Towards a Framework of Contextual Integrity: Legality, trust and compliance of CCTV system signage

Mark Lizar and Gary R. Potter

Introduction

The United Kingdom has long been recognised in camera surveillance research as having the most prolific use of CCTV video surveillance[i] systems in the world (Armitage 2002, McCahill & Norris 2002, House of Lords 2009). McCahill and Norris in 2002 estimated that in the UK there were over 4.2 million CCTV cameras, one for every 14 citizens. The UK CCTV industry grew between 4 and 7% Compound Annual Growth Rate (CAGR) between 2002 and 2009 (Hayfield, 2009). These figures indicate a higher camera-to-citizen ratio than any other nation (Carroll-Mayer *et al*. 2008).

According to forecasts, the world is in a hurry to catch up with the UK as "The global CCTV market is projected to reach around US$ 28 Billion by the end of 2013, at a CAGR of over 22% from 2010" (RNCOS, 2010). In light of the global growth of camera surveillance, the UK, as a world leader in the use of CCTV technology, is a critical country to study.

This high level of CCTV use is presumably due, at least in part, to the British public's acceptance of CCTV systems as a safety and security measure (c.f. Cole, 2004). For law enforcement, video surveillance has become something of a panacea. Video surveillance is seen as a cost-effective crime fighting strategy (Deisman, 2003). It has been embraced for its potential in the prevention and detection of crimes, and the

identification and prosecution of offenders. In the early days of CCTV, and in much recent debate, its role in combating terrorism also has been trumpeted[ii], although CCTV is more commonly employed for the purposes of combating low-level crime and anti-social behaviour, or for control of particular places and the crowds that frequent them. CCTV, it is claimed, facilitates development of a safer environment, improves police response times, reduces fear, raises property values, lowers insurance premiums, enhances visitor experience, and increases workplace efficiency, amongst other benefits (Deisman, 2003). Whether these claims are valid or not, it is clear that CCTV has great appeal politically, publicly and commercially.

Despite this long list of benefits, video surveillance technology is also subject to much criticism. Many claimed advantages, particularly those related to crime prevention and law enforcement, are far from clearly supported by research (see Gill and Spriggs, 2005, for a detailed review of the impact of CCTV on crime). More generally, concerns relate to the privacy of those monitored and recorded by camera surveillance and the control of personal data (images) generated by cameras (Rotenburg, 2008). In short, there are questions as to whether the public can 'trust' CCTV. Concerns over the misuse of camera surveillance and the data it generates are reflected to some degree in specific laws governing CCTV system use and in general data-protection and human rights legislation (see Johnson, this volume). A fundamental element of this legal framework, and a central focus of this chapter, is the legal requirement (in the UK) for organizations to give appropriate notification to the public that CCTV camera surveillance is in operation.

Notification, here, is best understood as the display of signs indicating CCTV system presence to those subject to surveillance. Notification can be understood as a way to

elicit informed consent from subjects under surveillance. The fact an individual remains in a location after being informed through signage that it is under surveillance implies the subject consents to be monitored[iii]. Even without this somewhat legalistic concept of informed consent, notification can be seen as a way for members of the public to evaluate the appropriateness and trustworthiness of public surveillance (Lippert, 2007). In this way notification can be seen not only as a key component of compliance in the UK, but also, regardless of jurisdiction, as a key component in CCTV effectiveness and in building public trust in a given CCTV system. Another (but by no means contradictory) perspective on notification in the form of signage is that signs serve the purpose of increasing the effectiveness of surveillance through (re-)emphasising both camera presence and purpose (Cole 2004, Lippert 2009b). One particular and peculiar outcome of this perspective is the existence, at times, of signs *without* cameras aimed at influencing behaviour (Lippert, 2009b), another is the observation that signage that falls short of legal standards may be more effective in deterring criminal behaviour than that which is legally compliant (Cole, 2004, Lippert 2009b). We begin to see here how signage takes on an importance beyond its role of accompanying and legitimizing an active camera surveillance system.

Legality, trust and compliance

Existing regulation for the operation of CCTV in the United Kingdom is found in two pieces of legislation from 1998: the Data Protection Act (DPA) and the Human Rights Act (HRA). The DPA stipulates that a person (data subject) must be notified (1) that personal information is being taken; (2) why that information is being recorded; and

(3) to whom this information will be accessible. In the CCTV context this means persons must be informed *when* recording is taking place, *why* that recording is happening, and *who* will control the personal data once recorded. The DPA is in effect an extension of well-established privacy frameworks that can be traced back, in modern times, to the 1948 UN Declaration of Human Rights. Instruments stemming from the UN Declaration include the 1973 American 'Fair Information Practices' which have left a lasting legacy "as one powerful mechanism for levelling the playing field in a game where participants have unequal starting positions" (Nissenbaum, 2004:110). These are practices designed to balance the power equation in the access, use and control of information and are relevant to the proportional use of public surveillance. The Organization of Economic Co-operation and Development (OECD) included these fair information practices in 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (OECD, 1980); the EU incorporated them into law via European Directive 94/95. This EU directive was pivotal to enacting privacy legislation across all European member states (Bennett, 1992).

The reasons that such entrenched legal frameworks have evolved and are applied to the use of video surveillance relate to the privacy and security risks presented by the use of public surveillance technology to the persons and communities this technology monitors. The very nature of video surveillance creates a significant power imbalance (House of Lords, 2009) because the individual cannot see the watcher and may be unaware of who is watching, what they are watching for, and how the data is being recorded, stored and used. They may, of course, not even know they are being watched and recorded in the first place. At the same time camera operators are anonymous and are in a position of power, accentuated by the fact that no one may be

monitoring their use of this technology (Rotenburg, 2008), thus making the subject of surveillance more vulnerable.

It is clear that UK law goes some way to addressing the privacy and trust concerns related to CCTV system uses. However, it should also be clear that the mere existence of relevant laws will not satisfy all these concerns, and that the legality of a system does not necessarily equate to its trustworthiness. The law, for example, allows camera surveillance use by anyone. This may be a concern in itself: video surveillance by official bodies may be more acceptable to some persons than CCTV use by private companies or individuals (Eurobarometer 2008). For others the existence of *any* video surveillance may be deemed intrusive and unacceptable.

The issues of power imbalance are exacerbated by advances in profiling through the development and use of identity management in conjunction with video surveillance technology. The term CCTV – *closed circuit* television – is often no longer adequate to describe the changing nature of video surveillance in contemporary society (Lippert, 2009a). This is due, in part, to the rapid increase in the capacity to store, manipulate, analyze, share and distribute an ever-increasing amount of surveillance data. These developments dramatically change the closed circuit context (*ibid.*), bringing into question whether the law will keep up with technological advances and their implications.

Regardless of whether the law's content is sufficient to counter privacy concerns, there may also be concerns as to how effectively laws are enforced and how sanctions should operate against those breaking the law. The existence of a legal framework around surveillance and data control recognises the existence of individuals' privacy concerns, but it does not end debate. Even where a legal standard minimum is applied

and effectively enforced there is much room for debate as to whether the legal standard addresses pressing concerns about privacy, and therefore whether legal compliance necessarily renders CCTV systems transparent, trustworthy, or useful.

We can illustrate the problem with reference to an empirical study. The legality of CCTV systems in the UK was considered by McCahill and Norris (2002) in a study of a London high-street (main shopping street), where it was found that only 53%[iv] of CCTV systems sampled had a sign, and only 22% of the signs that did exist were "in accordance with national laws" (*ibid*. p.22). With little over one in ten CCTV systems therefore complying with basic legal requirements under the DPA it is clear that the mere existence of a law is not enough to ensure even minimum standards of data protection and respect for the right to privacy[v]. Lippert (2007, 2009a, 2009b) makes a similar observation about CCTV and accompanying signage in Canada: notification as provided on signage often falls short of legal requirements. We can assume that similar problems exist in other jurisdictions.

The obvious point to make from this work is that many CCTV systems are not fulfilling their legal obligations of notification[vi]. However, observations on legality are only of limited use in discussions about privacy, data-protection or 'trust' in relation to CCTV system proliferation, particularly in a comparative context. Legal standards will vary across jurisdictions, and may change within jurisdictions. Legal standards may not match the standards that some members of society would like to see met before considering a system trustworthy. It is also apparent that simply commenting on whether individual systems are legal or not (or on the rate of legal compliance of systems within a single jurisdiction) masks some fundamental differences between systems that are clumped together in one of two binary

categories. The data cited above from McCahill and Norris (2002), for example, make it clear that some systems were illegal because their signs were not compliant with the law, whilst others did not have signs or other notification in place. Some system owners seemingly make some effort (albeit inadequately) to comply with the law; others seemingly make no effort (and may or may not even be aware of the legal requirements). We may well wish to distinguish between these levels of non-compliance or between those systems that *meet* the legal requirements (by providing the bare minimum of information) and those that *exceed* the legal requirements (by providing extra information, for example). Following this discussion we would argue it is more useful to consider 'compliance' as a scale than as a binary concept of legality, albeit a scale where there may be a cut-off point for what constitutes '*legal* compliance' in a given jurisdiction. With a compliance scale approach to assessing camera surveillance[vii] we can still comment on the legality of individual systems for specific and general purposes (such as monitoring compliance rates in different parts of the UK or at different points in time). We can compare levels of compliance and/or integrity across jurisdictions where, previously, a binary concept of legal/illegal would make such comparisons of limited utility (because of different legal requirements, if any, in different jurisdictions). We can use a scale of compliance to inform discussions where there is no legal standard, or where the legal standard is called into question; as an objective benchmark where standards applied for measuring compliance can vary. What is more a compliance-scale can be applied not only to camera surveillance, but to all scenarios where data is collected and potentially shared.

Aims

Keeping the above discussion in mind, the aims of this chapter are twofold. On the surface level we report on some original research into the extent and legality of CCTV systems on a busy high-street in London. The methodology and findings are broadly comparable to those of an early study of CCTV conducted on a similar London high street in 2002 (McCahill and Norris, 2002). The findings serve as an interesting study in the legality of CCTV systems in their own right; comparison to this earlier work adds a dimension to the analysis.

The essay, however, also has a deeper aim. The methodology and findings discussed, and the comparison with earlier research, demonstrate the value of a compliance-scale approach to surveillance research. We hope to illustrate a number of ways in which a compliance-scale approach to 'privacy' and 'information sharing' research can contribute to broader academic debates. Finally, we aim to suggest a number of directions for future research.

Methodology

The research reported here consisted of an audit of CCTV systems on a single high-street in central London. A central aim was to produce data on CCTV systems that would allow comparison with the earlier research of McCahill and Norris (2002) and a broadly similar methodology was therefore employed.

McCahill and Norris were attempting to provide a snapshot of CCTV coverage in the City of London as part of the European Commission funded Urban-Eye project reporting on the extent of CCTV use across a number of European countries[viii]. They

used a range of different methods targeting different sample populations of 'institutions' across London culminating in descriptions of CCTV usage on London's public transportation systems, in sports stadiums, at cultural/tourist attractions, and by criminal justice system agencies. They also researched CCTV usage in the London borough of Wandsworth as an indicator of the scope and extent of public surveillance by CCTV systems in shopping and business districts (McCahill and Norris, 2002). One element of the Wandsworth research was a survey of businesses around the main business area ('Putney High Street' and their use of CCTV, including details of signage use and content; it is this particular aspect of their research that we sought to emulate.

Our own research was conducted on King Street in the London borough of Hammersmith and Fulham, a London high-street comparable to Putney High Street based on the number and type of businesses. We conducted an audit covering type of business, whether or not it used CCTV and, if so, details of accompanying signage. The audit was completed through researchers' observations, supplemented, where possible, with face-to-face questioning of institutional staff and, in some cases, photographs of cameras and signs. The initial assumption, or hypothesis, was that the level of use of CCTV by businesses would be greater than that found in 2002, reflecting a general increase in CCTV use.

The research was conducted over separate field-trips to King Street. The first of these served as a pilot study: a 20 item survey was tested, the number of institutions and broad extent of CCTV use on the street was assessed, and potential accessibility problems were highlighted. During the pilot visit a number of photographs of CCTV

cameras and/or their accompanying signage were taken as data relating to the range of potential legal and privacy issues with which the final audit might need to deal.

The second visit was the main research event. The number of items in the audit was scaled down to cover whether or not the business/institution[ix] had CCTV, whether a sign was present, and sign[x] content. Space was also included in the survey for the fieldworker to record anything suspicious, unusual or otherwise interesting in relation to an individual CCTV system. This allowed us to assemble some detailed case studies of problematic use of CCTV and related signage, illustrating how the law is breached and many grey-areas where legality is unclear. Finally, details of the type and size of each institution were recorded. In total, data from 140 premises along with eight open street cameras and one unknown camera system[xi] were collected.

It is interesting to note that there was a mixed reception from those business owners and employees encountered during this study. Researchers were met in some cases with very friendly attitudes, but in others by very unreceptive manners. The field-worker was at one point surrounded by bank managers and asked that photographs taken be deleted, a request we complied with. Interestingly enough, however, there are no laws or signs about taking photgraphs inside a store, and there is therefore a certain irony around the concerns some CCTV system operators had about surveillance directed at their own surveillance systems!

Findings

One aim of this research was to assess the extent and legality of CCTV usage in King Street and compare it to the situation in Putney High Street, as recorded by McCahill and Norris in 2002.

The Putney High Street sample consisted of 212 premises, compared to 140[xii] in the King Street sample. In our study 77% (108) of the premises had a known CCTV system in operation, nearly twice as high as the 40% reported in the earlier study. 59% of the King Street premises with CCTV systems had signs indicating CCTV presence, a slightly higher rate than the 53% reported in earlier work.

In the earlier sample only 22% of CCTV signs were 'in accordance with national laws' (McCahill and Norris, 2002: 22). It seems that for the purposes of this earlier study the signs were deemed legally compliant if there was both contact information and 'purpose' provided. In our own research 17% of signs were in accordance with the law in that both contact information and purpose of surveillance were shown on the sign. This means that only about10% of CCTV systems were legal in the sense of having a sign that included required details, a rate similar to that found in the earlier research (see Table 1), while nearly 90% of CCTV systems in both studies were found to be illegal.

Table 1: Comparison of key findings

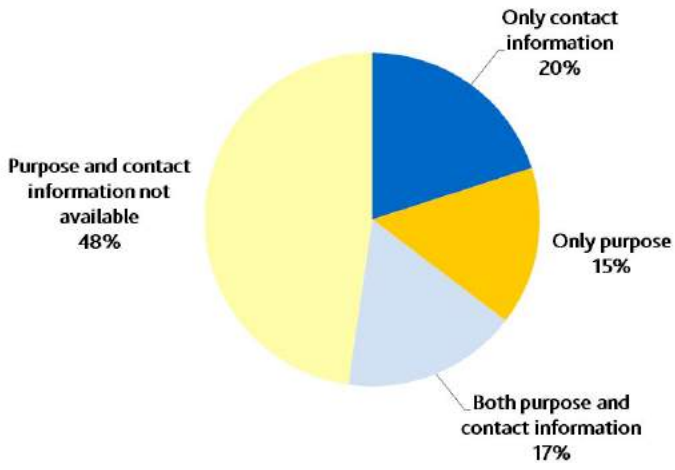
	King St. (2009)	Putney High St. (2002)
% of businesses operating CCTV	77%	40%
% of businesses with CCTV displaying signage	59%	53%
% of signs that meet legal notification requirements	17%	22%

% of CCTV systems with legally compliant signage	10%	12%

Within our sample it was possible to discern which legal requirements signage lacked (figure 1). For those systems with signs, 24 (37%) displayed contact details and 21 (32%) stated the purpose of surveillance. Only 11 systems (17% of those with signs) displayed *both* contact details and purpose.

Figure 1: Availability of Contact and Purpose Information

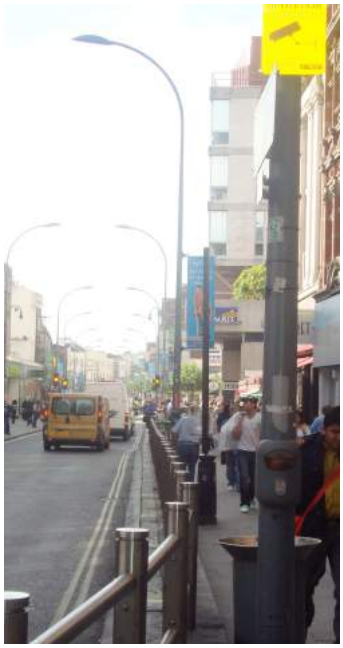
(% of locations with sign)



It was also possible, with our data, to look beyond these basic legal requirements and consider some other legal and non-legal[xiii] elements of notification that may contribute to the trustworthiness of the information sharing that occurs with CCTV systems. For example, of the 11 signs that met all legal requirements, only 2 (18% of

legal signs, or 3% of all CCTV systems) displayed information relating to a code-of-conduct for the system's operation[xiv].

Further examining the concept of *legal* compliance, the criteria we (and McCahill and Norris before us) have employed for assessing 'legality' may not be sufficient to distinguish all compliant and non-compliant systems. One useful aspect to consider here is signage positioning. In the case of CCTV operating in a particular business, it is argued (Lippert 2009a) there needs to be a sign warning persons they are being recorded at the entrance or prior to entering a surveilled area. This is important because without such a sign persons would be unaware of the presence of camera surveillance and therefore have no opportunity to consent. The data subject would also have no information about contacting the data controller or accessing the collected data. In a similar fashion we encountered signs connected to the open-street system in King Street that were three meters off the ground and therefore very difficult to read.



Pic. 1 – Open-street CCTV and traffic sign difficult to read from vehicle or pedestrian sidewalk.

These open-street CCTV signs indicated a purpose and identified who was operating the system, but the diminutive text was difficult to see. It is doubtful these signs are readable by vehicle drivers or pedestrians who would be subject to surveillance, and therefore whether the legal duty of notification has been successfully discharged. It is possible to identify other examples where, presence and content of signage aside, contextual issues (such as those relating to the purpose or positioning of the cameras or signs) throw the legality of the system into doubt and undermine the level of trust the system earns. Examples include a camera in a pub positioned inside the men's rest-room and a council-run open-street camera pointed straight into a block of apartments.

Pic. 2 – CCTV cameras inside men's washroom over urinals

Pic. 3 – CCTV camera focused into private residence

Discussion

Comparing our research with the previous study conducted by McCahill and Norris (2002) there is a limit to the meaningful conclusions that can be drawn. The two samples are snap-shots of two broadly similar, but separate, London locations. Differences (or similarities) may be due to contextual factors (such as local geographic or social conditions), or may reflect changes over the years, or because one or both samples is atypical. Nevertheless the level of CCTV usage by businesses was higher in our study. This is further empirical evidence of a recognised trend that CCTV use in the UK is increasing[xv].

It is also interesting to note the levels of legal compliance of signage found in the two studies. Both report that fewer than 60% of premises with CCTV had any form of CCTV signage. Over 40% of CCTV-using businesses in both research efforts are seemingly not even attempting to comply with the law. Of those premises in each sample with CCTV signage, about four-fifths failed to meet the legal requirements of providing both a reason why surveillance was taking place and the necessary details to identify and contact the data controller. Nearly 90% of CCTV systems in each sample are illegal[xvi], which is, in itself, a troubling finding and a major conclusion of this study.

In considering criteria with which systems fail to legally comply and aspects of signage that can be taken as over-compliance, we can apply a more useful analytical framework to the criteria of notification. It is possible, for example, to consider a scale of compliance rather than a simple binary indicator of system legality.

'Scale of Compliance'

On one level we can see the scale of compliance as a four-point scale. We can talk about (completely) **non-compliant** systems, **partially compliant** systems, **compliant** systems, and **over-compliant** systems. On another level we can see a more nuanced scale where two of these categories represent ranges rather than points on a scale. The category of partially compliant systems, for example, can be further sub-divided to reflect how many (and which) legal criteria systems lack. In our analysis so far this has included three factors: the presence of signage; whether a sign includes the purpose of surveillance and; whether contact information is provided. Factors such as the positioning of signs or cameras, or the size of signage text could also be factored into the scale. Similarly, 'over-compliance' may also be further divisible[xvii].

One particular example of over-compliance that we did encounter concerned two instances of signs warning of CCTV systems that were not actually present. These examples illustrate how signs themselves can serve a purpose in, for example, deterring crime or otherwise replicating the effects of camera surveillance without a corresponding camera surveillance system (see Lippert, 2009b).

In addition to a scale of compliance, a scale of the context of the (CCTV using) business can also be measured to provide greater insight than through a binary measure of surveillance usage. What has been striking throughout the research conducted here was how a small business with one camera and no recording equipment is treated the same as a large multinational business with high tech equipment and large databases of aggregated data. Future research could be used to further explore these ideas of compliance within this context; a scale that differentiates a small business from a large business with national or even global

reach. The level of compliance can then be examined in relation to the business context, the two scales together (compliance and context) providing a measure of the contextual integrity or trustworthiness of the surveillance. Further research into contextual attributes across jurisdictional boundaries will enable comparative research into the use and effectiveness of regulation.

On a methodological note, more rigorous methods could be applied, for example, cross checking with surveys distributed to premises owners or managers, Freedom of Information requests, or the use of multiple observers. More importantly, it would be easy to record more variables than we covered in the research, covering both further criteria for legal compliance and indications of size or reach of the business. For example, the positioning of signs and the positioning of cameras, as discussed above, could be added to the compliance scale. As such this research seeks to extend earlier research by proposing a methodology relevant to and comparable across all contexts and jurisdictions. This is important given the rapid global growth of camera surveillance. With the correct methodological approach, a contextual scale can be created that covers all factors relevant to legal compliance and all factors relevant to contextual integrity, we can compare not only legality (including degrees of compliance and what factors illegal or non-compliant systems lack), we can also compare the contextual integrity of a CCTV system.

Conclusions: towards a framework of contextual integrity

What constitutes legality in relation to public CCTV systems and accompanying notification varies between jurisdictions. Within a given jurisdiction what constitutes legality can also, of course, change over time. Often it may not be clear what the legal

standard is, particularly when technology relating to data collection and control evolves more quickly than the laws designed to regulate data and protect privacy (Nissenbaum, 2004). This can make direct comparisons on legality difficult and/or meaningless.

Even when legal requirements are met we do not necessarily learn much about standards of notification. In one jurisdiction systems may be legal because legal requirements are minimal or non-existent. In another, a system may be deemed illegal because it falls down on one requirement amongst many, even though it meets the rest. It is clear that from an objective point of view a system that is illegal because it fails to provide one minor piece of information is better, in terms of what we have here called 'trustworthiness', than a system deemed legal because of minimal legal requirements. Comparisons of legality may well be meaningless when what we are really interested in is the trustworthiness of a system. A methodological approach such as a scale of compliance and a framework of contextual integrity provides methods to evaluate trustworthiness, not only in specific contexts but also for comparison across jurisdictions.

The practices of open-street and business surveillance, which include the monitoring of individuals in public through a variety of media (e.g., video, data monitoring, and online tracking), are among the least understood and controversial challenges to privacy and autonomy in an age of information technologies. Research and discussion as to whether or not a legal framework actually reflects the trust concerns surrounding surveillance (not only CCTV systems) are not new. Nissenbaum (2004) extends earlier work on the problem of privacy between public spheres to explain why some of the prominent theoretical approaches to privacy, which were developed over

time to meet traditional privacy challenges, yield unsatisfactory conclusions about what is trustworthy in the case of public surveillance.

Ultimately, this research reveals the need for a methodological approach suited to discussions framed around legality, trustworthiness, and overall transparency and that is amenable to comparative and context-specific research. Further research directed at applying and updating these methodologies would be required to understand whether scales of compliance and contextual integrity would address the controversial issues represented by illegal CCTV signage (and in other data-protection and privacy situations). Additional research into applying this methodology to context-specific discussions of compliance and non-context-specific (e.g. comparative) discussions of contextual integrity combined provide a better indication of 'trustworthiness'. In this way they can be used to extend this research to address issues in data monitoring generally[xviii].

References:

Armitage, R. (2002) *To CCTV or Not to CCTV? – A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime*. Nacro Community Safety Practice Briefing. London: Nacro.

Bennett, C. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell: Cornell Universtiy Press.

Carroll-Mayer *et al*.(2008) *CCTV Identity Management and Implications for Criminal Justice: some considerations,* Surveillance & Society
5(1): 33-50 , http://www.surveillance-and-society.org

Cisco (2010) *Cisco Visual Networking Index: Forecast and Methodology, 2009-2014*. [Online] Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

Deisman, W. (2003) *CCTV: Literature Review and Bibliography*, Royal Canadian Mounted Police. Available at: http://dsp-psd.pwgsc.g.ca/Collection/js62-108-2003E.pdf. (Accessed 11/11/2009)

Eurobarometer, (2008). *Data Protection in the European Union* T. G. Organization,European Commission, DG Communication - Public Opinion Analysis Sector. **225:** 137.

Gill, M. and A. Spriggs (2005) *Assessing the Impact of CCTV,* Home Office Research Study 292. Available at: http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf. (Accessed 11/11/2009)

Gras, M. (2004) 'Legal Regulation of CCTV in Europe', Surveillance and Society 2(2/3): 216–29.

Hayfield, A. (2009) *The EMEA Market for CCTV and Video Surveillance Equipment - 2009 Edition*, email from IMS Research. Sent 29/10/2009.

House of Lords (2009). *Surveillance: Citizens and the State*. *Constitution Committee Publications Constitution Committee - Second Report*. HMSO, London

Lippert R (2007) "Open-Street CCTV Canadian Style" *Criminal Justice Matters* 68(1): 31-32

Lippert, R. (2009a) "Camera Surveillance, Privacy Regulation, and 'Informed Consent', in SCAN *A Report on Camera Surveillance in Canada Part One* Canada: SCAN. Available at: http://www.surveillanceproject.org/files/SCAN_Report_Phase1_Final_Jan_30_2009.pdf. Accessed 30/12/2009

Lippert, R (2009b) "Signs of the Surveillant Assemblage: Privacy Regulation, Urban CCTV, and Governmentality" *Social & Legal Studies* 18: 505 DOI: 10.1177/0964663909345096

McCahill, M. and Norris, C. (2002). *Working Paper No. 6 CCTV in London: Urban Eye working paper series*, Hull: Centre for Criminology and Criminal Justice, University of Hull. Available at: http://www.urbaneye.net/results/ue_wp6.pdf. Accessed 30/12/2009

Nissenbaum, H., (2004). *Privacy As Contextual Integrity* Washington Law Review 79:xxx pp. 101-139. Online version at: http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf, Accessed 30/12/2009.

Organisation for Economic Co-Operation and Development. (1980) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at: http://www.oecd.org/document/53/0,3343,en_2649_34255_15589524_1_1_1_1,00.html Accessed 11/12/09

RNCOS, (2010) "Global CCTV Market Analysis: 2008-20012" http://www.rncos.com/Market-Analysis-Reports/Global-CCTV-Market-Analysis-2008-2012-IM134.htm [last accessed July 5, 2010]

Rotenburg, M., (2008) *Comments of The Electronic Privacy Information Centre To Department of Homeland Security on Docket No. DHS-2007-0076,* [Internet] http://epic.org/privacy/surveillance/epic_cctv_011508.pdf Accessed11/12/09

SCAN, (2009) *Surveillance Camera Awareness Network (SCAN)* Available online at: http://www.surveillanceproject.org/files/SCAN_Report_Phase1_Final_Jan_30_2009.pdf. Accessed 30/12/09.

---

[i] Strictly speaking, CCTV is only one form of camera surveillance. The term CCTV is commonly used in the UK and in the literature; the term camera surveillance is used elsewhere in this book. We use the two terms somewhat interchangeably to avoid monotony.

[ii] After the IRA's terrorist attack on Bishopsgate in central London, a network of cameras known as the 'ring of steel' was assembled to allow the monitoring of all entrances to 'the City', London's central financial district. More recently, and especially in the wake of the July 7th 2007 bombings, CCTV has been touted for its utility in combating terror attacks associated with Islamic fundamentalism.

[iii] This, of course, assumes that the subject has seen, read and understood the sign, and that the sign provides the necessary information to meet the standard of informed consent.

[iv] All percentages cited in this chapter are rounded to the nearest whole number.

[v] This is assuming that McCahill and Norris were applying the correct legal standards in deciding whether signs in their study were "in accordance with national laws".

[vi] We will shortly report findings of more recent research that shows the situation in the UK has not improved.

[vii] It can also be applied to other types of surveillance and personal data collection.

[viii] (www.urbaneye.net)

[ix] The majority of the institutions were businesses, but there were also council operated cameras in the sample. We have used the terms institution and business interchangably from this point onwards.

[x] Initially it was hoped that technical data comparable to that recorded by McCahill and Norris would also be collected, but it was difficult to get these details than information on signage and as such we decided to focus on notification alone.

[xi] This is unknown in the sense that it could not be ascertained who owned and/or operated the CCTV.

[xii] Not including the open-street and unknown systems. It is worth noting that although the Putney sample is larger than the King Street sample, the King Street sample has less missing data.

[xiii] Legal and non-legal, that is, in the currently understood legal situation in the UK. What we consider non-legal issues here may be legal issues elsewhere; what we consider legal issues here may be non-legal issues elsewhere. Further, our interpretation of what is legal or not is based on the interpretation used by McCahill and Norris (2002) – it is possible, as discussed elsewhere, that this interpretation does not do full justice to case-law(see Johnson, this volume). All this demonstrates the utility of a method that goes beyond simple declarations of legality: the comparisons will still be useful even if the law changes.

[xiv] McCahill and Norris produce a table stating that 56% of their CCTV systems had a code-of-conduct, but there is no relevant commentary. It is not clear how this figure is arrived at – it seems likely that this figure reflects the proportion of CCTV system operators who, when asked, claimed the existence of a code of practice rather than the proportion of CCTV systems for which details of a code of practice (and how to consult it) were mentioned on the signage.

[xv] See, for example, security industry research that reported a compound annual growth rate in video surveillance sales of 4-7% between 2002 and 2009 in the UK (Hayfield, 2009).

[xvi] This assumes the provision of contact information and the reason for surveillance occurring on a sign accompanying the CCTV system are sufficient conditions to ensure legality.

[xvii] It should, of course, be noted that to be *over*-compliant all legal criteria must be met as a minimum requirement – provision of information or consideration that is not legally required does not off-set the failure to provide information that is legally required.

[xviii] For example, the same issues observed with illegal CCTV signage are apparent with the online tracking and use of internet protocol (IP) addresses, website cookites, and behaviour targeting. Where Terms Of Service Agreements and End User Licence Agreements take the place of CCTV signage.