



# State Surveillance and the Right to Privacy

Nick Taylor<sup>1</sup>

---

## Abstract

The influence of Article 8 of the European Convention on Human Rights on domestic law has ensured that the state's use of technical covert surveillance equipment has become legally regulated over the past twenty years, albeit in a somewhat piecemeal fashion. The passage of the Human Rights Act 1998 will see the development of the 'right to respect for private life' in UK law. This paper seeks to reflect upon the impact that the European Convention has had on the regulation of covert surveillance, and whether there is a theoretical justification for developing the 'right to respect for private life' beyond traditional private spheres and into the public arena. It is argued that overt surveillance in the form of closed circuit television cameras (CCTV) should thus be legally regulated according to the principles established by the European Convention, and that such an extension of the 'right to respect for private life' need not be detrimental to the common good.

---

## Introduction

Throughout the history of policing in Britain, the response to social disorder and rising crime rates has been to adopt the most modern equipment and techniques available. Over the past thirty years in particular, considerable advances in technology have dramatically increased the powers of the state to carry out surveillance upon its citizens. This inevitably brings with it the dystopic vision of an Orwellian society, where citizens are constantly under the vigilant gaze and attentive ear of 'Big Brother'.

Though the allusion to 'Big Brother' is a popular modern metaphor for the role of the State in social control, it ignores the numerous benefits increased surveillance has brought about. Surveillance does, undoubtedly, have two faces. It can act to curtail rights through, for example, reinforcing divisions within society, or it can be a vital tool in preventing and detecting crime. For citizens to accept and consent to certain forms of surveillance, that is to say its positive face, the state should be accountable for its actions. It cannot be left with an unfettered discretion to determine why and where it carries out surveillance on, and on behalf of, its citizens, without some form of legal responsibility. The governors and the governed should be subject to the law.

---

<sup>1</sup> Centre for Criminal Justice Studies, Department of Law, University of Leeds, Leeds LS2 9JT, UK.  
Tel: 0113 233 5033 (ext. 35027), Email: [N.W.Taylor@Leeds.ac.uk](mailto:N.W.Taylor@Leeds.ac.uk)

In the UK the massive growth in state surveillance directed towards crime prevention and detection has been largely unencumbered by the law, legislation often developing later to legitimise practices found to be in breach of human rights standards by the European Court of Human Rights. The aim of this paper is to reflect upon how the right to respect for private life as contained in the European Convention on Human Rights has impacted upon the regulation of various forms of covert surveillance by the police in the UK, and to consider the question of whether reliance on a concept of privacy can provide an adequate basis for laws governing overt surveillance by way of closed circuit television systems.

## Privacy and Covert Surveillance

Despite (or perhaps because of) the vast literature surrounding ‘privacy’, it has proved to be a somewhat nebulous concept. Wacks has argued, “Privacy has been so devalued that it no longer warrants if it ever did serious consideration as a legal term of art.” (Wacks, 1980a: 10). He continues, “the long search for a definition of “privacy” has produced a continuing debate that is often sterile, and, ultimately futile.” (ibid.). It is partly the difficulty of providing an adequate definition that has seen reluctance on the part of both Parliament and the courts to develop a domestic concept of privacy. Thus, despite the pertinent comment in the Canadian case, *R v Duarte* (1990 65 DLR (4th) 240, at 249), that ‘one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance’, such activities have been lawful within the UK even in the absence of legal regulation.

Despite the apparent difficulties of finding an adequate definition, a right to privacy is enshrined in many international documents and national constitutions. For example, Article 8 of the European Convention on Human Rights provides a right to “respect for private and family life”, which has affected, and continues to affect, UK law. Therefore, despite the lack of protection for privacy in domestic courts, a relatively comprehensive regulatory regime for state surveillance practices has developed over the past twenty years. The next section will reflect upon the influence of the Convention on the regulation of police surveillance techniques to date, to be followed by a consideration of how this influence might be developed and extended to the regulation of overt public space surveillance.

### *European Convention on Human Rights*

The European Convention on Human Rights sets out a minimum statement of rights to be protected in each signatory state, and provides a mechanism to allow individuals to enforce it against the state where the state has infringed their rights under the Convention and domestic law has failed to provide a remedy. In the context of state surveillance, the right most obviously under threat is the right to respect for private life contained in Article 8, which states:

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.

Before considering its particular application to the regulation of surveillance by the police, it is worth noting a number of general principles that have derived from the interpretation of the exceptions to the general right.

- In Accordance with the Law

European Convention jurisprudence has interpreted Article 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 UK* (1984) 7 EHRR 14, *Leander v Sweden* (1987) 9 EHRR 433). In *Kruslin v France* ((1990) 12 EHRR 546), a case concerning 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”. More recently the Court has expressed the view that as the interception of communications represents a ‘serious interference’ with private life the law must be particularly precise (*Kopp v Switzerland* (1999) 27 EHRR 91). With regard to interferences with private life in the ‘prevention of crime’ context, it appears that the European Court is demanding increasingly rigorous legal provisions (*Valenzuela v Spain* (1998) 28 EHRR 483).

- Legitimate Objective

If the primary right is engaged in a particular case then any interference with that right must be directed towards a legitimate aim. In terms of the right to private life, restrictions that may be justified are found in Article 8(2). The restrictions on the primary right are numerous and widely drawn and it is not overly burdensome to require state conduct to remain within such boundaries.

- Necessary in a Democratic Society.

This is essentially a test of proportionality. It has to be shown that any interference with a Convention right is both necessary to fulfil a pressing social need and is a proportionate response to that need. The importance of the aim in question and the actual situation through which the aim is being secured are factors to be taken into account (*Silver v UK* (1983) 5 EHRR 347). As stated by Harris et al, “action for the prevention of crime may

be directed against homicide or parking offences: the weight of each compared with the right sought to be limited is not the same” (Harris, O’Boyle and Warbrick, 1995: 297).

The lack of any legal regulation governing the use of electronic surveillance devices by the police in the UK would inevitably be problematic in light of the above principles. Attention was specifically drawn to this fact by the well-documented case of *Malone v Metropolitan Police Commissioner No.2* ([1979] 2 WLR 700). The defendant was prosecuted for allegedly handling stolen property and it became apparent during the trial that the prosecution had tapped Malone’s telephone. He challenged the legality of the tap only to find that there had been no violation of English law. Megarry V-C recognised that the interception of the defendant’s telephone calls was not a crime and as such ‘it was not a subject on which it [was] possible to feel any pride in English law’ (ibid: 732). Malone took his case to the European Court in Strasbourg who held that his right to respect for private life under Article 8 had been infringed (*Malone v UK* (1984) 7 EHRR 14). The interception of a telephone call fell within the definition of both ‘private life’ and ‘correspondence’ in Article 8(1) (*Klass v Germany* (1978) 2 EHRR 214). The Court acknowledged that although Home Office guidelines governed the use of the telephone tap this did not satisfy the requirement that an infringement of a person’s right to respect for their private life could only be legitimised if there was a legal rule directed towards one of the legitimate exceptions.

[T]he requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which the [police] are empowered to resort to this secret and potentially dangerous [measure]. (*Malone v UK*: para. 67)

Largely in response to this decision (and the privatisation of the telecommunications service), the Government introduced the Interception of Communications Act 1985 (IOCA) (Lustgarten and Leigh, 1994: ch.3). Through the 1985 Act the Government sought to provide a statutory framework for legitimate interception. Regrettably the Act went no further than the *Malone* judgment demanded and, as such, the misleadingly named Act regulated merely public telephone interceptions and the metering of telephone calls. During its passage through Parliament, the Act was criticised as “setting out to regulate canal traffic in the age of the high speed train and the motorway” (H.C. Debs, vol. 75, col. 241). To govern the use of public telephone interceptions whilst ignoring other forms of aural electronic surveillance was indefensible (see, Leigh, 1986). Subsequent caselaw also suggested that the Act failed to regulate the interception of cordless telephones (Effick [1994] 99 Cr. App. R. 312) or non-public networks (*Halford v UK* [1997] EHRLR 540). The number of warrants issued and those in force under IOCA increased virtually year on year until the Act was repealed by the Regulation of Investigatory Powers Act 2000 (Akdeniz, Taylor and Walker, 2001). Whilst a legal basis for interception was formulated (albeit rather loosely drafted), it was questionable whether clear limits and remedies were created (Taylor and Walker, 1996). With regard

to interceptions based on national security grounds it has been suggested that an adequate legal basis had been established (*Christie v UK* (1994) DR 78-A, 119, but see, Fenwick, 2000: 331) though in relation to the prevention of crime it is doubtful that the 1985 Act was sufficiently clear as to when an interception might occur (see, *Valenzuela v Spain* (1998) 28 EHRR 483).

Given the lack of comprehensive legislation to govern all forms of interception, the emphasis was very much on reflecting the specific demands of the adverse *Malone* judgment than any real concern to protect privacy. As Fenwick suggests, “since the driving force behind the response of the UK government in the [Act] was a need to provide a statutory basis for interception, it can be termed a largely procedural rather than substantive reform” (Fenwick, 2000: 346).

It would take a further expensive and arduous journey to the Strasbourg Court to challenge the use of other covert surveillance techniques. In 1992 the police placed an aural surveillance device on the property of Mr. Bashforth who was, at the time, under investigation for dealing in heroin. Mr. Khan visited the house, and, by means of the surveillance device, the police obtained recordings of a conversation in the course of which Khan admitted that he had been involved in the earlier importation of drugs by Newab. He was arrested as a result. At Khan’s trial the judge admitted evidence from the tape recording and Khan was sentenced to three years’ imprisonment. The House of Lords rejected an appeal stating that even if they were to take into account a possible breach of Article 8 of the Convention (which they were not obliged to do prior to the Human Rights Act) this did not necessitate exclusion of the evidence gained as a result. Lord Nolan said:

It would be a strange reflection on our law if a man who has admitted his participation in the illegal importation of a large quantity of heroin should have his conviction set aside on the grounds that his privacy has been invaded (*R v Khan* [1996] 3 WLR 162 at 175).

At Strasbourg the case presented a relatively straightforward breach of Article 8 (*Khan v UK* (2001) 31 EHRR 1016). Though the breach of privacy arguably could have been justified by reference to the ‘prevention of disorder or crime’ exception, as in *Malone* the lack of clear legal regulation of the surveillance practices in question failed the test of being ‘in accordance with law’. A further question for the Court was whether evidence gathered in breach of Article 8 thereby infringed an individual’s right to a fair trial under Article 6. If the fairness of the trial would be affected, the evidence gained as a result of the breach of Article 8 should be excluded from the trial. Taking into account the proceedings as a whole the Court found that there would be no unfairness in admitting the evidence. Such a decision has implications for future evidence gathering. Despite the recent developments towards a comprehensive regulatory framework for surveillance, evidence gathered in breach of the framework, which would thereby be likely to infringe Article 8, could still be admitted in criminal proceedings.

One of the effects of the Human Rights Act 1998 (HRA) is that it gives domestic judges the opportunity to interpret the Convention in a domestic context. Whilst taking into account Strasbourg jurisprudence, there is no necessity to follow it as binding precedent. Therefore, if the courts were to take an active interpretation of their role under the HRA, the conclusion of the inter-play between Article 6 and 8 could be different, thereby granting greater respect for the private life of citizens. However, given the current interpretation by the courts of their discretion to exclude unfairly obtained evidence, this appears unlikely (Fitzpatrick and Taylor, 2001).

It has been argued that Part III of the Police Act 1997 was passed when it became clear to the Government that they would lose the case of *Khan v UK* in Strasbourg (Starmer et al, 2001: 36, see also, *Govell v UK* (1997) 4 EHRR 438). Indeed, when the case was in the House of Lords, Lord Nolan had recommended that the Government legislate in the area to satisfy the Convention standards (*R v Khan* [1996] 3 WLR 162 at 175). Senior police officers too expressed a desire for electronic surveillance to be legally regulated given that the powers of the security services to carry out similar actions had already been given express legal approval in the Security Services Act 1989 (ironically, itself in part a response to *Harman and Hewitt v UK* (1992) 14 EHRR 657), and that the Intelligence Services Act 1994 and the Security Services Act 1996, had expanded the role of MI5 to aiding the police with preventing and detecting serious crime (Home Affairs Committee, 1995: 124, para. 4.11; 136, para. 3.8).

Part III of the Act was designed to regulate surveillance techniques that would otherwise involve unlawful conduct on the part of the police such as trespass or criminal damage. Article 8 was the obvious driving force behind the legislation. It would ensure that the regulatory scheme for surveillance techniques was widened, with respect for private life being the overall context. However, as with IOCA, significant gaps in the law remained. The legislation failed to regulate techniques involving, for example, long range microphones, telescopic lenses or other 'remote' techniques. Devices installed with the consent of the person in a position to give such consent for the premises were also left unregulated, entirely failing to respect the privacy of persons who are on the premises but do not know of the surveillance operation. The basis for allowing surveillance was unduly broad and appeared to be wider than the administrative guidelines they replaced. The lack of mandatory judicial supervision of authorisation procedures has been viewed as a 'great weakness' (Uglow, 1999: 296) and at best marginally satisfies the criteria for authorisation laid down in *Klass* (*Klass v Germany* (1978) 2 EHRR 214, paras.55-6), which views supervision by the judiciary as desirable though other independent safeguards might suffice. The Act represented an opportunity missed to provide a comprehensive framework for the regulation of all technical surveillance operations. Again, though it could be argued that the impetus for the legislation was the European Convention, the Act appeared to represent an attempt to head off future adverse rulings from Strasbourg rather than being a meaningful attempt to respect the private life of the individual. Though Article 8 reflects a minimum standard to be achieved, the Police Act appeared to be a minimalist attempt to achieve it.

The Regulation of Investigatory Powers Act 2000 (RIPA) finally represented a legislative attempt to provide comprehensive regulation. The Human Rights Act 1998 (HRA) was designed to give the European Convention a more central role in domestic law. A requirement of the HRA was that all legislation, past and present, wherever possible should be read and given effect in a way compatible with Convention rights (s.3) and where relevant to proceedings before them, the courts must take into account jurisprudence from the European Court (s.2). Furthermore, all public authorities are required to act in compliance with the Convention unless they are prevented from doing so by statute (s.6). This would have the effect of ensuring that the target of any unregulated surveillance practice by the state would have a right to a remedy in a domestic court. Arguably RIPA is, therefore, a further example of legislation in this field being driven by the demands of the Convention: certainly the timing would suggest so. However, it too has been criticised for its procedural rather than substantive compliance with the Convention. Despite the statements by the Home Secretary, Jack Straw, that RIPA is Convention compatible and that it is “a significant step forward for the protection of human rights in this country” (HC Debs. vol.345 col.767), Fenwick argues, “[I]n certain respects the RIPA realises the worst fears of those who viewed the HRA as likely to lead to a diminution in the protection for liberty in the UK” (Fenwick, 2000: 345).

Part I of the Act supersedes IOCA 1985 and extends the definitions of interception to include most forms of telecommunication including email. Judicial authorisation of warrants was not adopted in the legislation which still allows for executive authorisation. Part II of RIPA provides a regulatory framework for the use of three types of covert surveillance, namely, directed surveillance, intrusive surveillance and the use and conduct of covert human intelligence sources. However, the different authorisation standards applicable to intrusive and directed surveillance are difficult to justify and might not satisfy Convention standards. Part II also allows for a considerable amount of detail to be determined through the use of delegated legislation that does little for the clarity of the law. In *Amman v. Switzerland* ((2000) 30 EHRR 843) the European Court re-iterated the need for clear and precise rules governing covert surveillance techniques. Whether Part II of the Act meets those standards is open to debate.

Part III was seen as one of the more controversial aspect of the Act. It relates to the power to issue notices requiring the disclosure of encrypted material and the creation of an offence of failure to comply with such a notice. It is in such instances where a minimal interpretation of the Convention has led to the statutory rubber stamp for somewhat illiberal state action.

On the positive side, the Act is comprehensive and places many previously legally unregulated surveillance techniques on a statutory basis. However, the law remains fragmented – it does not offer a single legal regulatory system (Justice, 1998: 15) though one was promised by the Home Office (Home Office, 1999: para 4.1) – and the law remains weak in terms of the protection for privacy in electronic communications and the imposition of regulation. It is an Act that is not so much directed at the protection of

privacy, as a measure designed to ensure that the HRA has little impact upon the area. As Fenwick has argued:

Under the rhetoric about protecting human rights ... lies an unadmitted concern – to keep scrutiny of such matters outside the courts ... whereas had powers of surveillance remained on a non-statutory basis they would have been vulnerable to challenge under Article 8 of the Convention ... .  
(Fenwick, 2000: 345)

In summary, one could argue that the effect of Article 8 has been to ensure the development of a comprehensive statutory regime governing covert surveillance techniques. Unfortunately, the minimalist interpretation of Article 8 by the legislators has had a detrimental effect upon the quality of those laws. Successive pieces of legislation appear to simply rubber stamp or extend existing practice. However, the Convention is a living instrument and in recent years has been requiring ever-stricter standards in relation to state surveillance. Given this, and the input of the domestic courts' interpretation of Article 8, it could mean that the regulatory system will have to evolve to meet more exacting standards. Whether those standards will apply to overt surveillance techniques in the form of public space CCTV remains a matter of interpretation. However, if one wishes to influence the debate about the extent of privacy rights in the public arena an attempt must be made to justify that position by reference to theoretical foundations.

## **Privacy and Public Space Surveillance**

Given that the use of covert technical surveillance now has a comprehensive regulatory framework, albeit one that is heavily criticised, could the Convention also place similar demands on the use of the now ubiquitous public space visual surveillance schemes? If one could assert a claim to privacy in public, or a claim to privacy regarding the collection and retention of images recorded, legislation would have to follow. However, would the notion of asserting privacy claims in public lead to the common good being systematically neglected, as some would argue? In this section I will use Feldman's construct of privacy to establish that privacy can operate in the public arena. Following this, Etzioni's claims that privacy rights in the US have adversely affected the common good will be addressed to illustrate how this can be avoided in the development of domestic law.

The influence of the European Convention has not yet been fully realised in the area of public space surveillance. Firstly, there has been very little discussion of overt public space surveillance to date and, secondly, now that the Convention rights can be interpreted in domestic courts one might anticipate such interpretation to be more liberal, without the need to remain within the parameters of international consensus, thus jurisprudence from Strasbourg is not determinative of an issue. How then, might the concept of privacy be utilised in public space?

In the US, which has developed its notion of privacy over a century, the seminal Supreme Court decision in *Katz v United States* (1967, 389 U.S. 347; Shattuck, 1977: 16) determined that the test of privacy was not dependant wholly on location but where one would have a 'reasonable expectation of privacy'. Justice Harlan expanded on the test thus:

...there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognise as 'reasonable'. Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the plain view of outsiders are not protected because no intention to keep them to himself has been exhibited.

Subsequent cases have indicated that what is already in the public domain can be recorded and disseminated since it would amount to no more than exposing what could already be seen. For example, in *California v Greenwood* ((1988) 486 US. 35), the Supreme Court ruled that citizens could have no reasonable expectation of privacy in items they discarded in the dustbin for the express purpose of having strangers take it away.

Despite this US interpretation, it could be argued that we all carry out acts in public that we would consider to be of a 'private' nature, where subjectively, we might have exhibited an expectation of privacy. Furthermore, though we may have exposed certain actions to public gaze, this does not necessarily mean that we would be happy for many different actions, in different locations, to be recorded and collated into a permanent record of behaviour over a particular period. In open, publicly accessible spaces "ordinary people expect to remain anonymous. ... scrutiny of more than a casual character would seem to offend reasonable expectations of being able to remain anonymous" (Von Hirsch, 2000: 61). Norris and Armstrong have argued that although the law does not recognise a right to privacy in public "it is clear that rules governing the production and reproduction of order in public space are finely attuned to its micro-sociological dimensions." (Norris and Armstrong, 1998: 4). In co-presence the watcher and the watched can read signals from each other, such as a threatening look, and can challenge or question each other accordingly. CCTV surveillance modifies this relationship. The watcher and the watched are 'distaniciated'. The potential subject of surveillance does not know the extent to which he is being watched, if at all, but may modify his behaviour nevertheless. Whilst no one would anticipate a casual look to be a threat to privacy, how might prolonged visual surveillance fare?

Feldman's analysis of the right to privacy is instructive here (Feldman, 1994). He asserts that every individual will be part of a multitude of different interlocking spheres within society, such as through their workplace, membership of social clubs, family and so on. Each sphere represents an area marked off from those outside it, whilst inside, individuals have relatively little privacy against others in that sphere for the purposes of that sphere. For example, whilst those in the family home may enjoy a significant degree of privacy

from the outside world, they enjoy considerably less privacy as regards each other for the purposes of living in the communal environment. An appeal to privacy thus assumes a conflict of interests, differing according to the circumstances. Such an analysis offers an alternative to the idea that what occurs in public cannot, as a matter of fact, be private. Privacy in each sphere operates in four dimensions: space, time, action and information (ibid. 52). In relation to the use of public space CCTV one cannot control the spatial element of who can watch, or set time limits on when people can watch, but arguably there can be an active element and an information element. For example, though limited, one could have a claim not to be the subject of intensive surveillance without due cause, and a stronger claim to control the diffusion of information about what has occurred there. Though the expectation of privacy may be considerably reduced in a public setting, this does not automatically mean that all privacy is lost. The operation of public space CCTV might be justified on crime control grounds, but that incursion into privacy does not therefore mean that the CCTV operator can intensively focus on individuals without good cause or do as he or she wishes with the recorded images:

If the surveillance is overt, it carries with it a clearly implied threat that the fruits of the surveillance may be used for purposes adverse to the interests of the person being watched. This is calculated to undermine people's commitments to their own plans and values. It thus represents a failure of respect for people's dignity and autonomy (ibid.: 61).

Nissenbaum argues that a theory of privacy in public has never fully developed because until the advent of modern technology it has never really been an issue (Nissenbaum, 2000). As such traditional theories have reflected the dichotomy that privacy refers to intimate areas and public to non-intimate areas. Feldman's construct is not wholly bound to the ideas of the intimate and the non-intimate. To stray from the traditional theories might be to produce another ingredient to an already complex dish but:

... although an important purpose of philosophical theory is to introduce greater conceptual rigour, a normative theory that strays too far from ordinary usage and popular sentiment is thereby rendered unhelpful, or worse, irrelevant (ibid.: 19).

Whilst it can be seen that overt CCTV surveillance could theoretically impinge upon a right to privacy, does Article 8 itself currently demand practical measures to uphold privacy in this respect?

The European Court has never sought to give a conclusive definition of privacy, considering it neither necessary nor desirable. However, in *Niemietz v Germany* ((1992) 16 EHRR 97) the Court stated:

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 since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world. (ibid.: 29)

The 'right to establish and develop relationships with others' reinforces the idea that privacy vests in people not places, and as such could be capable of being exercised when in a public environment. Harris et al comment, "the expanding understanding of private life set out in the Niemietz case indicates that a formal public/private distinction about the nature of the location will not always be decisive" (Harris, O'Boyle, and Warbrick, 1995: 309). A pertinent factor should, perhaps, be the subjective behaviour of the individual rather than their location. A homeless person living his life in public spaces still has a right to have his private life respected. Prolonged or regular visual surveillance of them is arguably a failure to respect that right, if it is not based on justifiable grounds. However, the Strasbourg Court has not yet moved to a position of accepting visual surveillance per se as an affront to privacy, albeit one capable of legitimisation under the appropriate circumstances outlined in Article 8(2).

In *Friedl v Austria* ((1995) 21 EHRR 88) the applicant took part in a demonstration causing an obstruction to the highway. When the police broke up the demonstration they took photographs of the participants, including the applicant. The Austrian Government gave assurances that the photographs were taken solely to record the nature of the incident and no names were recorded, or action taken to identify the persons photographed by means of data processing. The Commission attached weight to these assurances and, noting that there had been no intrusion into the 'inner circle' of the applicant's private life; that the demonstration was public; and the applicant was there voluntarily, found that the taking and retention of the photographs did not breach Article 8. The questioning of the applicant to establish his identity and the recording of these personal data was an interference requiring justification under Article 8(2). This is consistent with the idea that; '[P]rivacy involves a bundle of interests, rather than a single right, so loss of part of the bundle does not entail loss of the whole'. (Feldman, 1994: 61)

The decision is also in line with the case of *X v United Kingdom* (App. No. 5877/72), where, similarly, the taking and storage of photographs of a woman taking part in a demonstration was not a prima facie breach of Article 8. Fenwick, aligned with other authors, argues that there is an identifiable trend within the European Court for a broadening scope of Article 8, and this is an area where one should look to the evolutive nature of the Convention rather than to individual decisions (Fenwick, 2002: 704). However, to find that CCTV surveillance in public spaces is a breach of privacy per se would be to broaden Article 8 in a way that, it appears, the European Court is not prepared to do. In 1996 Pierre Herbecq, a Belgian national and secretary-general of the 'Human Rights League', argued before the Commission on Human Rights that the use of public space CCTV interfered with his right to privacy (*Herbecq v Belgium*, App No.

32200/96). He was concerned that the cameras were not regulated by law thus depriving citizens of the knowledge of when they might be surveilled and by whom. As such people would censure their behaviour in order to avoid being conspicuous, effectively producing a 'chilling effect'. Herbecq did not complain about the recording of the images or their possible dissemination. The Commission declared the application inadmissible. As nothing was recorded, there wasn't any material that could have been made available to the general public, or used for anything more than keeping watch on places. What was being watched was simply public behaviour.

From the above cases it would appear that a dominant theme is the control of personal information. If the use of public space CCTV involves the collection and storage of information relating to identifiable individuals then this is more likely to engage Article 8. A case involving the legally unregulated use of CCTV surveillance is currently awaiting determination in Strasbourg. In August 1995 Geoffrey Peck, suffering from depression, allegedly attempted to kill himself using a kitchen knife. He had walked through the centre of Brentwood, Essex, with the knife in his hand and the incident was recorded by the CCTV operator. The police were alerted and Mr. Peck was detained under the Mental Health Act 1983. This incident was later included by the Council in a positive press release about the benefits of its CCTV system. Subsequently, a regional television company obtained a copy of the footage for broadcast. Although Mr. Peck's face was masked by the television company at the Council's request, a number of viewers still recognised him. Following a complaint by Mr. Peck the Independent Television Commission decided that the footage breached their privacy requirements. An unmasked photograph of the incident later appeared in a local newspaper, and the footage was also shown on national television by the BBC, again unmasked. The Broadcasting Standards Commission also held that an unwarranted infringement of privacy had occurred. Mr. Peck's application to Strasbourg regarding a potential breach of Article 8 is not based on the existence of the cameras, but on the disclosure of recorded material to the media. In support are a number of cases from the European Court that emphasise that Article 8 can be engaged when public authorities store and use personal information.

It is evident that domestic common law is also moving towards a position of protecting such information. In the High Court hearing of the Peck case in 1997 Harrison J. stated:

I have some sympathy with the applicant who has suffered an invasion of his privacy ... Unless and until there is a general right of privacy recognised by English law... reliance must be placed on effective guidance being issued by Codes of Practice or otherwise, in order to try and avoid such undesirable invasions of a person's privacy ([1998] CMLR 697).

It has been suggested that such a general right to privacy is beginning to emerge. Over the past decade the law of confidence has developed into what some would argue is a de facto privacy law. In *Hellewell v Chief Constable of Derbyshire* ([1995] 1 WLR 804) Laws LJ said:

... the disclosure of a photograph may, in some circumstances, be actionable as a breach of confidence. If someone with a telephoto lens were to take from a distance and with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would ... as surely amount to a breach of confidence as if he had found or stolen a letter or diary in which the act was recounted and proceeded to publish it.

Cases such as this had to be treated cautiously, however, being an application for an interim injunction it meant that the plaintiff only had to make out an arguable case. However, the passing of the HRA has given the courts the impetus they needed to continue the development of the law. Fenwick states that the HRA “provides the normative impetus for the consolidation of the radical developments” in cases such as *Hellewell* (Fenwick, 2002: 581). In the recent case *Douglas v Hello!* ([2001] 2 WLR 992) which involved the prohibited taking of photographs at a wedding, Sedley LJ stated that the law of confidence had now developed to the point at which it could provide a right to privacy as distinct from confidence. Privacy extended to:

those who simply find themselves subjected to an unwarranted intrusion into their private lives. The law no longer needs to construct an artificial relationship of confidentiality between intruder and victim: it can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy (ibid: 1025).

Undoubtedly the parameters of this common law action will develop only after much debate and legal activity. However, the recording and dissemination of CCTV material, such as in the *Peck* case, may well fall within those parameters. Though Mr. Peck’s actions were carried out in a public place, it could be argued that to broadcast the footage on national television represented an unwarranted intrusion into his private life.

With the reducing cost of CCTV systems there are few publicly owned schemes that do not have the capacity to record information. Therefore, if such publicly owned schemes can engage the right to privacy, such surveillance should be in accordance with law, aimed at a legitimate objective, and be necessary and proportionate.

The recent enactment of the Data Protection Act 1998 may prove to be a satisfactory form of domestic regulation as far as the Convention’s relatively limited demands require, but arguably it will fail to have a significant impact in this area. The Act requires that those who operate CCTV systems (data controllers) and who record images from which individuals can be identified, must register with the Information Commissioner and ensure that the system is operated in accordance with the data protection principles. The extent to which they impact on CCTV systems is made explicit through the guidance given in the CCTV Code of Practice published by the Information Commissioner (Data Protection Commissioner, 2000).

The first principle requires that data be processed fairly and lawfully. One aspect of this is that the CCTV system must be operated for a 'legitimate reason'. The prevention and detection of crime would satisfy this. The 'fair' processing of images would also require, in many instances, that adequate signage give the public notice of who collects the data and for what purpose. The second principle 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 would help to ensure the confidentiality of information obtained. Thirdly, data should be adequate, relevant and not excessive. This would have implications for privacy in terms of ensuring that cameras were not monitoring individuals in private spaces. The fourth and fifth principles necessitates that personal data should be accurate and, where necessary, kept up to date, and should not be kept longer than is necessary. Finally, adequate measures should be taken against unlawful processing. This would include satisfactory security arrangements in terms of who could access the recorded material. These requirements could ensure that at least the privacy of recorded information could be maintained.

However, the statute does have a number of drawbacks. Firstly, one would have to question how many data controllers are aware that the new DPA applies to recorded CCTV images. Furthermore, even if the data controller is aware, are the day-to-day CCTV operators aware of the requirements of the Act? Given the widespread adoption of CCTV surveillance there has been relatively little publicity or education about how the law applies to CCTV. The 1984 version of the Act was criticised as a "paper tiger" (Davies, 1996: 104) and Flaherty suggested, in 1989, that;

Data protection agencies are, in many ways, functioning as legitimators of new technology. ... [T]hey act rather as shapers of marginal changes in the operating rules for such instruments of public surveillance. (Flaherty, 1989: 384)

Similarly, it could be argued that the DPA has failed to have any significant impact upon the public. If the public are not aware that they have the right to see data that a CCTV operator may hold on them, how will they be in any position to challenge abuse except in the most obvious of situations? The role of the Information Officer has grown in recent years but the Office lacks the powers and resources to actively ensure CCTV is effectively regulated, though it may technically be 'in accordance with law'.

To be a justifiable incursion upon the right to privacy, CCTV surveillance must satisfy a legitimate aim. The most obvious legitimising factor from Article 8(2) is the prevention of disorder or crime. The claims in support of CCTV as a crime prevention tool are many and given considerable media attention (Norris and Armstrong, 1999: 60). The Home Secretary of the day, Michael Howard, was quoted as saying, 'I am absolutely convinced that CCTV has a major part to play in helping to detect, and reduce crimes and to convict criminals'. (ibid. 63)

Yet there has been relatively little reliable evidence to support this view. What evidence exists has been referred to as "post hoc shoestring efforts by the untrained and self

interested practitioner.”(Pawson and Tilley, 1994: 291). As a crime detection tool, CCTV has been shown to work in specific instances though the effect of its wholesale use is rather more ambiguous. Though crime detection is not included in a literal reading of Article 8(2) it is likely that the courts would adopt a more purposive interpretation. Whether widespread use of CCTV in public spaces is a proportionate response to an identified problem is perhaps more debateable. Rather than being a well-directed measure aimed at a particular target CCTV arguably is sometimes installed in public locations as part of a domino effect:

CCTV is now seen as the fashionable solution to everything. Councils are saying we need CCTV, either for political reasons, or because the town next door has got it... (quoted in Clarke, 1994: 28).

The right to privacy in public is a relatively weak right whilst the prevention of crime is an important social objective. However, there is arguably an element of arbitrariness in the proliferation of CCTV schemes to areas that provide little evidence of a need for mass surveillance. One could argue that by their very nature crime prevention measures are necessary before a real problem arises, and it is the flexibility of the language in the Convention that can be problematic when seeking to buttress rights. Of course, a reliance on privacy should not become a cloak for criminal activity, but arguably what is absent in the CCTV context is a system whereby schemes can only operate under licence in areas only where a legitimate need can be identified. This should require evidence to be provided as to when, where and how CCTV is seen to be an appropriate response to an identifiable problem. Once operational, the controls placed by the DPA on the collection, storage and dissemination of data (including images) are, in principle, sound policies and would be adequate when coupled with greater powers of enforcement. However, would legislation with its roots in privacy be detrimental to the common good?

## **The Limits of Privacy**

Within a liberal political framework privacy rights are principally and undeniably individualistic, and are, of course, not without their critics. Restricting the activity of the state reduces its ability to intervene to ensure that society is organised more equitably for the weakest groups, or to ensure that a greater balance is struck between individual rights and social responsibilities. Etzioni, for example, argues that in the US privacy is treated as a highly privileged value but that it is not an unmitigated good (Etzioni, 1999). “In several important matters of public safety and public health, the common good is being systematically neglected out of excessive deference to privacy.” (Ibid: 4). In the UK the position has not been replicated. The US has developed its concept of privacy over a century to the extent that it now holds a place as an implied constitutional right. In the UK the courts have only just begun to develop the concept of privacy. However, if privacy were extended in limited circumstances to public spaces, or the DPA was not considered to be an adequate response in privacy terms to public space CCTV, would such a development be detrimental to the common good? Having established that an

assertion of privacy in public is possible, this section seeks to ascertain that this claim need not necessarily adversely affect the common good.

Etzioni suggests a number of criteria to help determine whether the balance between individual rights, in this case privacy, and the common good has been achieved (Ibid. 10). His analysis obviously concerns the state of US law but can nonetheless be illuminating for the future development of UK privacy. Firstly, he claims that society should only take steps to limit privacy if it faces a well-documented and macroscopic threat to the common good. Arguably the European Convention takes such concerns into account through the exceptions outlined in Article 8(2). Disorder and crime are certainly well documented threats but before privacy is limited an evaluation should be carried out to determine whether CCTV really could be a solution to a particular problem. In essence, this is similar to the requirements of proportionality outlined earlier. The relatively weak status of privacy in public (or the collection of 'data' in the public domain) should therefore only be a bar to the arbitrary introduction of CCTV schemes in public spaces. If it could be established that a CCTV scheme was justifiable, a second issue must be considered. Can the common good be supported without privacy-destructing measures? From a political perspective CCTV is a very useful tool of crime prevention in that it is a highly visible response that invariably has the support of the media and the commercial sector. In the UK where 'rights' have traditionally been of a residual character, crime control has considerably over-shadowed concerns for individual liberties. As the then Prime Minister, John Major stated;

'Closed-circuit television cameras have proved they can work, so we need more of them where crime is high ... I have no doubt that we will hear some protest about a threat to civil liberties. Well, I have no sympathy whatsoever for so-called liberties of that kind.' (quoted in Groombridge and Murji, 1994).

If Article 8 were to apply to public visual surveillance systems it would at least ensure a debate about whether or not CCTV surveillance could be justified in an individual situation, or whether other methods of crime prevention might be equally, or more, successful with less intrusion. Indeed, as Etzioni points out (Etzioni, 1999: 213), it is social scrutiny of the community by the community that leads to the best crime prevention policy, namely, the community's own moral and informal enforcement mechanisms. This would lead to a reduction in the need for formal state surveillance. Whilst Etzioni uses this point to argue for less privacy, it may also support the case for increased privacy where the balance has tipped away from privacy. For example, to arbitrarily introduce CCTV into areas that do not necessarily support such a measure may be at the cost of community scrutiny, where individuals feel they no longer need to watch over each other as Big Brother is doing it anyway!

Thirdly, if privacy is to be curbed, is it to a minimal extent? For example, consideration should be given to the placement and number of cameras. A camera to monitor traffic flow would not necessarily require full pan, tilt and zoom facilities; indeed, the ability to record images might not be crucial. If Article 8 were engaged the issue of proportionality

would require that the least obtrusive means necessary should be undertaken, thus not barring surveillance, but ensuring it is appropriate and justifiable.

Finally, measures that treat the adverse effects of privacy-destroying methods are to be favoured over those that ignore such effects. The Data Protection Act attempts to ensure this in relation to the CCTV operators' collection and storage of personal data. For example, by placing limits on the duration images can be held for, and limiting the class of people to whom disclosure can be made, the Act is engaging measures that limit the privacy intrusion. However, as stated earlier, without stronger enforcement mechanisms much of the intention behind the Act might be lost.

In the US Etzioni argues for a reformulation of privacy to ensure that a more appropriate balance is found with the common good. In the UK it could be argued that the position is reversed. Privacy has long been a stranger to domestic courts, and the concept of privacy imported from the European Convention is far from an inalienable right. To extend the Convention's interpretation of privacy to the public sphere, or to apply its standards in regard to the collection of personal data in the public sphere, does not necessarily entail short-changing the common good. Privacy can be an essential element of a functioning community. Without privacy people might feel inhibited from forming close relationships within the family, or outside in social groups. It allows the social spheres to function and as a result a degree of privacy helps the community to function. Privacy need not displace the common good and whilst the European Convention can provide a framework for legislation, it is a matter for Parliament and the courts to determine exactly where the balance lies.

## Conclusion

It has been argued that a reliance on such a nebulous concept as privacy is not the long-term solution to resisting surveillance (Lyon, 2001). Paradoxically, it is a demand for privacy that drives the need for surveillance and therefore greater privacy and so on. However, a practical reality in relation to overt public space surveillance is that Article 8 already provides a context within which covert state surveillance takes place, and that reality recognises that privacy is not an inalienable right and that surveillance can be a necessity. Article 8 has ensured that the UK has, over the past twenty years, introduced a degree of legal accountability for covert police surveillance practices where none existed before. Arguably, successive governments have responded to the demands of Article 8 by introducing minimalist legislative responses, but without the impact of the Strasbourg Court very little would have happened in terms of privacy protection.

If it is accepted that privacy does not end when entering public spaces, at least to the extent of recording personal data, then the state should similarly be able to justify their reasons for infringing such a right, and should have their powers to do so explicitly detailed. Furthermore, once legislation is in place drawing on the principles derived from the European Convention, it could be applied to private operators, with necessity and proportionality being determined accordingly. The DPA, almost inadvertently rather than

by design, presents a reasonably sound ethical basis for CCTV operators to work from, and the proactive regulation of data collection and privacy protection has to be better than resorting to court action to develop the law. However, the enforcement mechanisms in the DPA arguably represent a rather weak response to the ubiquitous gaze of the surveillance camera. There are situations when the state has to intervene in the lives of its citizens, such as to prevent crime, but such intervention must be based on, and restricted by, principled legislation. Article 8 has played a major role in the development of comprehensive statutory regulation of surveillance practices, but as an international instrument it is inevitably imprecise and malleable. The development of a domestic concept of privacy through the Human Rights Act, based on the principles from Article 8, might ensure that not only are covert surveillance practices more tightly controlled, but that overt practices are also adequately regulated.

## Acknowledgments

I am grateful to my colleague Ben Fitzpatrick, and the anonymous referees, for their helpful comments on an earlier draft of this piece. Responsibility for errors remains my own.

## References

- Akdeniz, Y., N. Taylor, and C. Walker (2001) Regulation of Investigatory Powers Act 2000: Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights *Criminal Law Review*, February: 73-90
- Clarke, M. (1994) Blind Eye on the Street. *Police Review*, 5(August): 28-30
- Cooley, T. (1888) *The Law of Torts*. Chicago: Callaghan.
- Data Protection Commissioner (2000) CCTV Code of Practice. Available at: <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>
- Davies, S. (1996) *Big Brother: Britain's Web of Surveillance and the New Technological Order*. London: Pan.
- 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): 41-71.
- Fenwick, H. (2000) *Civil Rights: New Labour, Freedom and the Human Rights Act*. Harlow: Longman.
- Fenwick, H. (2002) *Civil Liberties and Human Rights*. (3rd ed.) London: Cavendish.

- Fitzpatrick, B., and N. Taylor, (2001) Human Rights and the Discretionary Exclusion of Evidence. *Journal of Criminal Law*, 65(4): 349-359.
- Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press.
- Groombridge, N. and Murji, K. (1994b) As Easy as AB and CCTV? *Policing*, 10(4): 283-290.
- Harris, D.J., M. O'Boyle, and C. Warbrick, (1995) *Law of the European Convention on Human Rights*. London: Butterworths.
- Home Office (1999) *Interception of Communications in the United Kingdom* Cm.4368.
- JUSTICE (1998) *Under Surveillance*. London.
- Leigh, I. [1986] A Tapper's Charter? *Public Law*, Spring: 8-18
- Lustgarten, L., and I. Leigh (1994) *In From The Cold: National Security and Parliamentary Democracy*. Oxford: Clarendon Press.
- Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- Nissenbaum, H. (1998) Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17: 559-596.
- Norris, C., and Armstrong, G. (1998) Introduction: Power and Vision, in C. Norris, J. Moran and G. Armstrong, (eds.) *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate, 3-20.
- Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg
- Pawson, R. and Tilley, N. (1994) What Works in Evaluation Research? *British Journal of Criminology*, 34(3), 291-306.
- Shattuck, J.H.F. (1977) *Rights of Privacy*. Skokie: National Textbook Company.
- Starmer, K., M. Strange and W. Whitaker (2001) *Criminal Justice, Police Powers and Human Rights*. London: Blackstone.
- Taylor, N., and C. Walker (1996) Bugs in the System. *Journal of Civil Liberties*, 1: 105-124.

Uglow, S. [1999] Covert Surveillance and the European Convention on Human Rights. *Criminal Law Review*, April: 287-299

Von Hirsch, A. (2000) The Ethics of Public Television Surveillance, in Von Hirsch, A. D. Garland and K. Wakefield (eds.) *Ethical and Social Perspectives on Situational Crime Prevention*. Oxford: Hart, 59-76.

Wacks, R. (1980a) *The Protection of Privacy*. London: Sweet and Maxwell.

Wacks, R. (1980b) The Poverty of Privacy. *Law Quarterly Review*, 96: 73-89.

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