Regulating CCTV

by A. A. Adams
School of Systems Engineering
The University of Reading
Whiteknights
Reading
RG6 6AY
Tel: 0118 378 6997
email: A.A.Adams@Rdg.ac.uk

Abstract

Given that the number of CCTV cameras in the UK is the largest in the world, and given that it is unclear when video data should be regarded as *Personal Data* (or what rights a blanket definition would reasonably provide to the surveilled) it is claimed that a CCTV Act is needed in the UK. This claim appears to be supported by the police authorities [Bal06a], although in addition to a broad claim regarding protection of privacy, their view is that private CCTV should be forced to be of sufficient quality and sufficiently accessible, to be of use to the police. Given the Office of the Surveillance Commissioners' [OSC] existing role in oversight of police surveillance operations, it is suggested that the OSC be made responsible for licensing and regulating CCTV systems and operators. Protection of raw video data as a potential source of *Personal Data* when processed is necessary (and currently outside the scope of the Office of the Information Commissioner [OIC]). Where raw video data is sufficiently processed to produce *Personal Data* or where it is linked with other data sufficient to identify individuals, the data would then pass to the aegis of the OIC. Specific proposals for securing data and infrastructure are suggested, in addition to some general *Surveillance Protection Principles*.

1 Introduction

Following the ruling of the Court of Appeal in Durant v FSA (Durant v FSA [2003] EWCA Civ 1746), raw video data is no longer regarded as *Personal Data*. This was never a suitable definition of such information, although the current definition that most video surveillance data is not protected is equally as bad. Given that the UK is acknowledged as the most visually surveilled society in the world, it is argued that it is time that the UK parliament passed specific legislation regulating the deployment and operation of CCTV systems.

We begin with a consideration of the development in UK law of the concept of raw video data as *Personal Data* in section 2. This is followed by a brief consideration of the concepts of identity, identification and authorisation (a subject to which much more significant consideration is needed in this context, but which is precluded by the limitations of space for this paper) in section 3. Section 4 concerns the regulation of organisations deploying and operating CCTV systems, something which has been sadly lacking in UK law. Necessity and Proportionality guidelines for when and how much CCTV surveillance is allowed are then considered in section 5 and followed by consideration of technological protections of privacy in section 6. Section 7 brings these threads together with concrete proposals for suitable elements of a regulatory regime for CCTV, including the appropriate regulatory body as well as some *Surveillance Protection Principles*.

2 When is Raw Video Surveillance Data *Personal Data*?

In publicly accessible areas of the UK, video surveillance is usually lawful provided members of the public are notified that video surveillance is in operation. There are details of who may run surveillance systems in what areas which we will discuss below (See section 4). Given that the organisation carrying out the surveillance is doing so

within the law, the only protection for the surveilled is if the data is regarded as *Personal Data*.

Between 1984 and 1998, video surveillance data not held on a computer was not subject to the provisions of the Data Protection Act 1984. Since most cameras in use in the UK were analogue cameras and recordings were held on video tape, the vast majority of video surveillance data was outside the scope of data protection.

Between 1998 and 2001, it could be argued that raw video surveillance data with no annotations or other analysis constituted data not held "in some structured fashion" and therefore should not have been regarded as "personal data" under the provisions of the Data Protection Act 1998. This was not the view of the Data Protection Commissioner, however, and in the guidelines provided by the office of the Data Protection Commissioner, it was clear that if an object of surveillance could be identified within a sequence then the Data Protection Commissioner regarded the sequence as constituting *Personal Data*. We will discuss below the problematic issue of multiple surveillance objects thus entailing video data sequences to be the *Personal Data* of multiple Data Subjects, as this remains an issue with current UK law and proposals for future regulations.

In 2001, the Freedom of Information Act 2000 amended the Data Protection Act 1998 in two relevant ways: one minor and one major. The minor one is that the Data Protection Commissioner was renamed the Information Commissioner and had their remit expanded to include significant other duties. The major change was that in order to provide an easy (though not necessarily a good) method for deciding on what data was subject to Freedom of Information and what subject to full Data Protection, even unstructured data about individuals became *Personal Data* and gained the full protections of the Data Protection Act 1998. This then formalised the existing view of the Data Protection Commissioner in regarding video sequences as the Personal Data of all those identifiable within the frame(s) and sequence(s) (see section 3 for some discussion on the issue of identity and identification within video surveillance).

Also in 2001, the first provisions of the Regulation of Investigatory Powers Act 2000 also came into force and the OSC was created and the Surveillance Commissioners appointed. It is clear from a close reading of these two acts that despite the plethora of CCTV cameras and systems in the UK, in the drafting of the Data Protection Act 1998, the Freedom of Information Act 2000 and the Regulation of Investigatory Powers Act 2000, CCTV surveillance was not a significant consideration in their preparation.

Despite the interpretation of the Data Protection Commissioner that raw video data constitutes *Personal Data*, there are no well-known instances of Data Subjects making a request under the Data Protection Act 1998 for copies of all *Personal Data* held including raw video data. In some circumstance, such as victims of crime, those accused of crime and those involved in disputes with the police over possible malfeasance in the execution of police duties, individual citizens (including police officers) and law enforcement agencies have requested or required access to raw video footage. Where the police demand such access there are often, though not always, well-established protocols for such requests.

In the 2003 Durant vs FSA case, Durant demanded access to a broad range of documents (not including raw video surveillance data) held by the FSA, each of which included some reference to Durant. The final judgement by the Court of Appeal (Durant v FSA [2003] EWCA Civ 1746) changed the interpretation of the Data Protection Act 1998 by the Information Commissioner. In particular, the Commissioner's interpretation of the application of the Act to raw video surveillance data switched radically. The Commissioner's current advice states[UK 05]:

> If you have a very basic CCTV system, its use may not be covered by the Data Protection Act.
> ⋮
> if your system is more advanced and allows you to zoom in on an individual member of staff whose behaviour is causing you concern, or you use cameras to monitor the movements and activities of your workforce, you'll need to inform us.
> ⋮
> . . . if a general scene is recorded without an incident occurring, the pictures are not covered.

This is a significant change in a number of ways, in that under the present interpretation by the Information Commissioner it is possible to be the Data Subject of a video sequence and to request access to that sequence while other individuals identifiable within that sequence no longer enjoy any protection. In some senses, therefore, it is the *intent* of the operator(s) of a surveillance system which defines the status of sections of data in the system. It is suggested that this does not provide a clear and useful boundary to the definition of status of data in recordings from surveillance systems.

Beyond the question as to when and for whom raw video surveillance data constitutes *Personal Data*, there are many other issues regarding regulation of both surveillance apparatus deployment and of the status of the data such systems generate.

3 Identity, Identification and Surveillance

So far, we have only considered the status of raw video surveillance data. In any surveillance activity, it is frequently the gestalt creation of a data shadow or data double from a number of sources of information which presents a significant threat to individual privacy, as opposed to any individual piece of or even set of single-sourced data. The creation of a data shadow depends on the association of data from multiple sources under a single *identity*. Sometimes this identity includes identification with social indicators such as a name. Consider the linking of timed video data from a London Underground tube station to the fare charging database of the Oyster card pre-payment system. Since Oyster Cards may be linked to banking transactions — automatically "topping up" the pre-payment card via Direct Debit whenever it drops below a useful threshold — this allows the possible tracking of an individual with a known name from their point of entry into the underground system, linking their name from their payment process to their appearances on that particular time period. Current tracking technology would allow the technical capability, at times of light traffic, to display names of passengers as they move through the London Underground system and out into the open air. This would require the deployment of higher quality, interoperable networked cameras in place of the current static systems. However, this kind of infrastructure development is a current topic of discussion by senior police figures and the Home Office [Bal06a]. Significant research efforts are being undertaken at various UK universities and other commercial and academic sites worldwide, to improve automated tracking facilities to allow tracking with fewer cameras, and in more crowded scenes. Re-establishment of "lost traces" according to a variety of statistical methods, is also being investigated.

Let us solely consider current technology for the moment. It is entirely possible with current technology to, with over 99% success, to capture a high resolution known-scale facial image for everyone entering a system through a gate, such as London Underground. Considering the man hours spent identifying images of the suspects sought by police in connection with the incidents on 21st July 2005 in London from a variety of sources and the use of such images in a public appeal for their identification, it is clear why the law enforcement authorities would regard such a system as useful. In other cases, such as the murder of solicitor Thomas ap Rhys Pryce shortly after his exit from a tube station in January 2006 and the subsequent attempted use of his Oyster card by those later convicted with his murder, the use of such a system is also obvious.

However, in order to be useful, such a system must capture an image of the vast majority of people passing through most gates and retain these images for a significant length of time (days at least and probably for weeks or months). Use of biometric authentication and identification systems such as the Schipol Airport Fast Track immigration system and widespread proposals to use fingerprint authentication for such trivial systems as paying for school meals demonstrate that the use of identification mechanisms is likely to rise, possibly exponentially just as the deployment of CCTV did in the UK in the 1990s.

The question of what constitutes an "identity" (along with the related questions of "identification" and "authentication") is complicated. Philosophers, and academics of many other disciplines, have struggled with the questions of identity for millennia, and there are still fundamental disagreements about its shape and boundaries. To take a simple example, Meyrowitz in [Mey85] makes a compelling argument that, prior to the advent of television in the mid twentieth century, most people had multiple identities defined by geographical and social "place": literally one was a different person "at work", "at home" and "at the club". These different identities were maintained by the informational segregation of these places and of the people one met in these places. Television, and other modern communication media such as radio before it and the internet after it, degraded these (never perfect) information barriers and collapsed the "sense of place" they engendered, thus levelling out separate identities and/or preventing their formation via interactivity with others. It should be noted that Meyrowitz' approach to identity is that each separate identity was formed as a collusion between the intent of the person holding the identity and the perception of those interacting with them, within the informational "place".

Much of the recent work on surveillance [Whi99, Bri98, Gal04, Lyo06] treats the data shadow as the identity under surveillance. The focus of this paper on how to regulate CCTV does not allow for a detailed discussion of this, nor of the impact on internal identity formation of the existence and visibility (to the subject and others) of the data shadow. But these are questions which should be considered as part of the background to all regulation of surveillance operations.

Data Protection legislation rightly places the issue of correctness of data high on the list list of both the responsibilities of data controllers (to ensure that data is correctly held to the best of their knowledge and ability) and the rights of data subjects (to have access to data and to have a right to have incorrect data corrected). While it is difficult to see how raw video data itself could ever be regarded as "incorrect" in this sense, any interpretation of the data could be incorrect, from the lowest level of tracking — interpreting a sequence of images as all showing a single individual, e.g. sharing identity between an image showing a face and a later image in the sequence showing the "owner" of that face committing a criminal act — to the higher levels of automatic or manual interpretation of an image or sequence of images — e.g. the interpretation of a sequence of images as showing an assault, theft or more nebulous criminal activity such as terrorist reconnaissance. Since the interpretation of video surveillance is a strong trigger for law enforcement activity and criminal prosecutions, and other forms of "social sorting" [Lyo02], the collection, processing and storage of such data should be properly regulated in a coherent targetted fashion and not subject to interpretation according to the analogies with written documentation, as caused by the Durant v FSA judgement.

4 Limiting the Operators

The Durant v FSA decision, and the Information Commissioner's interpretation of it with respect to the status of raw video data as *Personal Data* or not (mostly not it would seem) would seem to have significantly reduced the authority of the regulators in ensuring that CCTV installations are not abused. It has always been one of the difficulties of surveillance to know when one is being watched in order to exert one's rights under Data Protection and Surveillance regulations. Now that the vast majority of CCTV-derived data does not constitute *Personal Data*, this situation is exacerbated. All any operator has to do when faced with a Data Protection request is to claim that none of the data they hold is classed as *Personal Data*. The difficulty of proving otherwise leaves both citizen and regulator greatly weakened with respect to even mildly unscrupulous operators.

Thus, in proposing an act to provide a proper regulatory framework for CCTV, the following elements of control of deployment of CCTV system operators should be included:

Expectation of Privacy from CCTV Recording in Private Places. When one legitimately visits the another's home or other private property, one does not expect one's activities to be recorded. Thus, where video recording is performed on private premises it should be an offence to do so completely covertly. Exemptions for investigative journalism and similar public interest issues should be made. It should be sufficient to inform visitors that monitoring is taking place (implicit consent). Making visual records of "personal acts" such as sexual or hygiene activities should require explicit consent.

Expectation of Privacy in Semi-Private Places. As happens at present, notification that CCTV is in operation should be mandatory in semi-private areas such as offices. Covert camera placement should not be permitted and clear guidelines on the usage of these cameras should be available on request. It should be an offence to change the usage of such systems without making significant efforts to pro-actively inform those surveilled, particularly where they were aware of previous more limited usage. Retroactive changes to usage of surveillance systems (i.e. changing the intended use and applying that to already recorded sequences) should be forbidden.

Expectation of Privacy in Semi-Public Places. Deployment of CCTV systems in semi-public places such as shopping centres should be subject to further restrictions on use of trained operators, restricted access to control rooms and both live and recorded video footage. Visits to control rooms should be clearly logged and necessity and proportionality principles be maintained. The photographs of surveillance operators (including all management personnel with legitimate access to control rooms and surveillance recordings) should be available on demand to balance the scale of visibility [Dub03]

Expectation of Privacy in Public Places. Proponents of the benefits of CCTV in public places often claim that since there is no expectation of privacy in such places, that there should be no problem with recording and dissemination of surveillance footage. However, the lack of expectation of privacy only extends to the *immediate* and *reciprocal*. That is, one's presence in a public place is ephemeral and immediate. Thus knowledge of one's presence is limited to those with contemporaneous presence. Proof of that presence is also limited to the testimony of those others present. Similarly those others present who might gain knowledge of one's presence and activities are subject to a reciprocal knowledge by the observed. Live CCTV monitoring is not subject to the reciprocity rule, and recording of the scene denies the immediate

ephemeral nature of presence, creating a significant element of a data shadow. As the abilities to track and interpret these data shadows increases, so will the invasion of privacy that CCTV surveillance entails. Linking of these data shadows to other routes of identification removes the "anonymity of the crowd" that is part and parcel of the expectation of privacy in public places [Fro00]. Thus only public authorities should be permitted to operate surveillance of public places.

Boundaries. Obviously, there are boundary areas between each of these classes of place. The most troubling is that of boundaries with public space. Surveillance of public spaces, whether from within a building or on the outside of a building, should not be allowed by private agencies. Where appropriate physical or electronic Privacy Enhancing Technologies [PETs] (see section 6) are available and deployed to prevent "spillover" onto public spaces, deployment should be permitted subject to the maintenance and correct operation of the PETs.

4.1 Paying Peanuts, Employing Monkeys?

It is clear from the work of Goold [Gal04] and Norris and Armstrong [NA99] that the monitoring of CCTV is often regarded as a low skill job and operators are paid accordingly. Low paid staff are little motivated to pay attention to the ethics of their job. Regarding such work as requiring low skill and deserving of low pay also leads to significant staff turnover. Staff in jobs with low pay and low esteem are less likely to regard "codes of ethics" as anything other than something to which only lip-service needs to be paid (as amply demonstrated in the work of Goold [Goo04]). Given the one-sided power structure involved in remote surveillance [Lyo06], surveillance operation staff should have mandatory training requirements and registration with the OSC should be a pre-requisite for such staff. At a minimum, their terms and conditions of service and their and levels of pay and training should be approximately commensurate with that of Community Support Officers. Only where CCTV systems are used in little-trafficked areas to supplement or replace physical patrols (for example securing locked premises overnight) should these restrictions be relaxed. In such circumstances, those surveilled will either be other security personnel or those with significant authority within an organisation, or improperly present. Even in such cases, staff should be at minimum required to have undertaken minimal training in ethical restrictions on their use of surveillance technology.

5 Necessity and Proportionality Principles

The Home Office and ACPO review "CCTV strategy for crime reduction" was due for publication in December 2006, according to [Bal06a] but has yet to appear as of the time of writing (Jan 2007). In [Bal06a], Graeme Gerrard of ACPO (Association of Chief Police Officers) states that he wishes to see "proper regulation of CCTV to protect civil rights". However, he also would like to see both newly deployed systems and existing systems required to be "good enough for their recordings to be commandeered for use as police evidence" and "more compatible, that makes it easier for the police to access images". His interest in regulation seems more oriented towards making all CCTV systems useful and easily available to the police, rather than in protecting civil liberties. This pre-supposes that one of the primary purposes of CCTV should be to allow the police to access images. He also raises the issue of automated analysis of surveillance imagery.

In other discussions with UK police CCTV managers, it has been learned that future deployments of CCTV within, for example, the British Transport Police's areas will all comprise digital camera systems with network facilities to allow central access. In terms of value for money for a force as geographically spread as the BTP, which has responsibility for policing all of the UK's national rail infrastructure as well as the London Underground and (for some bureaucratic reason, various publicly owned underground car parks in London) this does indeed make sense. However, the broader the network infrastructure used to carry these images, the more vulnerable to external access this system becomes. Just as with the UK ID Card proposals and the NHS electronic patient records system, security of data on government networks seems to be something taken for granted without significant resources being spent on the security engineering.

Suggestions that privately deployed CCTV systems may be required to have a higher technological standard (which obviously opens them up to wider abuse of privacy than lower resolution systems) because they are therefore more use to the police in investigation and the CPS in prosecution, seems to be an unfunded mandate. In order to make any use of CCTV technology a company would then have to pay for it to be usable for police purposes. Whereas organisations such as banks, subject to the threat of armed robbery, might do well to heed the advice

of police as to what standard of equipment and processing is needed to ensure utility in criminal investigation, encouraging or mandating the update of existing or new systems over all would seem to be a recipe for increasing risk of privacy invasion without (once again) a significant study of the actual value this would produce in crime reduction or "clear-up".

The most worrying aspect of this is the suggestion that all new systems should be high quality, digital and networked. It is no large step to assume that the police would then press for "on-demand" access to both the live feeds and the recorded imagery for the purposes of manual and automatic tracking and analysis. However, much as the initial deployment of analogue CCTV in the UK happened with little public debate [NA99], the creation of a massive accessible network of high quality digital CCTV cameras in the UK would also present one of the biggest threats to individual privacy possible, when combined with the development of automated tracking, analysis and identification systems in projects such as REASON (www.reason-cctv.org), ISCAPS (www.iscaps.net) and AVITrack (www.cvg.rdg.ac.uk/ projects/ avitrack). The creation of such an infrastructure without clear explicit regulatory apparatus would be a grave mistake. Not only should the possible abuse by legitimate authority be considered, but also the worst case scenarios of the abuse of such systems by stalkers, crackers and general busybodies.

So, when considering both policy-level suggestions such as enforcing private CCTV systems to be higher risks to privacy, and in regulating licenses for the deployment of public and private systems, appropriate safeguards should be in place to consider the necessity and utility of the proposed systems and the potential costs not only in monetary terms to the public purse and the deployer, but in the risk to individual privacy that the system entails. Appropriate levels of security for high quality networked cameras should be required and their maintenance part of the ongoing licensing requirements. Appropriate logs of access should always be open to scrutiny by the appropriate regulatory authority.

6 Technological Privacy Enforcement?

PETs come in a number of different forms. An under-recognised form of PET is simply the limitations of basic hardware. Low resolution analogue cameras recording only one or a few frames per second are generally less of a privacy invasion than high resolution high frame rate cameras. Fixed focus/aim cameras as opposed to PTZ cameras are also usually less of a privacy risk (depending on the target of the fixed focus). Movable aim cameras (Pan/Tilt, with or without associated zoom) may have a simple PET included in their deployment by preventing their viewpoint from shifting to certain areas that would ordinarily be within the technical capabilities of the system. So, for example, a camera mount intended to allow 360 degrees of rotation in the x-plane and 90 degrees of rotation in the y-plane (thus giving in combination a hemispherical field of view) could have a physical restriction placed on the pan/tilt mechanism to disallow viewing of a particular combination of x and y coordinates, thus blocking a portion of the hemisphere from view of the camera. One of the benefits of this form of physical restriction is that it requires physical tampering with the camera mount in order to bypass it.

Where the physical field of view of a camera cannot be blocked from an invasion of privacy without removing some or all of the benefits of camera presence, it may be possible to employ partial signal distortion effects dependent either on feedback from the camera viewpoint mechanism or on interpretation of the visual image, to achieve a similar effect to physical blocking while allowing more complicated partial views. This is more usually what is referred to when computer vision experts refer to PETs.

Such processing can be performed in two places: at the camera itself, so that no signal containing the "private" information is ever transmitted from the camera; at the receiving station so that standard viewing of the surveillance footage does not contain the private information. In the second case, where the full image is transmitted from the camera, there are two further possibilities: the full image may be stored and available for later review, or only the restricted image may be stored. In addition, since the full image is being transmitted, legitimate, or illegitimate, bypassing of the privacy restrictions is possible and the full image may be captured or viewed.

The method of "elision" of the blocked area is also something which varies. The blocked area may be completely blanked (usually to a uniform colour, say black or grey, sometimes to a colour matching the overall colour of the image to avoid distracting the viewer). Attempts may be made to distinguish "depth" of image, so that someone inside a building and viewed through a window cannot be seen whereas the image of a person or vehicle passing in front of the building remains visible. Such processing is currently far from perfect and introduces both false positives and false negatives in blocking. Blocked areas may not be entirely blanked but may have the reso-

lution of that area reduced (pixelated) or randomised. Randomisation can be useful in that whole-image analysis techniques are sometimes less effected by randomisation than by other forms of elision.

Processor PET techniques, whether at-camera or remote system deployed may also be performed on detectable areas within an image. So, for example, people's faces or entire appearance might be elided, so that the presence and movements around the surveillance area of a person are visible, but not their individual appearance. Since, as amply demonstrated by studies such as those by Goold [Goo04] and by Norris and Armstrong [NA99], appearance of those surveilled is a key indicator used by operators to select targets for sustained attention, but that this is usually a severely flawed basis for such decision-making, such elision might well be highly useful in not only protecting privacy but also in improving the utility of CCTV surveillance.

We can thus form a hierarchy of constraints offered by PETs and use this hierarchy to influence the deplyment not only of CCTV systems and PETs currently available, but to allow future improvements on the protection of privacy offered by systems installed in the near future.

High Protection	Physical Constraints on field of view of cameras, with no facility for remote override of the protection.
	Smart-camera-based processing protections with no facility for remote override of the protection.
Medium Protection	Physical constraints on the field of view of cameras, with facility for remote override of the restriction, requiring authentication and a record of the time and extent of the lifting of restrictions.
	Smart-camera-based processing protections, with facility for remote override of the restriction, requiring authentication and a record of the time and extent of the lifting of restrictions.
Low Protection	Control centre-based processing protections which record the original sequence and make it and/or a live unrestricted image available, subject to authentication protocols and audit trail generation.
No protection	Control centre-based processing protections which record the original sequence and make it and/or a live unrestricted image available without access controls.

There are other elements which lie outside this linear structure, for instance smart-camera systems which allow remote access to a restricted feed but which also locally record the unrestricted feed, which record must be physically recovered from the system. There are currently a significant number of cameras in operation, such as those within most trains carriages and buses in the UK, where the sequences are captured and stored locally and only downloaded following an incident. For individual incidents such as assaults on staff or travellers or criminal damage, these systems can be quite useful despite the fact that the downloading of the images via a proprietary interface requires significant time. For major incidents such as the 7th and 21st July 2005, these restrictions were a severe problem. The exact nature of the problem and the efforts needed to overcome them are known but police sources have asked that they not be revealed.

In addition to the hierarchy above, the network infrastructure's vulnerability to intrusion must also be considered. Encrypted transmission over dedicated physical network wiring through physically secure routes is, of course, the least vulnerable, although even this is possibly open to intrusion. No system is perfectly secure. Cameras using no or weak encryption wireless transmission systems, particularly those based on the common wireless ethernet standards, are among the weakest architectures.

Of course where surveillance systems are designed to operate with public access, all concept of restricted access is removed as is any concept of privacy control. These include the many exterior view webcams connected to the web, on a permanent or temporary basis and often including significant PTZ control. Two examples are the Royal Holloway, University of London webcam showing progress on building an extension to their management school (www.rhul.ac.uk/Facilities-Management/internal/docs/maintenance/ManagementExtension.asp accessed 15.01.2007) and the permanent camera on the roof of the SECC conference centre in Glasgow (www.secc.co.uk/webcam/ accessed 15.01.2007). They also include systems such as that of Shoreditch council, which allows residents of an estate access to the cameras in their area [Bal06b], While, technically, the processing of images from these sources may constitute capture and continued processing of personal data, the opportunities to identify who is viewing and for what purpose are so limited as to make the regulation of such processing irrelevant. Such arguments form the basis of the arguments of, for example, Brin [Bri98] and McNealy [Spr99], that we have no privacy and should simply get used to the idea of living in a goldfish bowl.

7 Conclusion

Given the profusion of deployments of CCTV cameras in the UK and the profound threat to any form of anonymity of movement that expected (indeed requested [Bal06a]) further developments of CCTV infrastructure towards high resolution, colour, digital networked cameras represents, it is vital that a law specifically defining the limits of valid CCTV deployment and use is brought forward in the UK. Not only is this a necessity for the UK, but also to set a standard for the rest of the world should they follow the UK's example in widespread deployment.

Given the nature of raw CCTV footage as not sensibly falling within the useful definition of *Personal Data* itself, and in the acknowledged utility of CCTV information for law enforcement purposes (although principally in after the fact investigation rather than live policing tasks, except in certain limited deployment scenarios), the principle regulator for CCTV should be the Office of the Surveillance Commissioners, whose role and resources should be expanded to provide licensing for public space CCTV schemes, guidelines on their deployment and operation and audit of the adherence to these guidelines. The OSC should, and already does where necessary, work with the Office of the Information Commissioner [OIC], to ensure that where video data is significantly processed to the point where it definitely becomes *Personal Data*, or where it is linked to other identification information such as payment or access controls, that both data protection principles and new *Surveillance Protection Principles* are being followed.

These *Surveillance Protection Principles* should include:

- Clear announcement of CCTV recording.
- Photographs of operators (but not names and addresses) available to those surveilled.
- Licensing of operators and all others who have access to control rooms and raw data.
- Reasonable levels of security applied to transfer of images from cameras to control rooms.
- Where possible PETs to be implemented to prevent invasion of privacy.

In addition, the status of video data in criminal evidence should be made explicit:

- Clear rules of evidence to be applied to all systems suitable for use in possible proceedings.
- Disallowance as evidence data from any camera not subject to appropriate rules.
- Clear guidelines for police in requesting access to both live data and recorded data.

Acknowledgements

This work was supported by the European Commission under contract SEC4-PR-013800 (ISCAPS) and EPSRC under grant EP/C533402/1.

References

[Bal06a] M. Ballard. Home Office to grab for more CCTV power. www.theregister.co.uk/2006/11/22/cctv_powers/ accessed 11.01.2007, Nov 2006.

[Bal06b] M. Ballard. Privacy guardian to examine Shoreditch CCTV scheme. www.theregister.co.uk/2006/01/17/ic_eyes_shoreditch_cctv/ access 15.01.2007, Jan 2006.

[Bri98] D. Brin. *The Transparent Society*. Perseus, Jackson, TN, 1998.

[Dub03] L. Dubbeld. Observing bodies. camera surveillance and the significance of the body. *Ethics and Information Technology*, 5(3):151–162, September 2003.

[Fro00] A. M. Froomkin. The death of privacy? *Stanford Law Review*, 52(5):1461–1543, May 2000.

[Gal04] C. Gallagher. CCTV and Human Rights: the Fish and the Bicycle? An Examination of *Peck V. United Kingdom* (2003) 36 E.H.R.R. 41. *Surveillance and Society*, 2(2/3):270–292, 2004.

[Goo04] B. J. Goold. *CCTV and Policing*. Oxford University Press, 2004.

[Lyo02] D. Lyon, editor. *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge, Oxford, 2002.

[Lyo06] D. Lyon, editor. *Theorizing Surveillance: The Panopticon and Beyond*. Willan, Cullompton, Devon, UK, 2006.

[Mey85] J. Meyrowitz. *No Sense of Place*. Oxford University Press, 1985.

[NA99] C. Norris and G Armstrong. *The Maximum Surveillance Society: The Rise of CCTV*. Berg, Oxford, 1999.

[Spr99] P. Sprenger. Sun on Privacy: 'Get Over It'. www.wired.com/news/politics/0,1283,17538,00.html accessed 15.01.2007, Jan 1999.

[UK 05] UK Information Commissioner. Obligations towards CCTV Systems. www.ico.gov.uk/Home/for_organisations/topic_specific_guides/cctv.aspx accessed 11.01.2007, 2005.

[Whi99] R. Whitaker. *The End of Privacy*. The New Press, New York, 1999.