone v. Metropolitan Police Commissioner (no.2) (1979) 2 WLR 700
Niemietz v. Germany (1992) 16 EHRR 97
PG and JH v. UK (2002) European Court App. No. 44787/98
Peck v. United Kingdom (2003) 36 EHRR 719
Perry v. United Kingdom (2004) 39 EHRR 3
R v. Duarte (1990) 65 DLR (4th) 240
R v. Rosenberg ((2006) EWCA Crim 6
R. v. Shayler (2002) 2 WLR 754
R v. W (2003) EWCA Crim 1632
Rotaru v. Romania App. No. no. 28341/95
Silver v. United Kingdom (1983) 5 EHRR 347
Valenzuela v. Spain (1998) 28 EHRR 483
W v. United Kingdom (1988) 10 EHRR 29