Switching Off the Surveillance Society? Legal Regulation of CCTV in the United Kingdom

Lilian Edwards[1]

1. Introduction

The United Kingdom is the most closely watched society in Europe, and possibly, the world today. Since the late 1980s, over 1 million closed circuit TV (CCTV) cameras have been installed in Britain, with an estimated 500 or more being added every week[2]. Indeed in January 2004, the *Independent* reported that over 4 million cameras were being used in the UK, 20% of all the CCTV cameras in use in the world, and that the average Briton was caught on camera 300 times a day[3]. If anything the trend towards more extensive CCTV coverage is accelerating, as surveillance schemes are being introduced not just to improve policing and security, but in non-crime related areas such as the reduction of traffic congestion: the London Congestion Charging Scheme, for example, introduced in February 2003, relies on about 700 CCTV cameras covering around 203 entrances/exits to the 21 square kilometre London central zone[4]. Linked to techniques such as neural network facial recognition , car number plate recognition, and multimedia image databases plus the new "joined up" UK ID card scheme, such schemes though installed for reasons not connected to crime and security, could potentially prove to be highly privacy-threatening.

CCTV cameras are ubiquitous to the point of omnipresence in the UK: located in workplaces, housing estates, public thoroughfares, schools, and hospitals; on high streets, in shopping centres and malls, inside car parks and stores, in banks and post offices; on buses, coaches, and other forms of public transport. Some CCTV cameras are operated by private individuals, or corporate security organisations, while others are operated by local authorities, the police and other government or state-affiliated bodies. CCTV in public areas was heavily subsidised by governmental aid to local authorities during the Thatcher years, and still swallows a high proportion of total spending on crime

---

[1] Co-Director, AHRB Centre for Research in Intellectual Property and Technology Law; Senior Lecturer, Edinburgh Law School.

[2] Goold B.J. *CCTV and Policing* (2004, Clarendon Press).

[3] http://news.independent.co.uk/uk/this_britain/story.jsp?story=480364 .

[4] http://www.spy.org.uk/cgi-bin/cclondon.pl .

prevention (79% of total expenditure between 1996 and 1999[5]). As Goold remarks, although Britain may not yet have reached the stage where there is a camera on every street corner, that day is perhaps not so far away[6].

Systematic CCTV surveillance, or "the surveillance society", as an apparent enemy of basic human rights of privacy, is regularly criticised in some more politicised parts of the legal, technological, journalistic and academic press. On the other hand, among the general public, attitudes to CCTV are still broadly positive, with CCTV seen as a symbol of watchfulness, security and "hands on" control of crime[7]. Obviously any state with "a camera on every corner" runs a risk of becoming the classic Orwellian "Big Brother" telescreen society, feared and bemoaned by privacy activists everywhere[8]. But CCTV also has many publicly beneficial uses. In the public sphere, police forces and local authorities regard it as one of their main weapons in the fight to maintain control of petty crime, especially in open and public urban spaces. Cameras and video surveillance are intended to deter "spur of the moment" crimes such as car theft, shoplifting, vagrancy , breach of the peace, public drunkenness and assault, as well as generally to promote public order. If such crimes do occur, CCTV is one of the main ways of gathering evidence to successfully prosecute the perpetrators. Rates of pleading guilty for protagonists caught on CCTV are reportedly extremely high, resulting in reductions of costs and time spent for police and courts and distress to witnesses and victims[9]. CCTV may also be used initially to detect and identify the criminals, a function which might once have required questioning many hundreds of witnesses or informants. CCTV partially substitutes for manned surveillance and information gathering and thus assists detection of crime, especially when budget cuts make manpower redeployment in police forces essential. Potential victims among the ordinary public, especially the old, young, disabled and otherwise vulnerable, may well feel they

[5] See Koch, B.C.M. *The Politics of Crime Prevention* (1998, Ashgate).
[6] Goold, supra n 2, p 2.
[7] Ibid, p 20-43. The Information Commissioner is in the process of tendering for further work into "public attitudes to the deployment of surveillance techniques in public places" following suggestions by the Home Secretary that there is a need for better public debate on the issue (see consultation paper *Access to Communications Data – Respecting Privacy and Protecting the Public from Crime*, March 2003). See also HL Select Committee on Science and Technology, Fifth Report, infra n 12.
[8] Privacy International (http://www.privacyinternational.org/) is perhaps the UK civil liberties organisation with the most critical watching brief in relation to CCTV. In 1995, Simon Davies, the head of Privacy International expounded: "There is a grave risk that the CCTV system is out of control. Fuelled by fear of crime, the systems take on a life of their own, defying quantification and quashing public debate. In a very short time, the systems have challenged some fundamental tenets of justice and created the threat of a surveillance society. Once more, traditional approaches to law enforcement and social justice are being undermined without due process." (Cited in Simon Davies *Big Brother: Britain's Web of Surveillance and the New Technological Order* (1996, Pan Books). Spy.org are also leading a UK Public CCTV Surveillance Awareness Campaign at http://www.spy.org.uk/wtwu.htm .
[9] See the Scottish Centre for Criminology report on the Airdrie CCTV scheme, 1998, at http://www.scotcrim.u-net.com/.

would rather sacrifice a degree of personal privacy for a degree of personal protection (though this trade may in fact be illusory, as many privacy activists claim CCTV does not in fact deter crime as advertised but merely displaces it, or is not as cost effective a method of deterrence as other less privacy-invasive strategies such as better street lighting or more obvious manned surveillance[10]).

In the commercial sector, employers are also increasingly using CCTV to monitor their workers in an attempt to meet several goals: to promote greater efficiency among employees while reducing the cost of human supervision; to reduce crime, truancy and anti-social behaviour at work (eg, assaults on fellow employees) and provide a record of such if it occurs; to assess the employee environment to see if it could be optimised (eg, do employees waste time browsing the Internet or getting up to talk to other colleagues?); and to reduce and manage legal and other risks both for themselves and for employees ands customers (eg, are employees harassing female employees sexually? Are they downloading pornography or viruses? Are they short-changing customers?).

The question then is not *whether* CCTV should be regulated, so much as *how* should it be regulated so that a correct balance can be struck between the legitimate and publicly useful goals of video surveillance, and the fundamental human right of privacy, both for citizens and for employees. In this area, the UK balance to date is often seen as flawed. The issue of privacy has been substantially highlighted since the incorporation of the European Convention on Human Rights into UK domestic law by the Human Rights Act 1998; and perhaps even more significantly by the revision and extension of data protection (DP) law in the UK which occurred when the EC Data Protection Directive 1995[11] was implemented domestically in the shape of the Data Protection Act 1998. Prior to these events, CCTV enjoyed something of a regulation-free "honeymoon period" in the UK, largely controlled only by erratic, inconsistent and ill-maintained voluntary Codes of Practice. However by 1998, the House of Lords Select Committee on Science and Technology was noting that if public confidence in CCTV was to be maintained, there needed to be tighter control over its deployment and use[12].

---

[10] See Davies, supra n 8. See also http://www.privacyinternational.org/issues/cctv/cctv_faq.html .
[11] 95/46/EC .
[12] Fifth Report , available at http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldselect/ldsctech/064v/st0501.htm .

Unlike in many other European countries[13], there is no specific legal regime of licensing or control of CCTV operations in the UK, whether for private or public operators, and indeed, it is perhaps for this very reason that the UK has become so recognisedly a CCTV surveillance hotspot. Instead regulation, such as it is, is now mainly[14] to be found in the shape of three broad legal paradigms not specifically tailored to deal with CCTV: EC DP law as implemented in the UK in the Data Protection Act 1998 ("the 1998 Act") ; the emerging and much contested common law of privacy and breach of confidence; and the laws of (primarily) criminal evidence which control whether information gathered by CCTV is admissible in courts. In terms of enforcement and review, again, no one public post-holder exists whose remit is to maintain oversight of CCTV surveillance, but the Information Commissioner's office, which is responsible in the UK generally for the DP system, has taken especial note of the growth of CCTV both in public and in the workplace following the extension of the definition of "personal data" in the 1998 Act to clearly include visual surveillance images, and the Information Commissioner has recently issued both a specific CCTV Code of Practice[15] (now amended in light of the controversial leading case of *Durant v FSA*[16]) and a Data Protection Code on Monitoring at Work[17] which refers expressly to video surveillance and to the CCTV Code. Both of these are discussed in detail below, as is *Durant*. It is clear that the then Information Commissioner, Elizabeth France, felt it imperative that CCTV be controlled not just by many incoherent and un-reviewed industry Codes of Practice, but by "legally enforceable standards", and that this would have the dual role of both providing certainty for CCTV operators and reassurance to the public that safeguards were in place.

As well as formal legal regulation, CCTV is also still controlled to some extent by extra-legal codes of practice or "soft law", which, although not sanctioned directly by law enforcement bodies, may have some regulatory force (for example, breach of a code may result in sanction by an industry

---

[13] See elsewhere in this volume.

[14] It is possible that various other UK laws might also be used to control CCTV but there is no reported evidence of such. The new Sexual Offences Act 2003 in England and Wales contains a novel offence of "sexual voyeurism" which some civil liberties groups have suggested might be used to prosecute those who use CCTV for covert monitoring.in places such as changing rooms or toilets. The problem however is that the law demands evidence of "sexual gratification" by the offender as a result of viewing the scene in question, which considerably limits the applicability to "CCTV snooping".

[15] July 2000, available at http://www.informationcommissioner.gov.uk .This was in fact the first Code of Practice issued by the (then) data Protection Commissioner under the 1998 Act.

[16] [2003] EWCA Civ 1746.

[17] The Employment Practices Data Protection Code, part 3: Monitoring at Work, and Supplementary Guidance, available as above n 15.

body, or bad public relations)[18]. The Information Commissioner Code of Practice on CCTV is itself an odd hybrid in that it emanates from a public body independent of the government and commerce, thereby commanding more attention than an ordinary industry association; and it combines rules which "check off" legal requirements of DP law, with guidelines which merely indicate "best practice". We will examine the modes of legal control in turn below, with an emphasis on the pre-eminent regime in the area which is that of DP law.

[18] See further empirical research and discussion in Goold, Chapter 4, supra n 2.

2. Data protection law and CCTV

European DP law controls the automatic or partly automatic processing of "personal data" relating to "data subjects", which is collected or held by "data controllers". These latter must abide by the DP rules and in particular the Eight Data Protection Principles, implemented in the UK in Sched 1 to the 1998 Act, and foremost amongst which is the idea of "fair processing". DP law is harmonised on a European basis, although significant differences of interpretation do exist between member states, which have as yet mostly not been smoothed out by the European Court of Justice (ECJ). European DP law demands in essence that (with certain important exceptions) consent[19] be given to the collection of personal data from data subjects[20]. Furthermore, those who process[21] personal data ("data controllers[22]") must publicly notify the purposes for which the data is being collected[23] and not then go on to use or disseminate the data in ways outwith these purposes[24]. Notification of these purposes must be given to a body independent of state or commerce[25] (in the UK, the Information Commissioner) which is also responsible for ensuring compliance with the entire DP regime. Requirements as to data security[26] and how long data can be retained[27] are also part of the general scheme, as is the right of the data subject to access their personal data from whoever holds it[28], and, if necessary, correct it[29]. Special rights and duties exist in relation in particular to "sensitive personal data"[30] and the use of data for direct marketing[31]. European DP law is an omnibus rather than a sector-specific scheme of personal data privacy protection, intended to apply as much (say) to information collection and processing by hospitals, direct marketers, banks, supermarkets and credit reference agencies as CCTV operators. For this reason the rules operate at a level of some generality, unusual in UK legislation, and the Information Commissioner's office, as

[19] DP Directive 1995, Art 6 and 7 and Art 2(h).
[20] Ibid, Art 2(a).
[21] "Processing" is given a very wide meaning in DP law: Art 2(b) of the DP Directive 1995 defines it to include "collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, aligment or combination, blocking, reassure or destruction." Processing need also not be by automatic means, though it must be an "operation or set of operations". Manual files are also now included in the DP regime, subject to transitional arrangements.
[22] See DP Directive 1995, Art 2 (c).
[23] Ibid, Arts 18-19.
[24] Ibid, Art 6 (1) (b) –(c).
[25] Ibid, Art 28.
[26] Ibid, arts 16 and 17.
[27] Ibid, art 6(1)(e).
[28] Ibid, art 12.
[29] Ibid, art 14.
[30] Ibid, defined in art 2.
[31] Ibid, art 11.

noted above, sought to help the public by issuing its first Code of Practice in the domain of CCTV in July 2000, to assist in guiding CCTV operators, especially in small schemes, on how to comply with the law in this area.

2.1 Personal data

Whether CCTV footage falls within the category of "personal data" is the essential first step to deciding if and how CCTV is regulated by DP law. Section 1(1) of the Data Protection Act 1998 defines "personal data" as

> "data which *relate to* a living individual who can be *identified*
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller…." [italics added]

Thus on first principles it would appear that CCTV images captured of living individuals will be "personal data" so long as an individual can be identified who is depicted on-screen. This wide interpretation of personal data would have the *prima facie* consequence that all operators of CCTV schemes however basic would need to notify with the Information Commissioner as data controllers and that all identifiable CCTV images would be subject to the full DP requirements of fair processing (subject, of course, to exceptions such as those intended to promote law enforcement and national security[32], and to promote freedom of expression[33]). Only pictures of people who could not be identified would fall outside the scope of the DP regime, and, even then, not if they could be identified if cross-referenced with other data the data processor had, or was likely to have : for example, images in stadiums or cinemas can be cross matched with seat records; shops can match

[32] See ss 28 and 29, 1998 Act.

[33] See s 32, 1998 Act. But note that the exemption of journalists from seven of the Eight DP principles (data security is still required) is limited by a "public interest" test: s 32(b). It is an open question if it could ever be in the "public interest" for a journalist to train a CCTV camera on the door of (say) a celebrity's home or place of work night and day – the result at the High Court stage in *Campbell v MGM* [2002] EWHC 499 (QB), where an award of damages for breach of DP rights, albeit nominal, was made to Ms Campbell in similar circumstances involving mere "still" press photographs, as opposed to CCTV, would seem to indicate not. See further the discussion of the common law of privacy and the implications of the *Campbell* case below.

images of customers paying with names on credit cards or store cards they used during the transaction[34].

However in the leading case, of *Durant v FSA*[35] this wide interpretation of "personal data" was unexpectedly narrowed by the English Court of Appeal. *Durant* was not itself a case concerning CCTV images, but is recognised to have had a serious impact on the regulation of CCTV[36]. Durant was in dispute with Barclays Bank, and made a complaint to the Financial Services Authority (FSA) about their behaviour, which lead to a confidential inquiry by the FSA into the bank's conduct. Durant, having already failed in various law suits against Barclays, now sought sight of all records held by the FSA which mentioned his name or in were in any way "related to" him, on the grounds that they were "personal data" of which he was the subject and to which, by ss 7(1) and 8(2) of the 1998 Act, he thus had rights of access. The focus of *Durant* was thus primarily on how widely the phrase "relate to" in s 1(1) should be interpreted, so as to determine what information Durant had a right to see. This was an unexpected line of enquiry, as most academic commentary before that case had anticipated dispute only about the meaning of the phrase "identified".

A second area of dispute in *Durant* concerned redaction. Durant had already been given sight of some records by the FSA which had been "redacted" ie, had had the names of parties other than himself masked out so as to preserve their rights of privacy. DP law recognises that the privacy rights of third parties mentioned incidentally in records must be preserved notwithstanding the rights of subject access granted to data subjects. A balance is set up in s 7(4)(b) of the 1998 Act whereby if a data controller cannot comply with the request in hand without disclosing information identifying another individual, he is not obliged to comply with the request unless *either* that other individual consents *or* it seems reasonable to comply with the request without that consent. The question in *Durant* was whether Durant had a right to insist on seeing the un-redacted originals. In the CCTV context, an equivalent question would be to ask when an image of an identifiable

[34] See Carey P, *Data Protection : A Practical Guide to UK and EU Law* (Oxford University Press, 2nd edn, 2004) Chapter 15: CCTV.
[35] Supra, n 16.
[36] See for example Rowe H "CCTV Systems and the Data Protection Act 1998" (2004) 20 (3) CLSR 221. *Durant* lead directly to special guidance appearing as fast as possible on the Information Commissioner's website amending the CCTV Code of Practice: see http://www.informationcommissioner.gov.uk/cms/DocumentUploads/CCTV%20additional%20guide.pdf ..

individual must be obscured or "pixellated out" before a CCTV tape can be shown to another data subject or to a third party such as the police[37].

On the first point as to the width of the phrase "relate to", two interpretations were quoted from the Shorter Oxford Dictionary: a narrower definition which said it meant "having reference to, concern" ; and a wider definition , namely, "having some connection with, be connected to". Auld J, giving the lead opinion of the court, preferred the more restrictive definition. This was, he claimed, more in accordance with the purposes of the EC DP Directive, which were to give the data subject access to "information about himself" and not to specific documents *per se.* Section 7 of the 1998 Act, which implemented that part of the Directive in the UK, similarly was not intended to be an "automatic key to information", nor to allow access to any and all documents mentioning the data subject's name, nor, importantly, any and all which might be retrieved by putting the subject's name into a search engine. Instead, the aim of the data subject access rights was merely to enable the subject to protect *his privacy* by finding out what the data controller held about him, and whether the processing of that data unlawfully infringed DP law.

Auld J, having effectively narrowed the definition of "personal data", then gave two examples of what types of information *would* now be subject to DP protection. "Mere mention of the data subject in a document held by a data controller," would not, he opined, "necessarily amount to his personal data." Whether any particular information amounted to "personal data" would in general depend on where it fell in a "continuum of relevance or proximity" to the data subject. However, for guidance, if information was "biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or event that has no personal connotations" then it was likely to be regarded as "personal data" [38].

Secondly, the matter of "focus" needed to be taken into account.

> "The information should have the data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or

[37] A third point discussed at length in *Durant* related to the definition of manual filing systems for DP purposes: however this is not relevant to the topic of CCTV regulation and so is here omitted.
[38] *Durant v FSA*, supra n 16, para 28.

had an interest… In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity."[39]

Accordingly in the case at hand, many or most of the records Durant sought, which bore his name as the complainant and which would be found if Durant's name was used as a search term, but which fundamentally related to Barclay's Bank rather than containing "biographical details" about Durant, or with a "focus" on Durant, were no longer to be regarded as "personal data" relating to Durant, and thus he had no rights as data subject to request access to those records.

On the redaction issue, the issue was largely a dead one by this stage as so much of what Durant was seeking access to was no longer defined as his "personal data". Accordingly, Auld J merely noted, first, that if the identifiable references to other individuals contained in a record were not "personal data" relating to the applicant under the new, narrower interpretation, then no balancing act need be done under s 7(4) at all , ie, there was no need to decide if it was "reasonable" to release the information to the applicant (and thus blanket redaction would in many cases be justified) . Secondly, Auld J noted that even if references did constitute the "personal data" of *both* the applicant *and* another data subject, the data controller was not required to go through a first step of seeking the consent of that other person if it *was* reasonable to release the information. Thirdly, in deciding what was "reasonable", a data controller should take into account the "legitimate interest" (if any) the data subject had in requesting the disclosure of the identity of another identifiable third party individual; and the degree to which the third party information necessarily formed part of the data subject's *own* personal data to which access was sought. These last two factors were unlikely to come into conflict, as it would be "difficult to think" of a case where third party information was so bound up with the applicant as to constitute "personal data" relating to the applicant and yet the applicant had no legitimate aim in obtaining that third party data.

Durant is a very understandable decision on its own facts. The Court of Appeal was stuck between the rock of data protection and the hard place of forcing a data controller like the FSA to effectively give access to all its confidential records to an individual who might abuse that access, and at the expense of its own external relationships with the community it regulates. The FSA is a regulatory body whose efficiency is (or was) based on being able to investigate financial organisations on a

[39] Ibid.

basis of confidentiality (it should be noted this case preceded the coming into force of relevant freedom of information legislation). Durant was, in essence, it seems, seeking not so much traditional data subject access rights, as rights of freedom of information in relation to the FSA investigation which UK law simply did not give him at the time. He was also seeking a last bite at the cherry having failed to see Barclay's Bank punished both in his own litigation and during the FSA investigation. It is clear the court felt he was more interested in finding out "personal data" about others rather than himself, with a view to more litigation, not protecting his own privacy – a fundamental misconception of what DP law is meant to do – hence, no doubt, the repeated emphasis in the opinion on the purpose of the DP Directive being to protect the data subject's own *privacy*.

But transferred to the context of CCTV and data subjects whose images are captured on CCTV, *Durant* unexpectedly ushers in a major change in the law and one which may well jeopardise the legitimate expectations of privacy of UK citizens and employees, and be out of step with the rest of the European DP community. Indeed, several commentators have suggested that the *Durant* decision should have been referred to the ECJ to provide a harmonised EC response[40]. The Information Commissioner has now issued detailed guidance on what the narrowing of the definition of "personal data", and the two new guidelines as to "biographical" data, and "focus" mean in the context of CCTV[41]. The new guidance advises:

> "…If you have just a basic CCTV system, your use may no longer be covered by the DPA. This depends on what happens in practice. For example, small retailers would not be covered who:
> - only have a couple cameras,
> - can't move them remotely,
> - just record on video tape whatever the cameras pick up, and
> - only give the recorded images to the police to investigate an incident in their shop.
>
> The shopkeepers would need to make sure that they do not use the images for their own purposes such as checking whether a member of staff is doing their job properly, because if they did, then that person would be the focus of attention and they would be trying to learn things about them so the use would then be covered by the DPA.

[40] See Chalton S. "Reflections on *Durant v FSA*: The Court of Appeals' interpretation of "personal data" in *Durant v FSA* – a welcome clarification or a cat among the data protection pigeons?" (2004) 20(3) CLSR 175; editor's opinion of Mason's Out-LAW Reports at http://www.outlaw.com, 19-5-2004.
[41] See http://www.informationcommissioner.gov.uk/cms/DocumentUploads/CCTV%20additional%20guide.pdf .

4. It sounds like many users of basic CCTV systems are not covered by the DPA, is there an easy way to tell?

Think about what you are trying to achieve by using CCTV. Is it there for you to learn about individuals' activities for your own business purposes (such as monitoring a member of staff giving concern)? If so, then it will still be covered. However if you can answer 'no' to all the following 3 questions you will not be covered:

- Do you ever operate the cameras remotely in order to zoom in/out or point in different directions to pick up what particular people are doing?
- Do you ever use the images to try to observe someone's behaviour for your own business purposes such as monitoring staff members?
- Do you ever give the recorded images to anyone other than a law enforcement body such as the police?"

As can be seen from the above, the Information Commissioner seems to be taking the approach that if a simple CCTV system is not intended to (or is not physically able to) "focus" on any given individual, nor is intended to provide specific intelligence of a "biographical" nature about a particular person (for example, follow a suspect employee around) then it is not collecting "personal data relating to" any person at all, despite the fact that images of living identifiable persons *are , in fact,* captured. And since no personal data is collected, there is no need to respect the rules of data protection, nor for the system operator to notify the Information Commissioner as a data controller. The CCTV system, it seems, entirely drops out of the DP net.

What about more sophisticated systems? The guidance continues:

> "In many CCTV schemes, such as are used in town centres or by large retailers, CCTV systems are more sophisticated. They are used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness or assessing how an employee is performing. These activities will still be covered by the DPA but some of the images they record will no longer be covered. So if only a general scene is recorded without any incident occurring and with no focus on any particular individual's activities, these images are not covered by the DPA. In short, organisations using CCTV for anything other than the most basic of surveillance will have to comply with the DPA but not all their images will be covered in all circumstances. *The simple rule of thumb is that you need to decide whether the image you have taken is aimed at learning about a particular person's activities*." [italics added]

This leaves open the possibility that although a CCTV system of a certain complexity may "qualify" for the DP regime – with the result that the CCTV operator will need, for example,

to notify the Information Commissioner as to the purposes for which he is collecting the data - the images of persons which are collected incidentally, without "focus", will not be regarded as "personal data". This mean the key obligations DP imposes *from the point of collection*, such as fair processing, data security and no unreasonable data retention, disappear. Furthermore, persons whose images are so incidentally collected, and which are thus not categorised as their "personal data", will have no rights to access or correct these images under subject access rules, nor, perhaps, to control how they are processed. They will have in principle, it seems, no right to demand that those images be "redacted" – edited out – if a tape on which they feature incidentally is given to another data subject featured therein - as, extending the dictum of Auld J, the "reasonableness test" under s 7(4) of the 1998 Act, which requires the data controller to balance the access rights of the applicant data subject against the privacy rights of any other party whose personal details are disclosed, will not cut in if those details are not deemed "personal data" of the third party captured[42]. (And since editing is an expensive process which many CCTV controllers would need to contract out, a simple request, un-backed by law, is unlikely to cut any ice.)

In essence, the degree to which these CCTV images are part of the personal private sphere of the individual identifiable therein, has ceased to be the focus of the law's concern; what will really matter, in practical terms, is the intentions and goals of the CCTV operator when he or she sets up the cameras and how this is translated into the physical set up and management routine of the system. This has potentially staggering implications in the CCTV field. What if the London Congestion Charging Authority – whose CCTV cameras are primarily intended to track license plates so as to identify who should be paying the toll - incidentally collect images of semi-famous celebrities in potentially embarrassing situations (eg, badly dressed or with unstyled hair)? Leaving aside issues of common law privacy (see below), in DP terms it seems these pictures might well not be "personal data" at all, because the celebrity would not have been the "focus" of the system nor does the picture tell you anything very "biographical" about him or her. Their presence is incidental to the data collector's notified purposes. Accordingly the DP regime would not apply at the point of collection. The London Congestion Charging Authority's notification says nothing about one of the purposes of their data collection activities being to collect pictures which might one day make their unwanted way to paparrazi – but it would

[42] *Duran v FSA*, supra n 16, para 55.

become a possibility, with no breach of the First Data Protection principle which requires that methods of collection of data be "fair". What then happens to the "reasonable expectations" and privacy rights of the millions (including but not limited to celebrities) who journey into central London by car every day in reach of the camera eyes?

Of course it could be argued that once an incidental image captured of – say – Kylie Minogue, had been discovered *and* offered to the *Daily Mail* for a four-figure sum, that data now would certainly *become* "personal data" relating to, and identifying, Ms Minogue, and thus the processing of it, in the form of distribution or sale, would be controlled by DP law, which would spring into action as a relevant legal regime. Indeed this seems to be the interpretation favoured by the Information Commissioner, since in the guidance notes quoted above, the third question the operator of a small CCTV system must ask to know if he or she still needs to notify under DP law post-*Durant*, is "Do you ever give the recorded images to anyone other than a law enforcement body such as the police?". However although this interpretation – the idea that CCTV images might not be "personal data" at the moment of collection but could be retrospectively constructed as such - is (a) still not very satisfactory as requirements of fair processing should operate from the moment of collection, not *post hoc* , and (b) though not ruled out by *Durant*, does not seem on close scrutiny to be backed by it either. Auld J's opinion seems impliedly limited to requiring an assessment of whether information is to be categorised as "personal data" (or not) at the time when the data subject access application is made, based on the history of the information to date[43]. There is no reference to any factors which might turn non-"personal data" into protected data in the hands of a data controller at some later date. One would hope that such an interpretation would however recommend itself to a later court: especially given the second clause of the definition of personal data in s 1(1) of the 1998 Act, which clearly contemplates future events being relevant to the classification of information as personal data (data may become personal data when combined with "other information which is in the possession of, *or is likely to come into the possession of,* the data controller") [italics added]. Any other approach would also apparently breach Art 8 of the European Convention on Human Rights (ECHR) as it would mean there was no legal remedy in UK courts for a breach of the Art 8 right to respect for private life, as upheld in *Peck v UK*[44]. In any case, it seems likely

[43]Ibid, paras 24-31.
[44] (2003) ECHR Application No. 44647/98. Discussed below in detail, PN 2004-84.

that *Durant* as a whole may soon hopefully appear before the European Court of Justice for review[45].

2.2 Processing by "automatic means"

Unfortunately there is currently little other guidance on the definition of "personal data" at the European level with which to perhaps re-interpret or rebut *Durant*. The recent ECJ case of *Lindqvist*[46] does touch on the issue of what is personal data, in relation to textual information uploaded to the Internet, but in the CCTV context it is rather more relevant on the question of "automatic processing"[47]. Records of personal data fall within the DP regime only if that data is processed "wholly or partly by automatic means[48]". *Lindqvist* confirms that the uploading of digital images to a home page constitutes "automatic processing" so long as some part of the process, not necessarily all, is automated, ie, carried out by software. Thus if a web camera ("webcam") is manually set up to take pictures of an area and upload them to the Web, and images are captured of living identifiable persons with them which are "personal data" (*pace Durant*), then the whole process falls within the DP regime regulating automated processing of personal data. Since much CCTV surveillance is now effectively being carried out "on the cheap" by webcams, and outdoor webcams themselves are a new growing source of over-looked and often relatively unregulated surveillance[49], this is a significant and welcome clarification.

2.3 *How does the data protection regime regulate CCTV?*

If a CCTV system *doe*s fall within the DP regime even after *Durant*, then what obligations or restrictions are placed on the CCTV operator/data controller, and what rights does the data subject have?

---

[45] http://www.outlaw.com , 19-05-2994, reported that Durant had filed papers with the European Commission claiming the UK government has not implemented the Data Protection Directive correctly.
[46] ECJ, Case C-101/01, 6 November 2003.
[47] All that is said about personal data is that it definitely includes "the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies" (ibid, paras 25, 27). An interesting contrast is the recent Icelandic Supreme Court decision in the albeit very different context of genetic/health data, *Gudmundsdottir v Iceland*, November 27 2004, which by contrast to *Durant* widens rather than narrows the national interpretation of "personal data".
[48] DPD, Art 3; 1998 Act, s 1(1), see definition of "data".
[49] See for example the webcam of Edinburgh at http://www.camvista.com/scotland/edinburgh/capcity.php3 .

(a) Notification: CCTV operators must notify the processing of CCTV images to the Information Commissioner[50]. Carey reports that the most common purpose notified for the collection and use of CCTV images is "crime prevention and the prosecution of offenders.[51]"

(b) Conditions for processing: Processing of CCTV images is in principle only legal where it is undertaken in accordance with one of the conditions in Sched 2 of the 1998 Act, foremost of which is consent by the person whose image is captured. Data subjects however rarely have an opportunity to give prior consent to CCTV surveillance except in relation to private workplace surveillance, where such consent may often be included as a term in the employment contract. (Note, however, that consent is defined in European DP law, though not in the UK Act, as "freely given and specific and informed"[52], which standard a simple standard form contract assent may not meet.) CCTV cameras set up in public places by law enforcement authorities and local authorities can usually be justified as "necessary for the administration of justice"[53] but in any case ss 28 and 29 of the 1998 Act provide that public surveillance for the safeguarding of national security or for the prevention or prosecution of crime (including tax evasion) is exempt from the First DP Principle. CCTV cameras set up in public places (eg outside shops) by private individuals or commercial organisations which film non-employees are more problematic. In practice, the solution is usually to place a notice prominently next to the camera and to assume that anyone who walks past then impliedly consents to their image being captured. This approach is implicitly rubber-stamped in the CCTV Code of Practice as meeting the requirements of the First DP principle, so long as appropriate details are given on the sign, and the sign is appropriately placed, visible, and of appropriate size. Signs should always give the following information: identity of person responsible for the scheme, purpose of the scheme, and details of whom to contact concerning the scheme.[54] Using CCTV without signage for covert monitoring can only be justified to prevent identified specific criminal activity in limited circumstances.[55]

---

[50] Again the limitations on this requirement post-*Durant* must be considered – see above.
[51] Carey, supra n 34, p 244.
[52] DPD 1995, Art 2(h).
[53] 1998 Act, Sched 2, para 5(a).
[54] CCTV Code of Practice, "Siting the Cameras", rule 10.
[55] Ibid, rule 10, second part.

(c) Fair processing: As well as being concerned about signage, the CCTV Code indicates that the requirements of the First and Third DP Principles (fair processing, and processing not to be in excess of the purposes for which undertaken) also imply certain restrictions on how the cameras are set up and at what they are pointed. For example, cameras should ideally only monitor the spaces intended to be surveilled and not scan areas beyond that scope; domestic areas such as gardens should be avoided unless the owners are consulted; operators should be trained to recognise the privacy implications of the scope of their activities, eg, sunbathers in their own gardens have a greater expectation of privacy than passers-by.

(d) Quality of images: The Third DP Principle combines with the Second (data to be collected and processed only for specific notified purposes) and the Fourth (data kept to be accurate and up to date) to prescribe detailed requirements for image quality which are spelled out in the CCTV Code of Practice. Users who have time and date stamping should make sure these systems produce accurate data. Maintenance logs should be kept of the machinery, and maintenance kept up to a certain standard.

(e) Data retention : The Fifth DP Principle prescribes that personal data must not be kept longer than is necessary for the purpose of collection. This length of time will vary for CCTV images according to the purpose for which they were collected. The CCTV Code suggests that publicans will need to keep recorded data no longer than 7 days as they will be aware fairly quickly if anything significant happened which needs investigated, eg, a bar fight; while banks might wish to retain images collected next to an ATM machine for up to 3 months in order to resolve customer disputes about cash withdrawals.

(f) Access to and disclosure of images: The Sixth DP Principle provides that data must be processed in acordance with the rights of data subjects. Accordingly, procedures must be put in place to enable individual access to CCTV images if they represent “personal data” relating to the data subject (although see discussion above re *Durant v FSA*). A standard data access request form should be provided, and a fee of £10 may be charged for access. Access requests may be refused if the data controller feels the request falls within one of the exemptions in the Act such as national security, in which case the refusal, and grounds for it, must be logged.

(g) Data security: The Seventh DP principle provides that data collected must be kept secure and measures must be taken to prevent accidental or unlawful damage to personal data. A British Standard provides comprehensive technical guidance on issues of data security, tape management etc.[56] Removal of the medium on which images are stored for viewing purposes, should be carefully logged to rule out tampering and to provide an accurate record what was stored thereon.

2.4 CCTV in the workplace

Data protection operates in the workplace, as in all other venues except those specifically excluded in the 1998 Act[57]. It is not however entirely clear how far DP law restricts the use of CCTV in the workplace. Historically, there was a general belief that employers were entitled to do what they liked to monitor their own employees, whether by automated or conventional means. Also, as noted above, employees will usually be asked to consent to the use of surveillance in their contracts of employment which at least on paper appears to meet the requirement of consent in the First Data Protection Principle. However this is not the end of the story. As it has become more common to extensively monitor employees' phone calls, email, web access and physical movements by CCTV, pressure has grown to recognise and regulate this unprecedented degree of surveillance, especially as working hours have lengthened in the UK and "call centre" culture has circumscribed exactly what workers can and cannot do at their workstations. Both European DP law, and European human rights law as implemented in UK domestic law, require a balance to be struck between the employer's understandable and legitimate interests to maximise productivity and minimise legal risk, and the Art 8 privacy, and data protection rights of employees, which are not lost even in the "public space" of the workplace. The CCTV Code of Practice, discussed above, explicitly does not apply to the workplace but only to areas where the public have "free and unrestricted access". However, another Code introduced by the Information Commissioner in 2003, the Employment Practices Data Protection Code: part 3, does explicitly deal with monitoring at work[58]. This Code has been extremely controversial during its consultation stages in upholding privacy rights for employees

[56] See BSI – BS 7958:1991 "Closed Circuit TV – Management and Operation of Code of Practice".
[57] Although the place of more general rights of privacy in the workplace remains contested: see McColgan A. "Do Privacy Rights Disappear In the Workplace?" (2003) EHRLR 120.
[58] Available at http://www.informationcommissioner.gov.uk/.

and generally requiring the least privacy-invasive form of monitoring to be adopted. This is despite that fact that the Code is still only advisory except where it is taken as explaining the ambit of DP obligations. Broadly, the Code suggests that the best way to approach workplace monitoring is to undertake an "impact assessment": a process whereby

(i) the *purposes* behind monitoring are identified

(ii) any *adverse impacts* of monitoring are identified, eg invasion of worker's privacy rights; impact on relationship of mutual trust and confidence between worker and employer

(iii) *alternatives* to monitoring or different ways in which it may be carried out are investigated, eg, effective training of employees rather than monitoring; follow up on specific incidents, rather than prior blanket monitoring,

(iv) the *obligations* that arise from monitoring are recognised , eg, notification to workers of monitoring taking place; and

(v) a judgment should then be made as to whether the monitoring planned is *justified*. In particular, the employer should bear in mind that "significant intrusion into the private lives of individuals" will not normally be justified unless the employer's business is at real risk of serious damage. Furthermore, intrusion should be "no more than absolutely necessary".

How does all this affect CCTV? It is noteworthy that while there is a special legal regime for authorisation of interception of electronic communications (such as phone calls, email and web traffic) by employers[59], CCTV does not fall within this as it does not involve interception and thus was not a concern of the parent Act to these regulations, the Regulation of Investigatory Powers Act 2000. This is perhaps unfortunate, and hard for the general public to understand. The Employment Code of Practice does specifically suggest that the CCTV Code may be useful by analogy to employers; that if possible video and /or audio monitoring should be aimed at areas of particular risk, and confined to areas where expectations of privacy are low (eg, presumably not staff washrooms or toilets). Workers should be given clear notifications that video or audio monitoring is being carried out and where, by clear permanent signs rather than occasional notifications. Covert monitoring is justifiable only in rare circumstances involving suspicion of criminal acts or equivalent malpractice, and it is "hard to see" when covert video

[59] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI No.

cameras in toilets would be justified[60]. Persons other than employees who may be caught by video monitoring must be made aware of its existence. Employees will, like other data subjects, have a right to access images of themselves captured on CCTV cameras (so long as they are their own "personal data", as discussed above.) However, if CCTV cameras are deployed purely for the notified purposes of preventing and detecting crime, then subject access rights will not operate under s 29 of the 1998 Act, which is *not* limited to exempting only processing by the police or other law enforcement authorities.

It is suggested that the vague platitudes of the Employee Monitoring Code (despite their controversial provenance) are likely to do little to prevent blanket CCTV monitoring in the workplace, in a climate where virtually every major UK employer now has some form of monitoring in place. Such CCTV monitoring might still however be challengeable as infringing (a) the Art 8, ECHR right to respect for private life; or (b) the emerging common law rights of privacy with which the English courts have been grappling lately. We shall now turn to these possible sources of legal regulation.

3. Common law rights of privacy and breach of confidence, and the European Convention on Human Rights, Art 8.

Is there a common law right to privacy in the UK which may, can or will be breached by non-consensual and/or covert CCTV surveillance? It might be charitable to say that the common law of privacy in the UK is currently in a transitional state, but perhaps more brutally accurate to say that it is a confused, internally contradictory mess. English (and by extension, UK) law has traditionally refused to recognise the existence of a free-standing right of personal privacy, either in private spaces such as the home or in the public sphere. Instead, other legal rights have been asserted to protect privacy interests by backdoor means, using laws such as nuisance and trespass, libel and defamation, DP law as discussed above, and most significantly, breach of confidence. This action, which begun very much as a commercial action to prevent theft of trade secrets leading to economic loss, has been developed by the courts in a series of recent well

[60] Employment Code of Practice, Part 3: Monitoring at Work, Supplementary Guidance , para 3.5.3. The Code does allow however that drug-dealing might justify such surveillance but in such cases, the police should be involved first.

known "celebrity privacy" cases - pre-eminently *Douglas v Hello!*[61] and *Campbell v MGM*[62] - to the point where it is now almost impossible to say if the UK does or does not have a law of privacy, or whether it merely has a law of breach of confidence widely extended beyond its commercial roots, which can in some cases, but significantly not all, be used to protect rights of personal privacy[63]. The issue of whether the UK has or should have a nominate law of privacy has of course been made prominent by the UK's implementation of the ECHR requirement in Art 8 that the state provide adequate remedies for breaches of the right to respect for private life. Lacking a constitutional or statutory foundation for privacy rights, the UK courts now find themselves trapped between the desire not to pre-empt Parliament by retrospectively inventing a highly controversial new privacy law, and the need to decide cases consistently with the UK's international and, now, domestic human rights obligations. The simplest solution would of course be for Parliament to step in, grasp the nettle; and legislate but at present the political will to take on the thankless task of reining in the UK's voracious tabloid press in the interests of the privacy rights of rich and vapid celebrities seems, understandably, to be somewhat lacking[64].

In October 2003, in *Wainwright v Home Office*[65], a case involving no celebrities but instead the strip-searching of ordinary mortals visiting relatives in prison, the House of Lords categorically declared there was no general cause of action in English law for invasion of privacy. Six months later, in *Campbell v MGM*[66], at least some of their Lordships appear to have come out in, if not exactly the opposite direction then at least something at 90 degree rotation. *Campbell* is a case highly relevant to the regulation of CCTV in that it deals with the non-consensual taking of still camera photographs. Paparazzi staked out famous supermodel Naomi Campbell and took pictures of her exiting a Narcotics Anonymous meeting, an addiction which she had previously

---

61 [2001] QB 967 (CA).
62 [2004] UKHL 22; [2002] EWCA 1373; [2003] QB 633 (CA).
63 See further the analysis in numerous academic articles, including Singh R and Strachan J, "Privacy Postponed" (2003) EHRLR 12; Hudson A "Privacy: A Right by Any Other Name" (2003) EHRLR 73; Milmo P. "Courting the Media" (2003) EHRLR 1; Bhogal M. "UK Privacy Update 2003", (2004) 1:1 SCRIPT-ed, ' http://www.law.ed.ac..uk/ahrb/script-ed/docs/privacy_comment.asp . Breach of confidence was not an applicable head of claim in *Wainwright v HMA*, discussed infra (intrusive strip search by prison guards argued to be breach of privacy, no "confidential information" in question); nor in *Peck v UK*, supra n 44 (CCTV footage of applicant considering suicide released on TV without his consent; as material in public domain, no damages for breach of confidence possible).In *Wainwright,* the plaintiffs were given no remedy at all; in *Peck*, the European Court of Human Rights found that UK law offered no remedy when one was required under Art 8 of the ECHR and so awarded damages for non-pecuniary loss, though not to any great figure. See below.
64 The HL Select Committee on Media, Culture and Sport recommendation in June 2003 that Parliament proceed with a statutory privacy law fell on notably stony ground with the government.
65 [2003] UKHL 53, [2003] 4 All ER 969.
66 [2004] UKHL 22.

denied. These photos were subsequently published in the *Daily Mirror*. Ms Campbell claimed at various stages of her case as it moved from the High Court to the Court of Appeal to the House of Lords that she had suffered breach of confidence, breach of DP rights, and common law invasion of privacy. At first instance, she was successful to some extent on all three claims but received only nominal damages of £3,500. That decision was then reversed by the Court of Appeal in October 2002, who essentially held that as Campbell had lied about her addiction, she had no right to use a common law action of privacy to present a false view of herself to the public. As a celebrity who made her living from being in the public eye, she should not complain when the publicity she got was unfavourable to her. The House of Lords decision of May 2004, which restored Ms Campbell's fortunes, was split 3:2 in her favour, and has to be regarded very much as a decision not only on its particular facts, but also from its particular selection of Law Lords. Much seems to have turned on the fact that the pictures taken were not just generally invasive but revealed a medical condition (drug addiction) and that Ms Campbell's attempts to deal with that condition would not be helped by the publicity resulting. Since in DP terminology, information about a medical condition would be regarded as "sensitive personal data" this approach is understandable. Lord Hoffman (who voted against the appeal) was the strongest in favour of a general right of privacy, stating that "the importance of this case lies in the statements of general principle on the way in which the law should strike a balance between the right to privacy and the right to freedom of expression". Lord Nicholls also dismissed the appeal but upheld the general idea of a right to privacy in English law, not just an extended action for breach of confidence. Meanwhile, Lord Hope, who voted for the appeal, stated that "The underlying question in all cases is ... whether the information that was disclosed was private and not public. There must be some interest of a private nature that the claimant wishes to protect."

Where does all this leave CCTV? The problem with CCTV and breach of confidence as the principle actionable basis for invasion of privacy is that being filmed on CCTV usually occurs in public, and so does not necessarily involve either the creation or the exposure of confidences. This was exactly the scenario in the leading case of *Peck v UK*[67]. Here, Peck, who suffered from depression, was filmed on a public street on CCTV by Brentwood Borough Council, holding a kitchen knife with intent to commit suicide. The council CCTV operator, alerted by the CCTV

[67] [2003] EMLR 15.

footage of the knife but not knowing Peck intended to self-harm, called the police, who arrested Peck and prevented his suicide attempt. Subsequently, stills from the footage of Peck holding the knife were released to the media to prove that CCTV was effective in preventing and detecting local crime. As a result, Peck's inadequately masked and identifiable features appeared in several papers and then on a TV "Crime Beat" programme before 9 million viewers. Peck, backed by Liberty, sued the Council, seeking judicial review of their decision to release the pictures without his consent and without adequate masking. This application was rejected, as the ground for judicial review was that no reasonable council would have made such a decision, a level of review which the court acknowledged was almost impossible to meet in these circumstances. The council had not acted unreasonably given they were empowered by statute to set up CCTV schemes, and were pursuing a legitimate aim in publicising their CCTV scheme by release of the pictures of Peck, in order to deter commission of crimes in their surveillance area. Judicial review was simply inappropriate as a mechanism for dealing with the invasion of Peck's privacy rights.

Peck applied again to the European Court of Human Rights, who found in January 2003 that his rights of privacy under Art 8 had indeed been breached and that there was no remedy available to him in UK domestic law. Judicial review of the council was, as already seen, inappropriate to properly protect his privacy rights; complaints could successfully be made to media industry watchdogs, such as the Press Complaints Commission and the Broadcasting Standards Commission, but they had no power to award damages to compensate Peck; and most importantly, the action for breach of confidence was ill suited to the facts of his case and almost certainly useless, as it was very difficult to establish that the information released about Peck "had a quality of confidence about it or had been imparted in circumstances implying an obligation of confidence[68]". Furthermore, once the pictures had entered the public domain, which had occurred before they were broadcast on TV, their re-publication would not be actionable as a breach of confidence, so again no right to damages would arise.

But this did not mean, the Court held nonetheless, that Peck had not suffered an invasion of his Art 8 rights. Significantly, even though Peck had been filmed in a public street, "he was not there for the purposes of participating in any public event, and he was not a public figure."

[68] *Peck*, supra, para H-22.

Accordingly, he still had, it seems, reasonable expectations of privacy which had been breached. The council had not acted wrongly in principle in filming him or by installing a general CCTV surveillance scheme in a public area: but they could have tried harder to meet his expectations of privacy, by asking him for his consent to the pictures being released, or managing to mask his features more adequately, and imposing (and enforcing) a condition of such masking on any third parties to whom they passed on the pictures. None of these had been done adequately. As a result, Peck was awarded damages of 11,800 Euros.

Peck opens up as many questions as it answers in relation to CCTV. How far does it offer a remedy to every person who is unknowingly caught on CCTV? How far is the remedy it gives dependent on its own facts? Was the invasion of privacy created by the taking of the CCTV pictures or by their subsequently being made public? If the latter, how great a degree of publicity is necessary to create a breach of privacy? Welch[69] suggests that the decision in Peck was based on several factors which may not always be replicated in other cases. First, the court emphasised that the pictures in question were shown before a huge TV audience – would the invasion of privacy have existed if only one still had appeared in one small circulation newspaper? Secondly, Peck was *not* a celebrity. Would he still have had the same expectation of privacy in a public place if he had been, say, Naomi Campbell, the instantly recognisable supermodel? Thirdly, Peck was walking along the road minding his own business, of a sort – would he have had the same expectation of privacy if he had been participating in a public event, say a demonstration[70]? Fourthly, Peck was engaged in a peculiarly personal activity, namely trying to commit suicide. Just as with Campbell's battle with drug addiction, the court will naturally be drawn towards thinking that his private sphere was being invaded. Would his privacy have been so invaded if the CCTV footage released had merely shown him walking along the high street doing his weekly shop? On the other hand, Peck *was* carrying a knife in public and the CCTV operator could not discern that the only person he planned to harm was himself. What if he *had* been committing a crime? Would the release of the pictures without his consent then have been an acceptable act by the council? The European Court does note at para 74 that the disclosure of

[69] Welch J. "Case comment: *Peck v UK*" (2003) EHRLR 141.
[70] Compare *Friedl v Austria* [1996] 21 EHRR 83 where the claimant was found not to have suffered a breach of Art 8 when the police took photos of him without his consent while he was on a demonstration. The Court there did however note that privacy rights might extend "to a certain degree [to] the right to establish and develop relationships with other human beings and the outside world."

pictures "was not made to catch a criminal or find a missing person but to respond to the general aim of publicising the effectiveness of the CCTV system". This seems to imply, as Welch suggests, that if the CCTV pictures *had* been released to help detect or prosecute a crime, then although Peck's Art 8 rights would still in principle have been breached, the breach would have been balanced by the legitimate goal of controlling crime, and the interference would thus have been proportionate and justified. Would release have been justified if Peck had been shown on tape acting suspiciously and the council was trying to identify him or track him down, but this behaviour later turned out (as was indeed the case) to be a result of mental illness rather than criminal tendencies? Arguably, yes: although the balance struck will be finer and more difficult one. It can be seen that, as with the *Douglas* and *Campbell* cases, a right of privacy plead under Art 8 of the ECHR still needs to be balanced against other pressing concerns, including the rights of a free press, and the duty of public bodies to attempt to safeguard society and prevent crime. Bypassing the problematic lack of a privacy law in the UK courts by moving to an Article 8 standard of critique in the European Court does not make this job any easier.

4. Law of evidence and admissibility rules

Finally, it should be briefly noted that the laws of admissibility of evidence are also relevant to the control of CCTV. In principle, rules of admissibility of evidence should promote good practice in the administration of CCTV schemes, since if those schemes breach basic rights of privacy and due process, then the evidence gathered using them will be inadmissible in court and useless to the police and prosecutors. In practice however, the rules of evidence in England and Scotland[71] are rarely used to exclude CCTV evidence in any significant way. Traditionally, English and Scottish laws of evidence do not make special cases of photographic evidence, whether of still images[72] or video footage[73], and these are admissible in principle subject to the normal rules of due process, just as is the case with oral or documentary evidence. In recent years, some amendments have been made to the PACE[74] code of practice which controls evidence collection and police procedure in criminal matters in England to deal specially with

[71] The criminal justice and evidence laws of the two jurisdictions are separate and very different. Reference here will mainly be made to the English position.
[72] *Rv Maqsud Ali* [1966] 1 QB 688.
[73] *R v Fowden and White* [1982] Crim LR 588.
[74] Police and Criminal Evidence Act 1984 ("PACE").This operates only oi England and Wales.

video evidence. In one high profile case, *Perry v UK*[75], collection of evidence by covert CCTV without consent and in breach of provisions of the PACE Code which was then used against an accused, was found by the European Court of Human Rights to be a breach of Art 8, even though the conviction had been upheld in the English courts[76]. However in practice, in most cases CCTV footage seems to be accepted fairly automatically by courts, and most difficulties have arisen either in relation to (a) inadequacies in the professional competence of experts hired to compare video evidence to other images of the persons allegedly identified on CCTV[77] or (b) in the handling of the videotapes or other storage medium by police or in the police station[78]. It seems fair to say that evidence law in practice does not represent much of an obstacle to a policy of blanket CCTV surveillance in public places by law enforcement and other public bodies, if this is the way the government wishes to go.

5. Conclusions

From a civil liberties perspective, the current legal regulation of CCTV in the UK seems clearly unsatisfactory. Data protection law, combined with the CCTV Code of Practice, in theory provides a satisfactory code for preservation of basic privacy and due process rights, but has, as explored above, been perilously undermined by the interpretation the courts have given to the key concept of "personal data" in *Durant v FSA*. In any case, the most ubiquitous CCTV cameras are those operated by both state and private interests to patrol crime and antisocial behaviour, and such surveillance will generally be exempted at least partially[79] from DP law under sis 28 and 29 of the 1998 Act, which exempt data collection and processing for purposes to do with national security and crime prevention. One problem not even touched on above is that of enforcement: even where DP laws do operate, estimates from privacy activism groups are that perhaps as few as 10% of CCTV cameras are in fact DP-compliant [80] . The lack of resources available to the UK Information Commissioner is a well known constraint on enforcement of DP generally, even in areas where there is more public pressure for enforcement (such as on

[75] European Court of Human Rights, Application No 63737/00, 2003. See also *R v Loveridge* [2001] EWCA Crim 973.
[76] However the remedy granted was a nominal award of 1500 Euros for non-pecuniary damage - hardly a reversal of conviction.
[77] See *R v Devaney* [2003] EWCA Crim 2109; *R v Stubbs* [2002] EWCA Crim 2254.
[78] See *R v Riley* [2003] EWCA Crim 1694.
[79] Though only the First DP Principle is knocked out by s 29; the other seven persist. Section 28 (national security) essentially removes the processing entirely from the ambit of DP law.
[80] See Privacy International website.

consumer websites) than there is in the generally publicly applauded domain of CCTV. It is also unhelpful that in the workplace sector, CCTV is uncontrolled both by the CCTV Code of Practice, and by anything akin to the regime for interception of employees' electronic communications to be found in the Lawful Business Regulations[81].

The growth in judicial activism in the area of common law rights of privacy may hold out the promise of alternative routes with which to restrain blanket CCTV surveillance; but not, as we have seen , if privacy remedies continue to be tied explicitly to the law of breach of confidence, which, even after *Campbell v MGN*, is unlikely to be suited to CCTV where invasions of privacy are most likely to occur in public spaces and in relation to non-confidential types of information. Even where Art 8 rights of privacy have been vindicated by the European Court of Human Rights, as in *Peck v UK*, more problems are raised by the way the cases are argued than are solved (and even in the successful cases, damages awards for non-pecuniary privacy losses have tended to be nugatory).

Simply put, nothing in current UK privacy law prescribes that blanket public CCTV surveillance is wrong in principle; although illegality may arise where (some) data is not fairly collected and (some) data gathered via such blanket surveillance is in some way wrongly processed or abuses fundamental rights of privacy. This is particularly true where surveillance is backed by the claim that it is being undertaken for the purposes of preventing and detecting crime. *Peck v UK* makes this very plain, both in its domestic judicial review, and its European human rights incarnations. The regulatory choice that needs to be made is thus a political one, for the legislature not the judiciary, as to whether it is appropriate, notwithstanding a laissez faire liberty stance, and a public interest in protection from crime and disorder, to create a society which edges dangerously near to a "Big Brother" world. Other choices can, and often have been made: in France for example, surveillance of public spaces cannot be undertaken without a prior permit from the state and even then only if a particular risk of assault or theft is established[82].

In making these kinds of fundamental privacy choices, however, it would be helpful if there was a more vigorous and informed public debate on privacy in public spaces than currently exists in

[81] See n 58, supra.
[82] Loi No.95-73 du janvier 1995.

the UK. One step in this direction may be a number of current campaigns to build "maps" of where CCTV cameras are sited in UK cities[83], with a view to scaling up public awareness of just how prevalent CCTV surveillance really is. But in the end, a society gets the privacy it wants, and if the UK's citizens, whether through ignorance or choice, prefer to live in a surveillance society to gain what they see, perhaps credulously, as better protection from crime and terror, then that is a democratic choice that must be respected – even by privacy activists.

[83] This is one of the projects currently being discussed at MySociety.org, a funded public interest software project site. See http://mysociety.blogs.com/mysociety/2003/10/cctv_map.html . There is also some work on such a project for the UK already ongoing at Privacy International. Elsewhere in Europe, CCTV cameras in Zurich have recently been mapped by privacy activists, and similar efforts have extensively mapped CCTV camera zones in New York and Washington (see http://www.epic.org/privacy/surveillance/). Interestingly one CCTV maps to be found on the Web, of the CCTV cameras in Lewisham (see http://www.lewisham.gov.uk/socialcare/cameras.htm) is provided by the local council, apparently to promote public trust, with no concern that it might reveal the threatening nature of pervasive CCTV.