Chapter 14
Privacy, Surveillance and Identity

Mathias Klang

Surveillance technology

Throughout history, technology has been used to control the undesirable behaviour of others in a cost-efficient manner. Construction of walls such as Hadrian's Wall or China's Great Wall were motivated as cost-efficient defence systems. During the crusades, great castles were built to enable the defence of a territory using the minimum amount of manpower[1] and, more recently, barbed wire[2] has been used to control both persons and animals. Bentham's Panopticon was a creation aimed at the minimisation of the human costs of surveillance.[3] The costs of surveillance were transferred onto the individual and the architecture enhanced the levels of self-control among the inmates of the all-seeing prison. Taking this perspective, it is not surprising that camera technology today is being implemented and developed for use in surveillance.

This chapter looks at the merging of digital-optical systems currently being implemented to aid in the surveillance of socially undesirable behaviour. It will examine the legality of these systems and look at the level of preparation which the law has in meeting these systems currently in use. The chapter also examines the social implications of this development, which has led to the role of the camera as the unblinking, unforgiving eye in our urban environment. This will be done by looking at areas where digital technology has enabled major changes in the relationship between image and surveillance: facial recognition, pattern recognition, and number recognition.

Camera, self and image

Many societies make a strong connection between the image of a person and the soul. Primitive societies fear photography since it is believed that the camera will take with it something more than the image; it will also take part of the person or soul. In Oscar Wilde's *The Picture of Dorian Gray*, the image of Gray takes a central role. In his desire for eternal youth and beauty, Gray realises that his portrait will maintain its beauty while he himself will not: 'Why should it keep what I must lose?'[4] The permanency of the image robs Gray of his innocence and he wishes that his body be maintained while the image in the portrait decays. Wilde's tale of moral disintegration is an interesting play upon the connection between image and reality.

---

1 Runciman, S, *A History of the Crusades*, 1987, Cambridge: CUP.
2 Razac, O, *Barbed Wire*, 2002, Kneight, J (trans), London: Profile Books.
3 Foucault, M, *Discipline and Punish*, 1977, Sheridan, A (trans), Harmondsworth: Penguin.
4 Wilde, O, *The Picture of Dorian Gray*, 2003, Harmondsworth: Penguin Classics.

One of the major changes in photography was the introduction in 1888 of the Eastman Kodak 'Snap Camera'.[5] This camera 'freed' the photographer due to its revolutionary new film, which drastically shortened the time required for the camera shutter to be opened and therefore did not require a camera stand or that the photograph's subject remain motionless for a long period of time. These innovations were important steps towards the possibility of recording people's images without their consent. The portability and cheapness of the camera allowed it to develop further and become a leisure item, giving the photographer, or kodaker[6] as they were sometimes known, the ability to document and preserve images that would serve as proof that acts took place and give non-present onlookers the ability to share vicariously in the experiences of the photographer.

The dissemination and use of this technology re-interpreted our relationship between self and image. The new uses for the camera soon demanded social and legal reactions in order to curtail the ways in which this technology could and should be used. On the night of his death in 1898, two men entered his home and, without permission, photographed the body of Prince Otto von Bismarck. His heirs later sued to prevent publication of the photograph and to compel its destruction, along with all copies and the photographic plate. The court granted an injunction on the basis that the photographers should not profit from their illegal entry.[7] In 1907, the Law Regulating Copyright to Works of Portraiture and Photography[8] was enacted in Germany. This legislation granted individuals rights in their own images and created the possibility of preventing publication. In situations such as Bismarck, control is in the hands of the immediate surviving family for a period of ten years.[9]

In 1903, the New York State legislature created for the first time the right to sue for invasions of privacy after a young girl had been photographed without her knowledge and the image was used in an advertising campaign without her consent. The Rochester Folding Box Company was sued for using the image but the courts could not find that misappropriation of personality was protected by common law[10]. The court suggested that legislation needed to be enacted to protect individuals from similar occurrences, and in 1903 the New York Civil Law was amended at ss 50 and 51 to protect against individuals' images being used in commercial advertising.

---

5 See www.kodak.com.

6 Kerns, S, *The Culture of Time and Space 1880–1918*, 1983, London: Weidenfeld & Nicolson.

7 RGZ 45, Judgment of 28 December 1899, Bismarck, 170, 173, discussed in Helle, J, *Besondere Persönlichkeitsrechte im Privatrecht*, 1991.

8 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie, or 'Kunsturheberrechtsgesetz' (KunstUrhG), of 9 January 1907 (RGBl 1907, 7), last amended 2 March 1974 (BGBl I, 469).

9 KunstUrhG § 22.

10 *Roberson v Rochester Folding Box Company*, 171 NY 538 (NY CA, 1903).

The growth of camera surveillance

Surveillance cameras (closed circuit television, or CCTV) have been used since the 1950s, a period which also saw the development of the video cassette recorder, which further lowered the expense and ease with which images could be recorded and stored. At the end of the 1960s, the first commercial systems for the surveillance of retail stores appeared in the UK.[11] Since then, the use of CCTV has exploded and is continuing to grow: today, surveillance systems are gazing at us in everything from small corner stores to large banks, in transport systems from taxis to the London Underground, from lonely footpaths to crowded streets and sports arenas. They are used to prevent accidents and crime, promote security and safety, and monitor critical systems and heavy traffic. CCTV has quickly become a necessary infrastructure with which to ensure health and safety at a cost-efficient level. Along with the spread of CCTV systems there has been a growing interest in the study of their social effects, their efficiency and their advantages and disadvantages in relation to issues of privacy and public surveillance.[12]

For those who previously maintained surveillance without CCTV, the advantages seem obvious. Once the initial infrastructure has been installed, the task of monitoring no longer requires a significant physical presence; instead, a large number of cameras may be monitored by a single controller. It is, however, important to remember that the cameras are only part of the system. The images are sent to a control room, where the collective images from many cameras are viewed by controllers working long shifts in front of several monitors 24 hours a day, seven days a week. In order to be able to cope with the huge amounts of information that the cameras produce, several choices must be made by the controllers. They decide which cameras are viewed on the monitor and which individuals to watch for any suspicious activity. In highly developed systems, cameras can be used to follow suspect individuals' movements over long periods of time. In such cases, the decision to follow certain individuals is based upon the previous experiences of the controller.[13]

In a study of the effects of CCTV in the cities of Newcastle upon Tyne, Birmingham and King's Lynn, the results showed a fall in property crime (for example, break-ins, vandalism and burglaries) directly after the installation of CCTV systems.[14] This seemed to show that the cameras had a preventative effect, since the risk of being caught increased. The effect of CCTV on violent crimes was less clear. The cameras were deemed to be an important tool in police investigations following crime, rather than having a strong preventative effect.

---

11 Moran, J, 'A brief chronology of photographic and video surveillance', in Norris, C, Moran, J and Armstrong, G (eds), *Surveillance, Closed Circuit Television and Social Control*, 1998, Aldershot: Ashgate.

12 See, eg, Norris *et al, ibid*; Painter, K and Tilley, N (eds), *Surveillance of Public Space*, 1999, Crime Prevention Studies Vol 10, Criminal Justice Press, or the Urbaneye Project, at www.urbaneye.net.

13 For information on the work of controllers see, eg, Norris, C and Armstrong, G, 'CCTV and the social structuring of surveillance', in Painter and Tilley, *ibid*.

14 Brown, B, *CCTV in Town Centres*, Police Research Group Crime Detection and Prevention Series, Paper 68, 1995, London: Home Office.

In a study carried out in Airdrie, the number of reported crimes fell by 21% during the two years following the installation of CCTV systems.[15] Property crimes fell by 52%, while violent crime fell by 19%. Not all crimes statistics fell, though: drink driving and disorderly behaviour increased substantially and drug related crimes during the same period increased by more than 1,000%. Studies in Doncaster,[16] Burnley,[17] Glasgow,[18] Southwark[19] and Crawley[20] all show that reported crimes fell after the installation of CCTV. The studies suggest, however, that the effect of CCTV on crime is not permanent. Crime in all areas tended to rise again over time. Other issues investigated in these studies were whether the criminal acts were transferred to areas beyond camera control or whether the changes in crime statistics could be attributed to factors other than the installation of CCTV. The general picture that appeared was that the effects of CCTV on crime prevention may be difficult to determine but that the material gathered from these systems was seen as an invaluable asset to police investigations. These results are not limited to the UK; they have been confirmed in tests in other countries, such as Sweden[21] and Norway.[22]

While the advantage may be that CCTV allows for more monitoring in a more cost-effective manner, it has brought with it a new problem, in the form of information overload. The electronic gaze of the surveillance system does not blink or rest, but it is dependent upon the prolonged attention spans and experience of its controllers. Studies of controllers have shown that they tend to observe certain groups of individuals to a much larger extent.[23] This naturally leads to corroboration of their preconceived ideas about these groups once a crime is committed. This human connection can be seen as the weak link in the surveillance infrastructure, and intelligent surveillance software is being developed in the hope of increasing the efficiency of surveillance systems. This has led to the development of systems which have the ability to automatically sort and analyse data collected

15 Short, E and Ditton, J, *Does Closed Circuit Television Prevent Crime?*, 1996, Edinburgh: Scottish Office Central Research Unit.

16 Skinns, D, 'Crime reduction, diffusion and displacement: evaluating the effectiveness of CCTV', in Norris *et al*, *op cit* fn 11.

17 Armitage, R, Smyth, G and Pease, K, 'Burnley CCTV evaluation', in Painter and Tilley, *op cit* fn 12.

18 Ditton, J *et al*, *The Effect of Closed Circuit Television on Recorded Crime Rates and Public Concern About Crime in Glasgow*, 1999, Edinburgh: Scottish Office Central Research Unit.

19 Sarno, C, Hough, M and Bulos, M, *Developing a Picture of CCTV in Southwark Town Centre*, 1999, Final Report: Criminal Policy Research Unit, South Bank University.

20 Squires, P, *CCTV and Crime Reduction in Crawley: Follow-up Study 2000. An Independent Evaluation of the Crawley CCTV System*, 2000, Health & Social Policy Research Centre, University of Brighton.

21 Blixt, M, *Kameraövervakning i brottsförebyggande syfte*, RAPPORT 2003:11, Brottsförebyggande rådet (BRÅ).

22 Winge, S, *Politiets fjernsynsovervåking ved Oslo Sentralstasjon – en evaluering av kameraenes effekt på kriminalitet og ordensproblemer*, PHS Forskning 2001:1.

23 See, eg, Norris and Armstrong, *op cit* fn 13.

by the cameras. Below I will consider two types of biometric[24] data (facial recognition and pattern recognition) and numberplate recognition as examples of intelligent surveillance systems. Where once the operators were mediators, values are now encoded and programmed into the system.[25]

Facial recognition

During 2002, six UK cities tested facial recognition software; of these, the London Borough of Newham, Tameside in Greater Manchester and Birmingham did so publicly.[26] Facial recognition software attempts to map the landscape of the human face and reduce this landscape to a unique numerical code. The purpose of this exercise is to create a database of faces that can be stored, compared and retrieved efficiently. The numerical code is based upon the angles and measurements of the face: there are about 80 distinctive measurements, known as nodal points, which can be made of each face. Examples include distance between eyes, width of nose, eye socket depth, cheekbones, and jaw line. In order to achieve maximum efficiency, the facial recognition software should be able to function in diverse conditions, observing individuals in motion, in various lighting conditions and from different angles.

Since its commercialisation in the 1990s, the use of facial recognition software has been steadily increasing. It is interesting to note that the software has not been an overwhelming success and yet, despite the disappointing results, it is still being implemented as part of surveillance systems in many countries. The American Immigration and Naturalization Service discarded facial recognition software after unsuccessfully attempting to use it to identify people in cars at the Mexico-US border.[27] In January 2000, the police in Tampa Bay, Florida used facial recognition software at Super Bowl XXXV to check people entering the arena against a database of individuals wanted for police questioning. No warning was given to the individuals entering the stadium. According to the American Civil Liberties Union, the system did identify 19 individuals; some of these were false alarms, the rest petty criminals.[28] Within the UK, the London Borough of Newham has implemented the technology and there have been several requests for more information from other councils interested in applying the technology.

The major drawback with facial recognition software is that it is too sensitive to environmental changes. Simple changes such as lighting, clothing, headgear, weight loss or gain, alteration of facial hair and sunglasses can fool the system. The sensitivity of the system in these cases results in two types of errors, called false positives and false negatives. False positives occur when the system wrongly alerts

---

24 Van der Ploeg, I, 'Biometrics and privacy: a note on the politics of theorizing technology' (2003) 6(1) *Information, Communication, Society*, pp 85–104.

25 Lianos, M and Douglas, M, 'Dangerization and the end of deviance' (2000) 40 *Br J Crim* 261.

26 Meek, J, 'Towns secretly testing "spy" software', *The Guardian*, 13 June 2002.

27 Stanley, J and Steinhardt, B, *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida*, ACLU Special Report, January 2002.

28 ACLU, 'Q&A on Facial Recognition', at http://archive.aclu.org/issues/privacy/facial_recognition_faq.html.

that a person has been identified, ie a match has been made between the individual in front of the camera and someone stored in the database. False negatives occur when the system fails to identify an individual stored within the database as he or she appears in front of the camera. A study of facial recognition systems has found that most systems generate a high amount of errors even in so-called ideal conditions.[29]

The main arguments in support of facial recognition surveillance systems are based upon the premise of benevolent watchers preventing crime.[30] In order to be successful, though, two important conditions must be satisfied: first, those who are about to commit a crime must be entered into the database, and secondly, the system must be able to identify the individuals in the database. Although evidence suggests that current technology is not sufficiently advanced to fulfil these conditions, facial recognition surveillance systems continue to be installed.

Pattern recognition

The majority of surveillance systems are used reactively. At best, they alert the user to an act in progress which can be stopped if human reaction is swift; at worst, they statically collect evidence of an act and provide the basis for further investigation and evidence to be used when prosecuting the act. The reactive use of surveillance is also useful as a deterrent, as the systems increase the risk of a perpetrator being identified. The installation of surveillance systems for crime prevention is often heralded as a success, since installation is often followed by a decrease in crime within the field of vision of the camera.[31]

There are attempts, however, to use surveillance systems more proactively. This means not only that surveillance systems can be used to prevent acts through their deterrent effect, but that they can actually be used to attempt to determine when an act is about to take place. This information can then be used to prevent the act from occurring. The main thrust of research and development in this area has focused on security and safety in London Underground stations, where surveillance systems are being used to do more than passively record images.[32] Surveillance technology is here being used in an attempt to deal with a diverse set of problems such as overcrowding, passengers standing too close to the edge of the platform or falling onto the tracks, unattended luggage, intrusion into forbidden areas, and even unusual movements in passageways.

---

29 Blackburn, D, Bone, M and Phillips, P, *Facial Recognition Vendor Test 2000*, 2001, Evaluation Report, sponsored by DoD Counterdrug Technology Development Program Office, Defense Advanced Research Projects Agency & National Institute of Justice, at www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf.

30 Norris, C and Armstrong, G, *The Maximum Surveillance Society*, 1999, Oxford: Berg.

31 *Ibid*.

32 See, eg, Boghossian, B, *Motion-Based Image Processing Algorithms Applied to Crowd Monitoring Systems*, 2000, PhD thesis, Department of Electronic Engineering, King's College London; Fuentes, L and Velastin, A, 'Assessment of image processing techniques as a means of improving personal security in public transport', Second European Workshop on Advanced Video-based Surveillance, AVBS 2001, Kingston upon Thames, 4 September 2001.

Pattern recognition systems are based on the fact that many human activities follow predictable patterns. The actions which are of greatest interest to the observer are deviations from the pattern rather than the constant flow of ordinary behaviour. A good example is the movement of crowds within Underground stations, where the ebb and flow of commuters can be quickly recognised as a pattern of behaviour where few individuals deviate from the norm.

In order to analyse the movements of crowds and individuals within the field of vision of a surveillance camera, the first step is to eliminate non-essential information from the analysis. Non-essential data is actually that which is permanently within the field of vision, ie the background or, to put it another way, the stage upon which the actions will take place. This is done because what is important within this analysis is the movement or non-movement of non-permanent fixtures within the field of vision. After this is done, everything new within the camera's field of vision is analysed by the system. Movement is therefore seen as a 'blob' moving across a background.[33] The next stage is to enter material with which the system can compare any actions that are irregular and which may need investigation. Within public transport areas, most people move in regular, fixed patterns, and as a result the system can be programmed to compare the movements of a crowd with the actions of an individual who does not follow regular patterns of movement. Irregular patterns of movement can then be classed as being suspicious and a call to investigate can be automatically sent to security officials. Such technology is used in the area of suicide prevention: the behaviour of someone planning suicide differs from that of the commuter; they tend to 'wait for at least ten minutes on the platform, missing trains, before taking their last few tragic steps'.[34]

Pattern recognition surveillance systems are presently being tested in London Underground stations[35] and have been seen as relatively successful implementations of surveillance technology. The ability of such systems to detect unusual behaviour raises new questions. Surveillance systems are no longer passively monitoring what is being done; they are now also making assumptions about normality of behaviour, where deviation from the established norm of behaviour is seen as undesirable and questionable.

Numberplate recognition

At the beginning of the 20th century, the number of cars in the UK was on the rise and it was realised that a system of identification was necessary. The Motor Car Act 1903 required all vehicles to be registered with the authorities, and to carry numberplates.[36] The Act was passed in order that vehicles could easily be traced in

33 Fuentes, L and Velastin, A, 'People tracking in surveillance applications', Second IEEE International Workshop on Performance Evaluation on Tracking and Surveillance, PETS 2001, Kauai (Hawaii), December 2001.

34 Graham-Rowe, D, 'Warning! Strange behaviour' (1999) 164(2216) *New Scientist*, 11 December.

35 Henderson, M, 'CCTV to spot "odd" behaviour on Tube', *Times Online*, 10 July 2003.

36 The Act entered into force on 1 January 1904.

the event of an accident or contravention of the law. By 1930, numberplate numbers were running out and a new scheme was introduced, which consisted of three letters and three numbers. By the beginning of the 1960s, a further change was made, adding the year of issue or 'registration'. This information was useful for car buyers, in that they could immediately ascertain the age of a vehicle. In 2001, the numbering scheme was significantly altered, allowing for more easily recognised and remembered numbers and using the font known as Charles Wright. The standardisation of car numberplates is intended to minimise the risk of error and to maximise legibility. An additional advantage created by standardisation is that the numbers can be made machine readable. This is the first step on the way to automated numberplate recognition and to the implementation of camera surveillance in recording and tracking vehicle movements.

Within the UK, Scotland is leading the way in implementing the widespread use of Automatic Number Plate Recognition (ANPR) systems. These systems use cameras to capture registration numbers and automatically check them against various databases containing 'details of vehicles of local and national interest eg driven by persons wanted for questioning, seen in suspicious circumstances etc. Work is in hand to ensure that the most is made of what is already proving to be a useful crime fighting tool'.[37] ANPR systems are particularly useful when placed in key positions, for example on bridges, and at present the Scottish ANPR system is being expanded to cover the Forth and Tay Bridges.[38] In 2002–03, police forces in England and Wales invested £4.65 million to implement ANPR surveillance; the pilot project has been heralded as a great success, resulting in an increase in arrest rates.[39]

Another large scale implementation of ANPR can be seen in the London congestion charging zone. In 2003, London initiated its experiment into urban road pricing. The equipment involved in the congestion charge system is a network of 203 camera sites that monitor every entrance into and exit from the congestion charging zone.[40] Travel by car into the charging zone costs £5 if payment is made by 10 pm on the day of travel; an additional £5 surcharge will apply if payment is processed between 10 pm and midnight on the day of travel. Failure to pay by midnight will trigger the sending of a Penalty Charge Notice of £80 to the registered keeper or hirer of the vehicle.[41]

The growth and dissemination of ANPR systems may eventually lead to an ability to search and track any car travelling on the road network. As a result of

37 Cameron, R, *Annual Report of Her Majesty's Chief Inspector of Constabulary for Scotland 2002–2003*, laid before the Scottish Parliament by Scottish Ministers, September 2003.

38 Scottish Executive, 'Smart cameras for Forth and Tay Bridges', SEJD News Release 195/2003 (2003).

39 Police Standards Unit, *Automatic Number Plate Recognition (ANPR)*, Home Office, at www.policereform.gov.uk/psu/anprnew.html.

40 Transport for London: www.cclondon.com.

41 This is reduced to £40 if paid within 14 days and failure to pay the penalty charge within 28 days will result in the penalty being increased to £120.

successful local tests[42] of ANPR systems, the Police Standards Unit is preparing to launch a national ANPR surveillance system in 2005. With the advent of national ANPR, the area within which the individual remains unobserved shrinks substantially. Naturally, the reduction of crime is an important social value and it cannot be efficiently upheld without limitations on the individual's freedom. It is, however, important to ensure that safety measures are taken to provide for the privacy of the individual. The concept of privacy as a human right applies even to those who are guilty of crimes. The limitation of a criminal's privacy must be proportionate to the severity of the crime committed. Constant supervision should only be implemented if the crime warrants it – not because technology enables us to do so.

Law, CCTV and smart surveillance

When attempting to assess the legal effects of CCTV and the implementation of smart surveillance programs within Europe, it is important to identify the distinct legal approaches developed by individual states. Some European countries, such as Sweden and Norway, have chosen to enact specific legislation with regard to camera surveillance, while other countries, such as England and Finland, have chosen not to regulate in this manner.

The Swedish law on camera surveillance deals mainly with the rules relating to permits for the installation and use of surveillance systems in places to which the public has access.[43] Sweden has set itself apart from other countries by its attempt to control the use of surveillance systems through the implementation of a permit system. There is a clear set of rules governing situations in which CCTV systems may be implemented and how they may be used. The provisions pay a great deal of attention to the balance between the need for surveillance systems and the loss of integrity which these systems entail.

However, the existence of this legislation in no way negates the importance of the legislative instrument which applies to all European Union Member States: the Data Protection Directive.[44] In fact, whereas the Swedish law on camera surveillance applies only to surveillance in places where the public has a right of access, the rules created by implementation of the Data Protection Directive apply even to surveillance systems installed in places to which the general public has no right of access.

The UK Data Protection Act 1998 (DPA)[45] states that one of the functions of the Information Commissioner is to:

---

42 According to the Police Standards Unit, the first part of Project Laser involved nine police forces stopping 39,429 vehicles and resulted in 3,080 arrests. The second phase ran between June 2003 and June 2004: www.policereform.gov.uk/psu/anprnew.html. The system is expected to be implemented nationally in 2005.

43 Lagstiftningen om (allmän) kameraövervakning.

44 Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

45 For a more detailed discussion on the Data Protection Act, see Christie, Chapter 13 and Wong, Chapter 12.

> promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers [where] the Commissioner considers it appropriate to do so … [T]he Commissioner shall, after such consultation with trade associations, data subjects or persons representing data subjects as appears to him to be appropriate, prepare and disseminate to such persons as he considers appropriate codes of practice for guidance as to good practice.[46]

Through these powers, the Commissioner has developed a CCTV Code of Practice in which the importance of the growth of facial recognition systems is recognised and the importance of protecting the integrity of individuals is noted.[47] The principles contained within the Code include recommendations designed to maintain an acceptable level of privacy protection in the light of camera surveillance. Under the heading of Standards we find Recommendations 7–10, which are discussed below:

> 7 Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.

Recommendation 7 was created as a direct response to the Third Data Protection Principle, which states that 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'. Since surveillance systems are regularly placed in public spaces, it is important to ensure that they intrude as little as possible into the lives of individuals who are in no way connected to the purpose of the surveillance systems. If cameras are installed to prevent crimes in specific areas, then the cameras should be limited to those areas and not be used in an overly invasive manner:

> 8 If an automatic facial recognition system is used to match images captured against a database of images, then both sets of images should be clear enough to ensure an accurate match.

This Recommendation is based on the Third and Fourth Data Protection Principles. The Third Principle states: 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are obtained.' The DPA does not elucidate on the meaning of these words; however, the Principle explicitly refers to the importance of collecting no more data than is necessary for the given purpose. The task of ensuring that no more than the necessary amount of data is collected is complex in relation to CCTV surveillance. The Third Principle is closely linked to the Fourth Principle, which states that 'Personal data shall be accurate and, where necessary, kept up to date'. Data are considered to be inaccurate 'if they are incorrect or misleading as to any matter of fact'. The data controller must take all reasonable steps to ensure the accuracy of the data:

> 9 If an automatic facial recognition system is used, procedures should be set up to ensure that the match is also verified by a human operator, who will assess the match and determine what action, if any, should be taken.

---

46 DPA, s 51.

47 CCTV Code of Practice, July 2000, at www.crimereduction.gov.uk/dp98cop.doc.

This is based upon the First and Seventh Principles. The cornerstone principle of the DPA is Principle 1, which states, 'Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3, is also met'. A recurring concept in Schedule 2 is that the data processing is 'necessary'; in this situation 'necessary' is intended to ensure two features: first, that the collection of the data itself is necessary, and secondly, that the data processing should involve the minimum (necessary) amount of personal data. In terms of CCTV surveillance, this must mean that cameras should be used only when they are necessary for the prevention of crime and that in this pursuit the amount of information gathered should be kept to a minimum:

> 10 The result of the assessment by the human operator should be recorded whether or not they determine there is a match.

A great deal of the focus in the Code of Practice is on the importance of ensuring quality within automated decision-making systems; this is done to a large degree by taking into account individuals' rights and also by ensuring that the systems are checked by human operators. The involvement of human operators in the final decision-making stage is to ensure that the system remains accountable and is not arbitrarily unjust.

Individual rights

Human rights are today an integral part of political discourse; they are accepted and rarely questioned, and most states profess a belief in them despite any actions which contradict these proclaimed beliefs – in this manner they are truly hegemonic. Despite this almost universal belief in the importance of such rights, practical recognition of human rights is far from universal and uniform. The major drawback in human rights discourse is that such rights do not have an independent existence: they come into existence by virtue of the conscious social decision to create, and to believe in, the concept of inalienable human rights as an inherent part of human nature.[48] Despite rhetoric to the contrary, human rights are a social construct. The fact that the rights are socially constructed does not make them arbitrary or conventional, but it does contain within it the most important weakness of human rights and this is the fact that they require justification through contextual interpretation.[49] Creating and maintaining rights of privacy is especially difficult in the light of new technologies and in Europe the area of advanced CCTV surveillance must pay special attention to two particularly relevant European Conventions that create rights to privacy, namely the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[50] and the Charter of Fundamental Rights.[51]

---

48 Donnelly, J, *Universal Human Rights in Theory and Practice*, 2nd edn, 2003, Ithaca, NY: Cornell UP.

49 *Ibid*.

50 Council of Europe of 4 November 1950 (ETS No 5), at www.echr.coe.int/Eng/BasicTexts.htm.

51 Proclaimed by the European Council in Nice on 7 December 2000 (2000/C 364/01), at www.europarl.eu.int/charter.

The ECHR and the Charter are very similar with respect to privacy,[52] and this chapter, for the sake of brevity, will look only at the text of the ECHR. It is important to note that the Charter does not bind Member States of the European Union but obliges the European Council, European Commission and European Parliament to observe its content in their legislative work. The ECHR, however, has become substantive law in the Member States. Article 8 states:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The purpose of this Article is to ensure that privacy is protected. Naturally, there cannot be unlimited privacy, and the issue becomes one of balancing the right of the individual to privacy with the needs of the state.[53] What is important to note is that the use of surveillance systems is a *prima facie* invasion of an individual's right to privacy and as such it must be supported by adequate legislation to be justified under the ECHR. It should also be noted that the right to privacy is not only applicable against the state and therefore state-controlled surveillance. The ECHR, through the interpretation of the European Court of Human Rights, obliges the state to act positively and provide privacy even if the surveillance equipment is operated by a private actor.[54]

Loss of privacy is one of the main social costs of the massive implementation of CCTV: the gaze of the camera follows and records the innocent as well as the guilty and it is important to ensure that the systems in place do not burden individual privacy unnecessarily. The question is therefore one of proportionality. The implementation of CCTV to prevent crime or enhance security has a detrimental effect on an individual's privacy, and therefore the advantages of the system must be appraised in relation to these losses. This need for proportionality is reflected in Article 8 of the ECHR. The main arguments against intelligent surveillance systems fall into three categories: (1) system error; (2) function creep; and (3) privacy.

System error

Errors occur within any system, and it is important to attempt to keep them to a minimum. The most common faults are false positives and false negatives generated by the system, and all false responses should be minimised since they generate mistrust amongst users of the system. From the privacy perspective, false positives are the most damaging systems error as they can lead to the identification of an individual on false grounds. This identification and the actions resulting from it add to the loss of privacy of the individual identified.

---

52 Explanatory text to the Charter of Fundamental Rights: http://ue.eu.int/docCenter.asp?lang=en.

53 See Wong, Chapter 12.

54 See, eg, *X and Y v Netherlands* (1985) 8 EHRR 235; *Hatton and Others v UK* (2002) 34 EHRR 1.

Function creep

Function creep can occur in two ways: first, the system can be used for purposes other than for that which it was designed. This is prohibited by the DPA, which states that data may only be used for the purpose for which it was collected.[55] The second form of function creep occurs where individual operators use the system in an unauthorised manner. The frequency with which such occurrences take place shows that legislation on its own is not enough to prevent individual users looking at unauthorised parts of the system.

In Sweden, following the murder of the Swedish Foreign Minister in September 2003, most rules set to safeguard privacy against function creep failed. Since 1975, hospitals have been taking DNA samples from all children born in Sweden. This biobank is to be used for specific purposes regulated under the Swedish law overseeing DNA databases.[56] The purposes of access listed in the law are medical treatment and purposes such as quality control, education, research, clinical testing, and development work. After the murder of Anna Lindh, Huddinge University Hospital in Stockholm gave DNA samples to the police. The hospital claimed that its actions were legal since the police have the right to seize evidence while investigating serious crimes (Rättegångsbalk, Chapter 27). In this pressed situation, the interpretation of a conflict of legal obligations, ie to obey the police or to protect the integrity of the individuals whose data is stored in the DNA Database, requires great strength on the part of the responsible doctor. The law, it appears, did not provide adequate protection of the individuals' integrity as the law concerning the use of biobanks was easily ignored in favour of the efficiency of the Police investigation.

However, the creation of clear laws is not enough to guard against function creep. In an enormous display of function creep by individual operators using a system in an unauthorised manner, more than 200 policemen across Sweden are now suspected of unlawful access (*dataintrång*) after the murder of Anna Lindh. None of them were involved directly in the investigation; they were indulging their curiosity by using police systems to access information on the murder enquiry.[57] The creation of databases and the linking together of databases and surveillance facilities is one of the greatest privacy concerns today.[58] Connecting databases allows for data which is stored and collected for legitimate purposes to be compared in an illegitimate manner. Such illegitimate use of data must be an issue of great importance for the bodies concerned with the data protection of individuals.

Privacy

As previously shown, CCTV in general and smart surveillance systems in particular pose a great threat to the individual's right to privacy. The loss of privacy via

55 Data Protection Principles Two and Three.
56 Lag (2002:297) om biobanker i hälso- och sjukvården m.m.
57 Brottsbalk (1962:700) 4 Kap § 9c.
58 Norris and Armstrong, *op cit* fn 30.

surveillance should only be permitted if the benefits created by such systems greatly outweigh the sum of an individual's loss of privacy. This utilitarian argument is morally appealing, and is supported in legal philosophy and in substantive law. Its foundations lie in the realisation that the individual's right to privacy is not, and nor should it be, an absolute right.

However, arguments in support of smart surveillance are based firmly on arguments of criminal deterrence – an effect which, on the whole, has not been proven either in theory or in practice. The deterrent effect is seen to come from the fact that the criminal justice system can use smart surveillance as an important tool in its efforts to identify criminals. Even if the deterrent effects of smart surveillance have not manifested themselves in tests, it would be acceptable to implement such systems if the crimes themselves were serious enough to motivate that every possible effort should be made in an attempt to prevent, or solve, them. However, in most cases, the greatest effects of smart surveillance have been seen with lesser crimes or crimes against private property. The question which needs to be asked is whether the right to privacy should be curtailed in this manner in an effort to prevent these types of crimes, or whether it would be better to use economic resources on other crime prevention initiatives.

Privacy is a fundamental human right, meaning that it is granted to all individuals and can only be removed or reduced in a limited set of circumstances. The use of surveillance systems comprising of databases and cameras deployed in public spaces prior to the commission of any crime is a substantial limitation on the right of privacy of individuals within the database. Details of known criminals stored within a database connected to a surveillance system which actively searches for them without a crime being committed, following them in case a crime is committed, is neither an efficient use of resources nor a legitimate limitation on the individuals' rights of privacy. If we see certain rights as inherent and privacy as such a right then the system of monitoring even before an offence has been committed is a serious limitation on privacy and the storing of potential suspects' profiles can be seen as dehumanising. This trend is further supported by the adoption of pattern recognition systems that limit the individuals' right to deviate from the given norm, as shown in the section on pattern recognition.

Conclusion

The subject of surveillance is a large area to deal with in a single chapter. The task is made particularly difficult since we stand only at the precipice of large scale dissemination of smart surveillance systems which are commonly justified on the grounds of combating evils (such as terrorism). Despite the novelty of widespread CCTV and smart surveillance, there is much opposition to its deployment. It is not currently seen as a panacea for criminal activity.

When it comes to judging smart surveillance from a legal perspective, it is important to consider the whole data processing process and to be aware that legal safeguards are not capable of creating fault-free systems: the potential for systems abuse must be acknowledged and striven against. When using the DPA to ensure individual privacy against intrusions by smart surveillance systems, the weaknesses of this legislation must be considered and prepared for.

Within the European Union, data protection legislation is seen as a great advantage and a step forward in the protection of individuals' privacy. However, it is important to remember that the legislation was produced prior to the development of advanced smart surveillance and should not be the only piece of legislation that can be effectively used to defend individuals' privacy. The human rights instruments are also important tools, but have not been used effectively and proactively to ensure that the individual retains their privacy, which is so often taken for granted. Presently, the world is involved in a quest to minimise criminality and terrorism. While these are worthy causes, they must not become ultimate goals in themselves.