NOTES / AANTEKENINGE

REGULATION OF THE USE OF CCTV AS A CRIME PREVENTION TECHNIQUE*

1 Introduction

Having been used for a number of years as part of the security apparatus of banks and stores, closed circuit television (CCTV) is increasingly becoming more prevalent on the streets of South Africa. CCTV monitoring takes place in a number of cities, including Johannesburg, Durban, Cape Town, Port Elizabeth and Pietermaritzburg. (My own interest in this matter derives from my involvement in the Justice Monitoring Project (JUMP), the brainchild of Prof Michael Cowling, which tasked students in 2004 to *inter alia* monitor the use of CCTV evidence obtained from the camera network which is run as a joint venture of the South African Police Service (SAPS) and Business Against Crime in Pietermaritzburg.) Whilst it has been argued that CCTV cameras can make a meaningful contribution to enhancing the safety of our city streets, the question arises: at what cost? This paper seeks to examine this question in the context of a discussion of the use of CCTV as a law enforcement technique. The focus of the note will be on data collection rather than data collation, and the issue of admissibility of video evidence will not be dealt with.

CCTV may be briefly described as a television system wherein signals are not publicly distributed and images are not broadcast. Instead, such images are transmitted from cameras to particular monitors serving a limited area (as Luk "Identifying Terrorists: Privacy Rights in the United States and United Kingdom" (2002) 25 *Hastings International and Comparative Law Review* 223 225 fn 9 points out, a CCTV system can be as simple as a single camera, a monitor and a recorder). In the context of cameras located within a city, the images transmitted are primarily of pedestrians walking or transacting on the streets. As Froomkin ("The Death of Privacy" (2000) 52 *Stanford Law Review* 1461 1476) has noted, whilst moving about in public is not truly anonymous, one at least enjoys the idea, largely consonant with reality in a city environment, of being able to move about with anonymity. This freedom is naturally threatened by privacy-destroying technology such as CCTV.

It is evident that the use of such technology involves trying to balance the competing values of safety and privacy. As more cities make use of video

* This is a revised form of the paper presented at the Society of Law Teachers of Southern Africa Conference held in Bloemfontein from 17-20 January 2005.

surveillance, it appears as if privacy is on the losing side (Burrows "Scowl Because You're on Candid Camera: Privacy and Video Surveillance" (1997) 31 *Valparaiso University Law Review* 1079 1079). Whilst this trend is understandable given the standard contradistinction between the tangible harms inherent in security concerns as opposed to the intangible harms occasioned by infringement on privacy, whether it is justifiable is another matter altogether. Spencer ("Security vs Privacy" (2002) 79 *Denver University Law Review* 519 519-520) has raised a number of concerns about the tangible/intangible division as a framework for decision-making, namely (i) that the framework is incomplete and locks into short-term benefits and consequences rather than taking account of the long-term effects on privacy; (ii) that by embedding the decision in a concrete factual context the decision will inevitably be weighted in favour of preventing tangible harms; and (iii) that the tangible/intangible dichotomy is not as clear-cut as it may seem, since security proposals often serve intangible goals such as allaying fear, whilst privacy intrusions can have tangible consequences such as disrupting or inhibiting behaviour.

Whilst CCTV usage is on the increase in a number of countries, and especially the United States in the wake of the September 11 attacks, the UK is unique in its use of CCTV in public spaces (Newburn and Hayman *Policing, Surveillance and Social Control* 2002 155). Writing in 2002, Slobogin ("Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity" (2002) 72 *Mississippi Law Journal* 213 222) noted that

> "[t]here are now well over 800 local public video surveillance programs in operation in the United Kingdom, involving between two and three million cameras, and creating more video images per capita than any other country in the world. Between 200 000 and 400 000 of these cameras monitor public areas; many are equipped with zoom lenses that can read the wording on a cigarette packet at 100 yards and bring nighttime images up to daylight level".

All major cities and most sizeable towns have CCTV surveillance of their public spaces (Newburn and Hayman 158). In London, police say that every worker or shopper is caught on at least 300 cameras each day (Slobogin (2002) 72 *Mississippi LR* 214). The cameras have also moved beyond the city, into villages, schools, hospitals and even, in Bournemouth, a coastal path (Taylor "Closed Circuit Television: the British Experience" (1999) *Stanford Technology Law Review* 11 #1). It is said that the UK is home to 10% of all the CCTV cameras in the world, and it is anticipated that there will be some 25 million CCTV cameras in operation by 2007 – one for every two adults in the country (Geldenhuys "Closed Circuit TV – The Wide Eye of the Law" (May 2004) *Servamus* 54; for a general discussion of the use of surveillance in the light of the legal regime under the Human Rights Act of 1998, see Taylor "Policing, Privacy and Proportionality" (2003 Special Issue) *European Human Rights Law Review* 86).

2 Use of CCTV

Since CCTV was first introduced in 1956 (Burrows 31 (1997) *Valparaiso University LR* 1080), it has found widespread use in shop security, monitoring traffic violations, and as a law enforcement tool in urban centres

(Luk 25 (2002) *Hastings International and Comparative Law Review* 227). Moreover CCTV is used in the workplace to monitor employees, to deter theft and fraud, and to ensure safety. Recently there has been a proliferation of "reality TV" programmes which make use of video surveillance and CCTV footage to invade people's privacy (Luk 25 (2002) *Hastings International and Comparative Law Review* 227). The popularity of such programmes suggests that whatever the rationale, society currently has a desire to gaze and be gazed upon (Luk 25 (2002) *Hastings International and Comparative Law Review* 227). Allied to this, investigative journalism programmes such as SABC's "Special Assignment" and M-Net's "Carte Blanche" have frequently made use of hidden cameras to obtain footage of various matters. Whilst voyeurism in the narrow sense also drives many applications of video surveillance technology (Luk 25 (2002) *Hastings International and Comparative Law Review* 229), it is clear that there is both the means and the market to indulge the seemingly insatiable desire to see ordinary people living their lives (Burrows (1997) 31 *Valparaiso University LR* 1109).

For present purposes, we shall focus on the use of CCTV in the context of street crime, where it is used as a method to identify criminals and as a tool for crime prevention (Luk 25 (2002) *Hastings International and Comparative LR* 228). In terms of the language of situational crime prevention (for a full discussion of these techniques, see Clarke "Situational Crime Prevention" (1995) 19 *Crime and Justice* 91), the formal surveillance constituted by CCTV is categorized as an "opportunity-reducing technique" (Clarke (1995) *Crime and Justice* 113), which aims to reduce the opportunities for the commission of crime and to increase the possibility of crime being detected (Geldenhuys (May 2004) *Servamus* 54; and see 56 for different mechanisms for crime prevention). Given the longstanding use of CCTV in the commercial sector, it is reasonable to assume that citizens realize the possibility of being monitored in a shopping mall, in a bank, or at an ATM. However, one can confidently assert that few citizens expect the same level of scrutiny on the streets (Burrows (1997) 31 *Valparaiso University LR* 1080). In the light of this, it is appropriate to examine the benefits and drawbacks of CCTV usage.

2 1 Benefits of CCTV usage

(i) The use of CCTV has a clear benefit in respect of the identification of, and arrest of, suspects (Glanz and Nacerodien, cited in Geldenhuys (May 2004) *Servamus* 55; Burrows (1997) 31 *Valparaiso University LR* 1123), and concomitantly, in disproving false accusations of crime (Burrows (1997) 31 *Valparaiso University LR* 1124).

(ii) The video footage taken by the CCTV cameras is of assistance in the gathering of evidence (Glanz and Nacerodien, cited in Geldenhuys (May 2004) *Servamus* 55), although difficulties can arise with regard to the quality of recording, the sheer hard work involved in locating relevant images, the difficulties in identification (even with good images), and the invariable need to subject the images captured on tape to interpretation (Slobogin (2002) 72 *Mississippi LJ* 228).

(iii) Video evidence can be most useful in the speedy resolution of cases, as suspects generally plead guilty when confronted with such evidence (Glanz and Nacerodien, cited in Geldenhuys (May 2004) *Servamus* 55). As Burrows notes ((1997) 31 *Valparaiso University LR* 1124) surveillance footage can be a devastating weapon when the accused denies guilt on the stand, only to have to watch her crimes revealed on surveillance tapes.

(iv) CCTV allows for the coordination and facilitation of rapid response from a central control room (Glanz and Nacerodien cited in Geldenhuys (May 2004) *Servamus* 55). This further enables proactive policing, in that the control room personnel can identify suspicious behaviour prior to a crime actually occurring, and can further assess the type of situation which the police officials may need to deal with in advance (Glanz and Nacerodien cited in Geldenhuys (May 2004) *Servamus* 55). This benefit may be diluted by technological (camera) or human (operator) malfunction (Slobogin (2002) 72 *Mississippi LJ* 226-227).

(v) CCTV makes possible more effective utilization of police officers, freeing up police officers to patrol other areas, thus allowing for a saving on resources, as well as saving time spent gathering evidence and attending court (Burrows (1997) 31 *Valparaiso University LR* 1124; and Geldenhuys May 2004) *Servamus* 54).

(vi) The use of CCTV may further serve as a deterrent to potential perpetrators, in that the presence of cameras may have a 'chilling effect' on conduct (Froomkin (2000) 52 *Stanford LR* 1469). However, in order to have a deterrent effect, the presence of the cameras must be known to such potential perpetrators, which is not always the case (Slobogin (2002) 72 *Mississippi LJ* 228). Further, not every type of offender is deterred by the presence of cameras (Slobogin (2002) 72 *Mississippi LJ* 229). It may also occur that citizens are less careful about surveillance if they assume that the cameras will do the job (Slobogin (2002) 72 *Mississippi LJ* 229).

(vii) One of the primary benefits of CCTV use is that it is a source of comfort to law-abiding citizens (Geldenhuys (May 2004) *Servamus* 55). CCTV provides a visible security presence, thus inducing a feeling of safety (Taylor (1999) *Stanford Technology LR* #7), with concomitant economic benefits that accrue for businesses in town centres (see Newburn and Hayman 159). Thus the power of the "symbolic" message, that the spaces covered by the cameras are safer as a result of the presence of CCTV cameras (irrespective of the reality) is at least as important as any "real" effect it may have (see Newburn and Hayman 160). Moreover CCTV usage constitutes good political capital, in that it passes on the message that something is being done – which costs a lot of money, which is modern and which is "proven" – that will ensure public safety (see Newburn and Hayman 160; and Taylor (1999) *Stanford Technology LR* #21).

2 2 Drawbacks of CCTV usage

(i) One of the drawbacks identified with regard to CCTV use is that crime is simply displaced to surrounding areas which are less protected (Geldenhuys (May 2004) *Servamus* 57; Burrows (1997) 31 *Valparaiso University LR* 1127; and Slobogin (2002) 72 *Mississippi LJ* 230). Thus, the argument goes, there is no true crime reduction as a result of CCTV, and any reduction in crime achieved in one area is negated by the increase in crime in another.

(ii) There can be no complaint if CCTV prevents serious crime from being committed. However, violent crimes are very difficult offences for cameras to prevent or deter, given the fact that they frequently occur spontaneously (Slobogin (2002) 72 *Mississippi LJ* 232). It seems that many of the crimes "solved" through CCTV in England relate to very minor offences which are subject to discriminatory prosecution, such as littering, drunkenness, urinating in public and loitering (Slobogin (2002) 72 *Mississippi LJ* 247). Taylor ((1999) *Stanford Technology LR* #23) comments in this regard that shopping areas and city centres are becoming

> "increasingly purified and privatised to the extent that the limits of acceptable behaviour are being driven by the forces of consumerism. Public spaces are becoming increasingly less public".

(iii) It seems that CCTV operators may over-scrutinize certain groups, and that the choice of subject for surveillance may largely be determined by stereotypical assumptions (see the study by Norris, cited by Taylor (1999) *Stanford Technology LR* #24-30).

(iv) It has also been argued that CCTV in city centres may give rise to a reduction in tolerance, as a result of targeting difference, and managing it out (Taylor (1999) *Stanford Technology LR* #33). According to Rosen (cited in Slobogin (2002) 72 *Mississippi LJ* 248) the primary use of CCTV in the UK today is not to thwart serious crime but to "enforce social conformity". This reduction in tolerance in turn results in the nature of any conflict which then does arise being more extreme (Taylor (1999) *Stanford Technology LR* #33). The informal social controls which served to maintain public order have declined as a result of the use of CCTV in public spaces (Newburn and Hayman 158).

2 3 Does CCTV achieve its purpose?

Does CCTV monitoring work? The evaluation schemes used to assess its effectiveness, though very positive in their conclusions, have been criticised as technically inadequate (Taylor (1999) *Stanford Technology LR* #13; and Slobogin (2002) 72 *Mississippi LJ* 224). The surveys used to obtain public opinion on CCTV usage have also been criticised as misleading (Taylor (1999) *Stanford Technology LR* #17). It has been argued that in fact very few cities which have employed CCTV surveillance have experienced a drop in crime, and that the use of this technology has been deemed much too expensive given its relative lack of effect (Burrows (1997) 31 *Valparaiso*

University LR 1128; and see Slobogin (2002) 72 *Mississippi LJ* 225). Moreover, on occasion the use of the technology has proved unreliable, in that the operators have not done their jobs properly, or the wrong person has been arrested (Burrows (1997) 31 *Valparaiso University LR* 1127). This assessment may be too bleak however. There has been some significant reduction in crime recorded in certain cities (see Luk (2002) 25 *Hastings International and Comparative LR* 228; and Slobogin (2002) 72 *Mississippi LJ* 230-231, who concludes that a "fair conclusion" is that a properly run CCTV system "might be able to reduce some types of street crime, particularly theft, by 10 to 25% in 'high crime areas' in comparison with similar public areas that have no cameras"), and as Clarke points out (19 (1005) *Crime & Justice* 130) there may be an indirect diffusion of benefits (*ie* beyond the directly targeted persons, places or crimes) deriving from the use of CCTV in public. The question of the cost-effectiveness of CCTV surveillance has not been fully resolved however (see Slobogin (2002) 72 *Mississippi LJ* 231-3). Nevertheless, given the fact that CCTV is widely regarded as the new "silver bullet" (providing a "simple remedy for a difficult or intractable problem" – *American Heritage Dictionary of the English Language* 4ed (2000)) of law enforcement (see Taylor (1999) *Stanford Technology LR* #21; Slobogin (2002) 72 *Mississippi LJ* 233; and Newburn and Hayman 158), these concerns are likely to be downplayed.

3 Constitutional issues

It has been argued that CCTV usage limits a number of rights. Slobogin states that the discouragement of expressive conduct limits the right to freedom of speech ((2002) 72 *Mississippi LJ* 252); that the "stalking" of the cameras limits the right to freedom of movement in that a person may not feel free to move in a particular way, to loiter or to go where she wants to with the camera watching (Slobogin (2002) 72 *Mississippi LJ* 258); and the right to be free from searches (Slobogin (2002) 72 *Mississippi LJ* 267). It appears however that none of these limitations will result in surveillance being prohibited, although they are all strongly indicative of the need to properly regulate surveillance. Most of the discussion of the constitutional validity of CCTV use in public has been in the context of the right to privacy.

Video surveillance of innocent public activities has been criticised as an unreasonable intrusion on the privacy of the individual, since it "ignores the fundamental fact that we express private thoughts through conduct as well as through words" (Slobogin (2002) 72 *Mississippi LJ* 217). Thus to track a person from block to block without her knowledge to focus on a letter she is reading, words she may be mouthing, or an itch she may be scratching, is unreasonable (Burrows (1997) 31 *Valparaiso University LR* 1128). Writers who voice these criticisms insist that there is a right to public anonymity (Slobogin (2002) 72 *Mississippi LJ* 240 explains that such right "promotes freedom of action and an open society" and lack of such anonymity "promotes conformity and an oppressive society"), which is associated with the right to privacy, and is only surrendered when

> "one does or says something that merits government attention, which most of the time must be something suggestive of criminal activity" (Slobogin (2002) 72 *Mississippi LJ* 239; see also the broader interpretation of the right to

privacy proposed in Taslitz "The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions" (2002) 65(2) *Law and Contemporary Problems* 125ff, particularly 131).

This right is clearly limited by surveillance, which results in a chilling effect on people's behaviour for fear of their actions being misconstrued (Slobogin (2002) 72 *Mississippi LJ* 244; and Granholm "Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches" (1987) 64 *University of Detroit Law Review* 708). A further impact of the infringement of the right to public anonymity could be unsettled emotional consequences flowing from the knowledge of being watched (Slobogin (2002) 72 *Mississippi LJ* (2002) 245; and Granholm (1987) 64 *University of Detroit LR* 708).

Some writers have argued for a reasonable expectation of privacy in public (Granholm (1987) 64 *University of Detroit LR* 695), which is violated by constant video surveillance (Burrows (1997) 31 *Valparaiso University LR* 1121). It has been pointed out that CCTV surveillance is more intrusive than ordinary surveillance – the policeman on the beat is restrained in his activity by the fact that others are watching him watch them, but there are no such strictures on the operator (Welch "*Peck v United Kingdom* – Case Comment" (2003 Special Issue) *European Human Rights Law Review* 141 146; and Granholm (1987) 64 *University of Detroit LR* 698). Thus the whole process of surveillance in public can be regarded as a failure to respect the dignity and autonomy of individuals, a judgement bolstered by the fact that the fruits of the surveillance are intended to be used for purposes adverse to the interests of the person being watched (Feldman, cited by Taylor (1999) *Stanford Technology LR* #37). Consequently, it has been argued that surveillance is only appropriate in case of emergency (such as terrorist threat – see Granholm (1987) 64 *University of Detroit LR* 703) or where there is individualized suspicion concerning a person (Granholm (1987) 64 *University of Detroit LR* 700; and Taylor (1999) *Stanford Technology Law Review* #37). Even where the surveillance is of a targeted individual however, such person retains the right to ensure that the material gained is not used for unauthorized purposes (Taylor (1999) *Stanford Technology LR* #37).

It is perhaps instructive that in the only case dealing with CCTV use in public spaces so far, these arguments were not supported. In *Peck v United Kingdom* (2003 EMLR 15 (ECHR)), the European Court of Human Rights held that there had been a breach of the applicant's right to privacy in terms of article 8 of the European Convention on Human Rights. CCTV footage of the applicant's attempted suicide with a knife was released to newspapers and was published without the applicant's identity being masked. Subsequently the footage was broadcast by a television company, where although masking was used, it was held to be ineffectual. The unjustified infringement of the right to privacy was however assessed on the basis of the *publication* of the CCTV footage. The Court of Human Rights took the view that the monitoring per se of an individual's actions in a public place by CCTV camera or otherwise does not interfere with the right to respect for a person's private life.

Whilst there has been no case in South Africa dealing with the effect of CCTV surveillance in a public place on the privacy of those filmed, the Constitutional Court has stated that

> "privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly" (*Bernstein v Bester NO* 1996 2 SA 751 (CC) par 67).

However, in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* (2000 10 BCLR 1079 (CC)), the court has stated that people still maintain a right to privacy in the social capacities in which they act, and that "they still retain a right to be left alone by the State unless certain conditions are met" (par 16). Thus the question remains to be decided.

4 Regulation

Criminological writers in particular have raised the spectre of state control arising from CCTV monitoring, as foreshadowing an increasingly totalitarian state (Clarke (1995) 19 *Crime & Justice* 133). With the advent of new forms of privacy-destroying technology, some have asked whether Huxley's "brave new world" is at hand. However, it is submitted that there is no need to descend into dystopianism. Surveillance which is properly constrained and effectively targeted can simultaneously function as both a form of social control and a means of respecting rights (see Newburn and Hayman 167-8, who cite Lyon in this regard; and Luk (2002) 25 *Hastings International and Comparative LR* 224). This begs the question – what constitutes proper regulation? This matter has received some academic attention, and has resulted in the drawing up of two significant codes of practice: the American Bar Association (ABA) Standards on Technologically-Assisted Physical Surveillance (1997) (hereafter "ABA Standards"), and the CCTV Code of Practice (2000) drafted by the UK Data Protection Commissioner. In South Africa there is a draft code of conduct drawn up by SAPS, but this has not yet been finalised. A synopsis of the suggested features of regulation follows.

4 1 Decision to utilize surveillance

The decision to undertake surveillance should be taken by a politically accountable law enforcement official or government authority such that surveillance will be "reasonably likely" to achieve a legitimate law enforcement objective (ABA Standards 2-9.3(b)(i)), for which there is a demonstrable need (*eg* where there is a high, recurring rate of street crime which other law enforcement measures have failed to curtail) (Granholm (1987) 64 *University of Detroit LR* 711). Burrows further proposes that these concerns must be proved before a neutral magistrate, who would then make an order granting general surveillance ((1997) 31 *Valparaiso University LR* 1135).

4 2 Training and Accountability of Operators

All CCTV operators should be trained and certified, and equipped with "at least a minimal comprehension of the ethical, moral and fundamental privacy ramifications of video surveillance" (Burrows (1997) 31 *Valparaiso University LR* 1133; and Geldenhuys (May 2004) *Servamus* 56). Operators should be furnished with written guidelines to ensure optimal implementation. Furthermore, all operators are to be held accountable by using administrative rules and sanctions (ABA Standards 2-9.1(f)(i)). Brin has argued that the best way of ensuring accountability is by "watching the watchers" (cited in Slobogin (2002) 72 *Mississippi LJ* 307). This can occur either through a process of "auditing" the surveillance tapes to check whether there are any violations of the rules or through actual surveillance of the operators, which would not only check inappropriate behaviour but also sensitize the operators to the effect of surveillance (Brin, cited in Slobogin (2002) 72 *Mississippi LJ* 307).

4 3 Consultation

All details of the planned video surveillance should be made public, including details of where and when surveillance will take place, the goals of surveillance, and which offences might be deterred (Granholm (1987) 64 *University of Detroit LR* 711; and see 1st Data Protection Principle of CCTV Code of Practice (UK) which further requires the identity of the data controller along with the purposes for which the data are intended to be processed). Thus there should be public consultation, both prior and during the surveillance, to allow the public to express its views on the practice of surveillance and to suggest changes. As Slobogin points out, ideally, dissemination of information about properly regulated CCTV surveillance will lead to the realization amongst members of the public that most people are not targets, and any fears about improper scrutiny will be allayed ((2002) 72 *Mississippi LJ* 311). Granholm urges the need for majority support for all aspects of the surveillance and a right of the community to veto the surveillance project ((1987) 64 *University of Detroit LR* 711). This view has not found widespread support however (see Taslitz (2002) 65(2) *Law and Contemporary Problems* 183-4), and it is submitted that once the procedure set out above has been followed, the process may be implemented. The results of the surveillance should further be made available to the public (Granholm (1987) 64 *University of Detroit LR* 712).

4 4 Notice

The community should be given clear and conspicuous notice of the surveillance (Granholm (1987) 64 *University of Detroit LR* 711; and Burrows (1997) 31 *Valparaiso University LR* 1133). If the rationale of CCTV is deterrence, then it is imperative to notify those who will be subject to camera surveillance (Slobogin (2002) 72 *Mississippi LJ* 297). By giving notice, citizens who object to surveillance are able to steer clear of areas where the cameras are used (Taslitz (2002) 65(2) *Law and Contemporary Problems* 183).

4 5 Nature of Surveillance

The surveillance should be restricted to the scope necessary to achieve its objectives (Taslitz (2002) 65(2) *Law and Contemporary Problems* 185), and thus personal data should only be obtained, and information disclosed, for specified lawful purposes (ABA Standards 2-9.1 (c)(ii)(E) and (F); and 2nd Data Protection Principle in CCTV Code of Practice (UK)). Any personal information which is recorded must be accurate, and therefore the images recorded must be clear, recorded on good quality tapes, and any time or location references must be correct (4th Data Protection Principle in CCTV Code of Practice (UK)). Persons captured on camera ("data subjects") have the right to be provided with a copy of the information constituting the personal data held about them (6th Data Protection Principle in CCTV Code of Practice (UK)), unless the data are being held for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and disclosure of such data would be likely to prejudice one or both of these purposes (see the exemption to subject access rights in s 29 of the UK Data Protection Act 2000).

Cameras should be situated in such a way as to prevent them recording more information than is necessary for the purpose for which they were installed (3rd Data Protection Principle in CCTV Code of Practice (UK)), that is to avoid them filming private areas (Granholm (1987) 64 *University of Detroit LR* 712). Discriminatory surveillance, based on a targeting of certain social groups should be avoided (Slobogin (2002) 72 *Mississippi LJ* (2002) 298-9; and see also ABA Standards 2-9.1(d) (i)). Granholm further proposes a limitation on the telescopic capacity of the system so as not be able to see what a person is reading or saying, as well as a total embargo on tape recording or sound monitoring of events ((1987) 64 *University of Detroit LR* 712). In similar vein, the 6th Data Protection Principle of the CCTV Code of Practice (UK) ensconces the right to prevent processing of data likely to cause damage or distress.

No surveillance should be indefinite in nature (Granholm (1987) 64 *University of Detroit LR* 712). When the objects of the surveillance have been achieved, the surveillance should be terminated (ABA Standards 2-9.1(d)(ii); and Slobogin (2002) 72 *Mississippi LJ* 300). The aforementioned consultation with the community will allow for an opportunity to evaluate the efficacy of the CCTV monitoring on an ongoing basis.

4 6 Storage and Dissemination of Data

The principal feature of CCTV that distinguishes it from ordinary (non-technological) surveillance is the capacity to record observations (Slobogin (2002) 72 *Mississippi LJ* 301), and it is this capacity, along with the potential for the information generated in this way to be abused, which may create concern for the public. As Froomkin comments, "[o]nce created or collected, data is easily shared and hard to eradicate; the data genie does not go willingly, if ever, back into the bottle" ((2000) 52 *Stanford LR* 1469; and for a discussion of unintended consequences of CCTV usage, such as disclosure of personal information, see Spencer (2002) 79 *Denver University LR* 519ff). Thus it should be held that information should not be kept for longer than the

purpose for which it is used requires (5th Data Protection Principle of CCTV Code of Practice (UK)), that the personal data captured should not be subjected to unauthorised or unlawful processing and should be protected against damage or loss (7th Data Protection Principle of CCTV Code of Practice (UK)), and that personal data should not be made available to others by putting images on the Internet or on the data controller's website.

4 7 Sanctions for non-compliance

Burrows has argued that non-compliance with the principles regulating use of CCTV should be able to give rise to the full gamut of legal sanctions: inadmissibility of the CCTV recording ((1997) 31 *Valparaiso University LR* 1136; and Taslitz (2002) 65(2) *Law and Contemporary Problems* 185 concurs), criminal charges ((1997) 31 *Valparaiso University LR* 1137), and the possibility of a civil suit ((1997) 31 *Valparaiso University LR* 1138; Taslitz (2002) 65(2) *Law and Contemporary Problems* 185 concurs). However, as Slobogin points out, the sanction of inadmissible evidence can be circumvented, and in any event it benefits only a tiny number of people subjected to illegal surveillance ((2002) 72 *Mississippi LJ* 219), and moreover the use of a criminal sanction in these circumstances would be rather draconian (Slobogin (2002) 72 *Mississippi LJ* 309-310). Since the cost of civil suits may be prohibitive, it seems that administrative sanctions would be preferable.

5 Conclusion

The apparently successful use of CCTV in shopping malls in terms of reducing crime and anti-social behaviour has been seized on as a means of achieving similar results in city centres, in so doing sparking the regeneration of city centres. Though fashionable and having achieved a measure of success, this strategy is not without its costs to the privacy of the average citizen in the area of the camera's operation. Some writers have seen this as the creeping onset of state control, and have called for the "silent unblinking lens of the camera" to be stopped (see Burrows (1997) 31 *Valparaiso University LR* 1139). However, CCTV cannot without more be seen as a threat to the average citizen – whilst it can invade privacy and "generate a web of surveillance which far exceeds anything that is historically known", it can also "be liberating and protective" (Young, cited in Newburn and Hayman 168; Slobogin (2002) 72 *Mississippi LJ* 250-251 points out that whilst the potential effects of public surveillance "are not Orwellian in magnitude", use of such surveillance is "clearly not an unalloyed good"). It is incumbent on the law enforcement authorities to supply the regulation of CCTV that will keep this delicate balance intact.

Shannon Hoctor
University of KwaZulu-Natal, Pietermaritzburg