



Protecting Personal Data in Camera Surveillance Practices

Lynsey Dubbeld¹

Abstract

This paper explores in which ways privacy (in particular, data protection principles) comes to the fore in the day-to-day operation of a public video surveillance system. Starting from current European legal perspectives on data protection, and building on an empirical case study, the meanings and management of privacy in the practice of Closed-Circuit Television (CCTV) will be discussed in order to identify the ways in which data protection is addressed in the operation of a video surveillance system. The case study suggests that views expressed by actors involved in the use of CCTV and the organisational and technical measures that have been employed, are related to a number of data protection issues, in particular principles regarding data quality. In addition, the case shows that while regulations (consisting in particular of organisational procedures) pertaining to the permissibility of data processing can be discerned in the practice of centralised CCTV, few indications exist that mechanisms taking into account data subjects' rights were established. Therefore, the system of video surveillance discussed in this paper suggests that different elements of data protection feature in different ways in the context of CCTV. This finding gives clues as to future research on privacy and camera surveillance.

Introduction

The growing use of public video surveillance systems has repeatedly elicited questions about privacy. Although Closed-Circuit Television (CCTV) has often been hailed as an indispensable tool in crime prevention, crime reduction, law enforcement, etc., and has become an increasingly popular security measure in the fight against terrorism, it has also evoked concerns over the loss of privacy.

Several studies, surveys and reports have suggested that the privacy implications of video surveillance are an issue of concern among the public (e.g., Smink and Hamstra, 1998; EPN and Telindus, 2001; Koops and Vedder, 2001). Civil liberties groups and activist consortiums that have criticised the growing use of camera surveillance have tended to invoke notions of privacy (e.g.: ACLU, 1999; BCCLA, 1999; Davies, 1998; Zoom: dossier cameratoezicht, 2000). Also, the media frequently report on privacy problems posed by CCTV applications (cf. Gray, 2003).

¹ Centre for Studies of Science, Technology and Society, Faculty of Business, Public Administration and Technology, University of Twente, The Netherlands. <mailto:l.dubbeld@utwente.nl>

In a survey of the five major national newspapers in the Netherlands I found that between 1997 and 2003, a total of 647 articles on camera surveillance were published, 147 of which referred to privacy issues. Meanwhile, policies and legislation regarding camera surveillance have developed in the light of privacy regulation (see for Dutch examples e.g.: Baas and Cozijn, 1996; Registratiekamer, 1997; see for European policy e.g.: Opinion 4/2004 on the processing of personal data by means of video surveillance, 2004).

In other words, privacy is often brought to the fore in debates and policies regarding CCTV. Yet the meanings of privacy and the ways in which privacy issues play a role in the context of video surveillance remain largely unexamined (cf.: Dubbeld, 2004). This paper aims to provide a clarification of these issues: it will explore the privacy issues addressed in public video surveillance systems by describing approaches to privacy protection taken up in the day-to-day operation of a public CCTV scheme.

Put briefly, the central question in this paper is: In which ways is privacy addressed and dealt with in the practice of public video surveillance? This question includes sub questions such as: How do data protection principles figure in the everyday practice of CCTV? In which ways do actors involved in using camera surveillance refer to privacy issues? Which technical and organisational measures for privacy protection are proposed, implemented, and used by those involved in the practice of video surveillance?

In order to answer these questions, I will confront some of the ideas about privacy developed in the legal framework for data protection with an empirical case study of CCTV. The case study analysis will allow for an exploration of approaches to privacy that come to the fore in the day-to-day operation of electronic visual surveillance.

Theoretical background

A growing number of studies have analysed the everyday practices of CCTV (e.g.: McCahill and Norris, 2003). Most notably, Norris and Armstrong, in their study of three British town centre CCTV schemes, revealed control room operators' behaviours, attitudes and working rules when producing targeted observations of groups and individuals (Norris and Armstrong 1999). More recently, Michael McCahill extended the analysis of CCTV to include not only the activities of operators, but also their interactions with other actors involved in the use of camera surveillance, such as retailers, police, the city council, local newspapers, etc. (McCahill, 2002; cf.: Coleman and Sim 2000).

Although these studies provide revealing insights in the practical operation of camera surveillance systems, they have little to say about the day-to-day management of privacy in the context of CCTV (e.g.: Weitenberg *et al.*, 2003). Given the media attention and public concern regarding privacy implications of camera surveillance, the lack of analysis of privacy in studies of surveillance is, to say the least, surprising. This paper aims to overcome this shortcoming, by exploring, identifying and describing the ways in which privacy principle come to the fore in the operation of camera surveillance.

The empirical exploration in this paper is based on a framework drawn up from legal approaches to data protection developed in Europe since the 1970s. Although I am committed to studying privacy issues in the context of an empirical practice, it is also necessary to take into account some of the notions that have become available in legal theory and practice: in a sense, privacy risks can only be identified and described on the basis of some level of understanding of what privacy means. The analysis in this paper will therefore be based on a basic legal framework that will provide points of reference for the empirical exploration of camera surveillance practices.

The case analysis presented in this paper is informed by contemporary surveillance studies, in particular the approaches to studying CCTV developed in the works of Clive Norris and Michael McCahill (e.g.: Norris and Armstrong, 1999; McCahill, 2002; McCahill and Norris, 2003). These studies have provided useful insight into methodologies for the empirical study of camera surveillance practices.

Methods

The analysis in this paper is based on a case study of a centralised system of camera surveillance currently employed in a number of railway stations in the Netherlands (see section 3). The case study involved empirical fieldwork, conducted in winter and spring 2001-2002, which consisted of observations, interviews and a literature survey.

I carried out observations and held informal interviews in the CCTV system's central control room. I spent 136 hours following operators in their routine work at different times of the day, and talking to them in the canteen during breaks.

Also, I conducted several one-hour, semi-structured interviews. Interviews were held with three facility managers in the railway company who had been involved in the implementation and operation of the CCTV project, and the manager for the central control room. Also, I interviewed spokespersons for two Dutch advocacy groups that were critical towards public camera surveillance, two policy makers at the Dutch data protection authority, the unit manager for the control room staff, and two police officers working in the local Railway Police station.

In addition, a survey was made of texts relating to the case, including the railway company's policy documents, internal reports, technical evaluations, and customer surveys. I also reviewed newspaper articles (in the four main Dutch national newspapers in the period from 1992-2003) that featured the railway company's video surveillance projects.

The empirical data were analysed by mapping the actors involved in the practice of centralised CCTV (including human and non-human actors) in order to identify the locations where privacy came up as an issue. Then, the privacy themes that emerged in this map were drawn up, and fragments taken from field notes, interviews and text summaries were categorised under a number of headings (cf.: McCahill, 2002: 29-30). In this way, it became possible to discover the meanings that were assigned to privacy by those involved in the practice of camera surveillance and to describe to what extent aspects of privacy that we know from legal frameworks for data protection came to the fore in practice.

Privacy notions

This section will briefly discuss a number of aspects of privacy that will serve as a point of departure for the empirical analysis of video surveillance. In order to explore the ways in which privacy issues figure in the day-to-day operation of centralised CCTV, I will use a set of notions derived primarily from European legislation and policy regarding data protection.²

The choice to focus on informational privacy approaches follows from the perception that data protection issues have received widespread attention in current privacy perspectives on CCTV (e.g.: CCTV: looking out for you, 1994; Hoek et al., 2000: 31, 55-56; EPN and Telindus, 2001: 25).³ In addition, a regulatory framework concerning CCTV applications has developed, which has been modelled on data protection views (see e.g.: Armitage, 2002; Opinion 4/2004 on the processing of personal data by means of video surveillance, 2004). Allied with data protection legislation, institutions (data protection authorities and information and privacy commissioners) have been established which supervise compliance with the law.⁴ CCTV has been one of the technologies that data protection commissioners have taken into account in their publications (e.g.: Flaherty, 1999; Registratiekamer, 2001; Homburg and Dekkers, 2003). In some cases, the privacy rules laid down in data protection legislation that have been applied to camera surveillance systems have been supplemented by guidelines and codes of conduct developed by national data protection authorities (e.g.: Cavoukian, 2001; Camera's op de werkplek, 2002).

Therefore, it seems legitimate to hold that, especially in Europe, data protection has become a widely shared perspective on privacy in the context of camera surveillance practices. Therefore, I will discuss some of the legal principles of European data protection, which will shed light on the categories of situations that have come to be perceived as subject to a consideration of individuals' privacy interests.

² Of course, currently, a wealth of different privacy notions exists, many of which go beyond data protection issues. The fact that the focus in this paper is on one specific type of privacy is not meant to convey the impression that other aspects of privacy are irrelevant or unimportant with respect to the study of CCTV. In fact, as I have argued elsewhere (Dubveld, 2004), concepts of bodily integrity and the private sphere unmistakably bear relevance to a conceptualisation of the privacy implications of public video surveillance systems as well.

But a complete analysis of the privacy aspects of camera surveillance practices requires more space than this paper allows for. For this reason, the privacy analysis of CCTV presented in this paper will be limited to a consideration of European data protection principles, and not discuss other legislative developments that could be relevant to CCTV, such as the European Convention of Human Rights (cf.: Neyland, 2000; Dodd, 2002; Dyer, 2003).

³ The privacy implications of CCTV are occasionally also referred to in terms of the right to respect for private and family life (e.g.: Hert and Gutwirth, 1995; Hempel and Töpfer, 2002).

⁴ At least, this has been the case in Europe and Canada, which have adopted omnibus legislation in the area of data protection that has included arrangements for the implementation of agencies to supervise compliance with the law. The US approach to data protection has been dominated by the development of sectoral legislation and self-regulatory policies within organisations, without here being any over-arching, independent supervisory institutions like those in the European Union and Canada.

Of course, data protection arrangements and informational privacy concepts are far from uncontroversial, stable, or unequivocally supported. Some countries have defined legislation in terms of information privacy, others in terms of data protection; in some theoretical perspectives, privacy is conceived as a trade and consumer issue, while others have focused on privacy as a fundamental human right (Blok and Vedder, 2002; Regan, 2003).

Nevertheless, within these different perspectives, a number of recurring themes and principles can be distinguished. As Bennett and Grant suggest, in the area of data protection a process of international policy convergence has taken place: ‘... there is a broad international consensus, at least among the industrialized countries, about what it means for an organization to pursue privacy friendly policies’ (Bennett and Grant, 1999: 6). A number of data protection criteria can be distinguished that are widely agreed upon (Bennett and Grant, 1999: 6; cf.: Bennett, 1992: chapter 3; Gutwirth, 2002: 83-95; Blok, 2002: 127). The variety of approaches to data protection appear to share an underlying concern with giving individuals a number of rights with respect to the protection of their personal data and requiring organisations to take into account some rules regulating their information processing activities (Regan, 2003: 263-264; Prins, 1998: 217), thus addressing power inequalities between data subjects and data processing organisations (Gutwirth, 2002: 86).

Legally, the European Union’s data protection directive (EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, or EU Directive for short) has set out the principles for data protection that are now perhaps most widely endorsed.⁵ The EU Directive, and its national counterparts, includes several types of data protection principles (cf.: Vedder, 2001: 405-406): following the chronological order of the phases of data processing and the concomitant steps for data protection to be taken by data controllers, three distinct categories of data protection principles can be distinguished.

The first set of principles that I distinguish relates to the general basis of data processing, i.e., criteria for assessing the *permissibility* of the set-up and use of information systems, which are based on the idea that data processing should be lawful and fair, and should serve well-defined, justifiable purposes (see: Gutwirth, 2002: 96, 101).

Once the permissibility of the information system and its purposes has been established, a second type of principle comes to the fore, i.e., those aiming to ensure *data quality*. The central tenet is that data processing should be appropriate and proportionate in relation to the purposes identified. In addition, a number of criteria relate specifically to the intrinsic quality of information

⁵ Admittedly, the EU directive, although illustrative of data protection perspectives, is not necessarily representative of all data protection regimes. The directive applies to EU countries only, and is far from uncontroversial there and elsewhere. Most notably, the US has strongly opposed the EU approach, and has favoured the implementation of self-regulatory instruments in the private sector (e.g.: Regan, 1995; Blok, 2002). However, as the case study analysed here concerns a data processing system in the Netherlands, i.e., an EU country, I will focus on data protection principles distinguished in the EU Directive (see section 5). The principles distinguished in the EU Directive recur in its Dutch counterpart, ‘Wet Bescherming Persoonsgegevens’.

(i.e., information should be accurate, complete, and up to date; and technical and organisational safeguards for security of data systems should be in place).

Finally, data protection provides for a number of *rights for data subjects*, in order to allow individuals to have some control over their personal information. Put briefly, individuals have the right to know about, access and correct their personal data (Gutwirth, 2002: 102-103).

These three types of principles appear (although often in different wordings) in several international agreements, national laws, and organisational guidelines and codes of practice. To sum up: after the general *permissibility of data processing* has been assessed, criteria for adequate uses of information are at stake, which consist of mechanisms for ensuring *data quality* as well as for protecting *data subjects' rights*.

To conclude, the notion of personal data protection described here serves to provide points of reference for the empirical study of camera surveillance practices. That is, issues concerning the protection of personal data will be at the basis of my exploration of the privacy issues coming to the fore in the context of CCTV applications: these issues convey some basic ideas about the meaning of privacy and describe a number of specific situations that privacy rights have a bearing on. Put briefly, data protection involves issues regarding the permissibility of the application of data processing systems, the quality of data processing and the consideration of data subjects' interests in privacy protection. The following sections will explore these issues on the basis of a case study.

The case study

The case study I analyse here concerns a centralised CCTV scheme that is currently in use in a number of railway stations in the Netherlands. In autumn 2000, one of the major Dutch railway companies introduced a system that connected cameras located in fifteen railway stations across the country to one central control room, where live monitoring would take place 24 hours a day. This type of centralisation of video surveillance was unprecedented in terms of extent and range in the Netherlands. The CCTV scheme was part of a larger set of measures taken to improve public safety in train stations and adjoining areas.

Camera surveillance in Dutch railway stations

Video surveillance has been employed in railway stations in the Netherlands since the early 1990s. By the year 2000, approximately 1000 cameras were in operation in railway stations across the country (internal report, 19 October 2000).⁶ The majority of these cameras were monitored in seven control rooms located on the larger train stations and owned by the railway company whose CCTV scheme is analysed in this case study. In the late 1990s the railway company decided to reconsider its policy with regard to the operation of camera surveillance in

⁶ Internal reports produced by the railway company referenced and cited in this paper have been translated from Dutch by the author. These reports are not included in the bibliography, as they are confidential and could reveal the identity of those who participated in the research. For the same reason, field notes and interview transcripts cited in this paper have been anonymised.

train stations, which resulted in a proposal for the centralisation of the divergent CCTV systems (internal report, 29 September 1999). The seven local control rooms that had been in use, monitoring and registering the camera images of 24 stations, were reorganised, and the number of train stations under surveillance expanded.

It was expected that the set up of a centralised CCTV network would realise 'maximum flexibility for the presentation and recording of images' (internal report, 29 September 1999). For instance, the implementation of a central control room would enable the operation of new colour-cameras, the introduction of new motion detection systems linked to the CCTV system, etc. Also, operators could be assigned additional tasks such as handling fire alarms, elevator alarms, etc. (internal report, 29 September 1999). The central control room aimed to establish systems that would allow continuous live monitoring (which would contribute to crime prevention) as well as digital recording of incidents (which would aid law enforcement and public prosecution).

In the period between October 2000 and December 2000, the centralised control room was installed, which meant that 1100 cameras at fifteen locations throughout the country came to be monitored from a single location. Images captured by these cameras were monitored live 24 hours a day by security personnel. Automatically, video registration of images took place after incidents had been noticed, the tapes of which were kept for seven days in order to be used by the police and judiciary to serve as evidence if required. Also, all fifteen stations had sixteen cameras each on 'hot spots', the images of which were continually stored (and kept for seven days).

This was the system that I observed in the winter of 2001, when I started my field study of centralised CCTV in Dutch railway stations.

The central control room

The central monitoring room served as the hub of the railway company's CCTV network. The control room hosted five desks: three for live monitoring, and two spare ones ('replay suites'), which could be used to make back-ups or review tapes. Each desk was equipped with eight monitors: six for watching images; one showing a chart of the station that was being monitored; and one running software to register incidents, provide information on emergency aid, display a map of the country indicating the locations of train stations linked to the control room, and give notice of special events requiring specific attention at particular times and places, etc. All operators also had a phone, hands-free head set, keyboard, and walkie-talkie at their disposal. The guards used a central walkie-talkie when they were on street patrol in the nearby station.

Specially designed software enabled the operator to watch a pre-fixed set of cameras or stations through an automated schedule showing the images of the different camera sets at 10 or 30 second intervals. However, control room operators could also operate the system manually. The system was programmed in such a way, that it was impossible for two operators on different desks to view images of the station on different desks at the same time.

During at least one shift, usually at day times (7 AM till 3 PM), a team leader supervised the centralists and acted as the contact person for railway company managers, visitors, and external parties (such as the system maintenance company, the cleaning company, police and public prosecutors, etc). In times of emergencies or at busy hours, supervisors could also take turns behind the monitors – in fact, two of the team leaders working in the control room at the time of my research were former operators who had been promoted to the position of supervisor. These supervisors, four in all, were also responsible for planning the work schedules for employees, contacting services in case of deficiencies or malfunctions in the system, and reporting to the railway company on a weekly basis.

In other words, the central control room brought together a range of technologies and human actors, all of which were mobilised with a view to the improvement of the public's feelings of safety in the railway company's public transport facilities. In the next sections, I will discuss in which ways privacy issues came to the fore in the day-to-day operation of this surveillance system.

Privacy in the practice of centralised video surveillance

In this section, I will argue that in several senses data protection has been an unmistakable component of the practice of CCTV studied here.

Put briefly, the protection of personal data came to the fore in two ways. First, actors' views referred to issues that could be seen to express data protection considerations. Secondly, in the practice of CCTV in railway stations a number of procedures and regulations were adopted that could be seen as examples of the application of data protection guidelines.⁷

Actors' views

Views expressed by some of those involved in operating centralised CCTV (such as the control room operators and the railway company's facility managers) suggest that privacy was often perceived as a legal issue concerning technical and organisational measures for the protection of personal data. Those using video surveillance in railway station areas often explicitly referred to privacy as a data protection concern.

⁷ Unfortunately, because of practicalities in the field study, I am unable to include in this analysis attitudes towards privacy among the observed populations of CCTV. Having gained permission to do research of the centralised system of CCTV through the railway company in charge, I was committed to taking into account their rules and regulations. This meant, amongst others, that I was not allowed to talk to travellers in railway stations. As a result, the views of the observed would be virtually absent or invisible in my case analysis, which in turn meant that those who were perhaps most likely to express views on privacy, be subjected to privacy sensitive surveillance, or experience privacy invasions, could not be included in my analysis. I have tried to overcome this problem by analysing questionnaires, interviews and reports which have surveyed the privacy opinions of observed populations, and by identifying and describing (through the camera images monitored by the operators, and through observing situations in the stations while they were on patrol) the actions taken by the individuals and groups under surveillance. In this way, I have deduced (rather than seen and heard myself) the views and actions of observed populations. The public opinion surveys that I had access to suggest that the public tends to identify privacy concerns in the context of CCTV with data protection issues.

Data protection legislation was referred to when issues regarding data storage and data access were discussed. For instance, in one of their meetings, control room team leaders discussed the possibility of using an extra console in the control room – which at the time was used solely for making copies of tapes – for live monitoring. While it would have been more convenient to have an extra desk for operators to use during busy hours, the team leaders nevertheless refrained from implementing the plan: if operators were given access to the extra desk, they would also (automatically, as a consequence of the computer's technical design) be able to make copies of tapes, and as one of the team leaders said, 'that is not allowed by the Registratiekamer [former Dutch data protection authority]' (internal meeting central control room, 14 March 2002).⁸ The railway company's privacy policy for CCTV had laid down that only team leaders were allowed to make copies, and giving operators authorities to do the same would therefore run against the official data protection procedures (and therefore, possibly, elicit criticisms by the data protection commissioner).

In a similar vein, when discussing the privacy issues of video surveillance, the railway company's facility managers who had been involved in the introduction and development of the centralised CCTV scheme referred to organisational privacy policies that had been implemented in view of data protection legislation. In one of my interviews, one of the facility managers said that she considered privacy to have 'been taken care off' as a consequence of the implementation of these privacy policies (interview railway company facility manager, 25 January 2002).

- Has privacy been considered an important issue during the implementation of camera surveillance, for instance with respect to the centralised control room?

[Very brief, firm] 'No.'

- You didn't expect any complaints or resistances from travellers or customers?
'No, because it [CCTV] fits with our general mission to create safe, pleasant railway stations. We comply with the legal frameworks. We have registered with the Registratiekamer [former Dutch Data protection commissioner], the current ...'

- College Bescherming Persoonsgegevens [the current Data protection commissioner in the Netherlands].

'Exactly, that one. It has all been taken care off. But it has actually been a necessary evil: if you want to use video surveillance, you have to make arrangements [with respect to privacy protection], and so we have complied.'

⁸ Recommendations by the Dutch Data protection commissioner were also referred to when principles for data retention implemented in the railway company's CCTV system were discussed. In general, the Dutch data protection commissioner would recommend that organisations using CCTV in the public domain or in their premises remove collected data as quickly as possible, preferably within 24 hours (see e.g., Registratiekamer, 1997). In many cases, however, storage could last up to three days or even a week, if there would be good arguments for doing so. For example, in view of the pace of work of law enforcement agencies and the possibility that witnesses and/or victims might only report crimes after several days, seven days came to be considered as a reasonable and legitimate time lapse for data retention. The railway company consulted the Dutch Data protection commissioner prior to setting up its CCTV systems. After the centralised scheme had been implemented, the Data protection commissioner again expressed his approval of the railway company's policy to store camera images for seven days (internal meeting railway company and Data protection commissioner, 25 February 2002).

But there has never been a consideration of privacy in the decision making process about the introduction of CCTV. And we have never had any complaints.'

- Do you think that the procedures that have been put in place now are considered adequate by the public?

'Yes.'

- Because there is a privacy policy?

'We have laid down how data is being recorded, how long we will store data, to whom we can transfer copies, for which purposes data can be transferred...'

In other words, those involved in the use of video surveillance identified privacy with protections regarding the processing of personal data, the procedures and norms of which were drawn from data protection regulations that were supervised by the Dutch data protection commissioner.

Technical and organisational measures for data protection

The centralised CCTV system utilised several technical and organisational measures that could be seen as being illustrative of data protection principles. These included for instance technical arrangements for security of data transmission and data storage, the set-up of a privacy policy, and the development of procedures relating to data transfer. Each of these measures could be seen as the direct results of European and Dutch data protection law being applied in practice (see also section 5). In fact, as a result of the Dutch counterpart of the European data protection law, the railway company was required to register its CCTV project with the data protection commissioner and implement adequate privacy policies regulating its use.

Technical measures

In the centralised system of CCTV, various sets of technical measures relating to the protection of personal data were established.

First, the railway company aimed to ensure security of data transmission. The cameras monitored in the central control room were part of a closed circuit that connected divergent locations over, in several cases, considerable distances. In order to ensure data security during the transmission of images the railway company used a wholly owned fibre-optic data network. Data collected through video cameras would therefore be transported to the control room via a secured network that could only be accessed by the railway company in charge.

At the time of the implementation of the central control room, the secure network had not been installed. However, it turned out that one of the railway company's subsidiary divisions was tapping images from the CCTV network in order to use these for the observation of flows and movements of travellers on railway station platforms (interview railway company facility manager, 25 January 2002). After negotiations, the situation was changed and the secure system was implemented, which was to ensure that only the railway company's department in charge of the centralised control room had access to and ownership of the network.

A second set of technical security measures was concerned with regulating data access. In the central control room, operators logged on to PCs and monitors with individual user names and

passwords. Operators did not have the authority to access stored data or make copies of records. Stored data could only be accessed and copied by team leaders who would have their own, specific security level that gave them authority to make copies (see above, section 4.1).

Thirdly, the railway company employed a number of technical measures aimed at maintaining particular levels of physical security of camera equipment in the control room.

For instance, the entrance to the building where the control room was located was equipped with a camera and an intercom through which the operators could see and hear who was at the door before opening it. As the privacy policy stipulated, the control room was only accessible by security personnel hired by the railway company (such as operators monitoring cameras in the control room and security guards employed for doing foot patrols in railway stations who would use the control room canteen when having breaks), managers of the railway company, and those who needed access to do maintenance work in the control room (such as the system administrator and cleaning personnel).

Also, a number of physical security measures were in place within the monitoring room itself. The control room door could be closed but not locked (because the room was used 24 hours a day, locking it was simply not convenient). However, the camera equipment in the control room was physically secured: desktops of PCs linked to monitors were kept in fireproof cupboards under the operators' desks.

Several techniques also existed that were intended to ensure that data collected in the CCTV system would be stored and used in appropriate ways. For example, stored images were kept for seven days – the maximum amount of time allowed by the Data protection commissioner (see note 7) – and then removed automatically by the IT system on the basis of a first-in-first-out scheme.

Also, the CCTV system software ensured that copies of tapes were not manipulated, through adding a watermark that would only be visible in copies that had been made by the group leaders at their password secured PC in the central control room. While this type of protection was generally thought to be important with respect to the admission of footage in court cases (where tapes could serve as additional evidence), the railway company also saw these guarantees as an important element of its policy of maintaining system security. As one of the team leaders said, as he explained the password secured CCTV system to me, 'privacy is all taken care off' as a consequence of the authentication method (field notes, 8 November 2001).

Organisational measures

In addition to technical security measures, the railway company also implemented a number of organisational procedures that aimed to provide safeguards for privacy by protecting personal data against unauthorised access.

For example, the private security guards who were involved in monitoring signed a confidentiality agreement that prohibited them from discussing issues related to the CCTV scheme with anyone outside the company. According to the unit manager supervising the control room personnel, the

agreement was meant to safeguard the 'privacy of the [railway company's] data', while it would also reassure employees that their privacy was protected in respect of the information that outsiders and colleagues could discover about their work conduct during working hours (interview security company unit manager, 14 March 2002).

Also, there were detailed procedures relating to data transfer. As was mentioned above (in section 4.1), only team leaders were allowed to make copies of tapes. These copies could only be handed over to police or to the District Attorney after these had filed an official request form requesting specific data. A filing system kept track of the copies that had been made and sent to the authorities.

The railway company management had also set up a privacy policy for the central control room which laid down a number of procedures and regulations with respect to data protection (see section 4.1). In fact, in the early phases of camera surveillance in train stations the railway company set up a privacy procedure even though at the time data protection law did not require this. For instance, several of the railway company's CCTV systems used analogue data storage techniques such as analogue VCRs, which meant that data protection law was not applicable (as it only applied to information stored and processed digitally). Nevertheless, the company decided to conform to the regulations laid down in data protection law concerning digital camera systems – not only because later improvements to its CCTV system would require similar rules anyway, but also because of general corporate policy (internal report, 07 October 1997). Later, when digital camera systems were implemented on a large scale, the privacy policy was updated and again registered with the data protection authority (interview railway company facility manager, 25 January 2002).

'We had always had a procedure, actually from the very early start onward. We had one, but I [in 1999, when the central control room was set up] had to register it under another name and in an updated version. That was obligatory, because we were introducing digital media. That was the borderline at the time, in fact. With analogue media you could get away with a lot of things, to put it that way, but with digital systems you can't escape the requirement to build in some guarantees.'

To conclude: in the practice of centralised CCTV in Dutch railway stations a number of technical and organisational instruments for security of data processing systems and protection of personal data were developed. It seemed that actors involved in the operation of video surveillance were familiar with data protection issues and took into account requirements laid down in Dutch data protection law. The next section will discuss in more detail in which senses legislative principles of personal data protection occurred in the centralised system of camera surveillance.

Data protection in camera surveillance practices.

Views on privacy expressed by those involved in the use of centralised CCTV can be regarded as illustrative of an increasingly widespread perception that camera surveillance is capable of having impact on protection of personal data. Put differently, the technological safeguards and

procedural arrangements for privacy protection described in the previous sections could be considered to be evidence that those involved in the operation of centralised video surveillance were aware of and took into account data protection interests. That is, in the operation of CCTV in Dutch railway stations privacy issues came to the fore in ways that were reminiscent of the legal framework for data protection, or that could be considered as the result of data protection rules being applied in practice.

As section 4 suggests, in the practice of centralised CCTV in Dutch railway stations, several approaches to privacy were expressed by actors involved in operating the system and taken up in the organisational procedures and techniques that they implemented. These approaches appeared to be in line with several principles of fair information processing that have been laid down in national and international legislation in Europe since the 1970s, especially the EU Directive and its Dutch counterpart (which I focus on here, see note 4).

For one, the case study revealed that the railway company in charge of the video surveillance equipment implemented a number of technologies to ensure system security regarding data processing – and technical security measures are one of the data protection principles mentioned in data protection legislation (article 17 paragraph 1 in the EU Directive). The technical design of authorisation levels (which ensured that operators could not make copies of tapes, while team leaders could) aimed to prevent unauthorised access, disclosure and transfer. Similarly, physical mechanisms for securing the data network and control room location (such as the secured network cabling and fireproof cupboards for control room equipment) were set up in order to regulate access to data processed in the CCTV system.

Also, the use of an automated software system that automatically removed stored images after seven days seems indicative of the application of article 6 paragraph 1e in the EU Directive, which holds that data not be kept for longer than is necessary. Ensuring accuracy of personal data is one of the other principles for data quality laid down in the Directive (article 6 paragraph 1d). The control room's software system that was designed to watermark copies of tapes could be regarded as a way to apply the accuracy principle in the practice of camera surveillance.

In addition, organisational measures for secure data processing (which the EU Directive mentions in article 17 paragraph 1) were laid down in the railway company's privacy policy for the central control room. The privacy guideline developed by the railway company included procedures with respect to data transfer, which is a topic addressed in the EU Directive's article 6 paragraph 1b. In a similar vein, the notion of confidentiality of processing (article 16 in the EU Directive) appears to be taken up in the agreement of confidentiality signed by the control room operators.

In other words, in the empirical analysis of a centralised CCTV system, a number of data protection issues can be distinguished, most of which refer to what the EU Directive discusses in terms of security of processing, confidentiality of processing, and data quality. From the perspective of categories of data protection principles that I discussed above, it could therefore be said that the ways in which privacy has been addressed in the practice of video surveillance in railway stations are predominantly related to regulations concerning data quality. That is, those

involved in the operation of centralised CCTV tended to identify privacy issues with mechanisms and procedures related to personal data being accurate, complete, up to date, and data processing being confidential and secured.

The focus on principles relating to data quality might seem to imply that other categories of data protection mechanisms (i.e., those that I in section 2 discussed as principles pertaining to the permissibility of data processing and the rights of data subjects) have been largely absent in the approaches to privacy coming to the fore in the network of centralised video surveillance.

However, principles regarding the permissibility of data processing systems (such as lawfulness, fairness, and purpose-specificity) are, although not explicitly referred to by those involved in the use of camera surveillance, clearly visible in the privacy policy for the central control room. The privacy guideline set out that the use of CCTV in train stations was aimed at a range of public security issues, including the deterrence of crime, the enhancement of feelings of safety among travellers, and the protection of the railway company's property. The description of the video surveillance system's purposes in a privacy policy document could be perceived as ways in which the widely shared data protection principle of purpose specificity (laid down, for instance, in EU Directive's article 6 paragraph 1b) has been taken up and given form in practice.

On the other hand, the case study gives few clues as to the ways in which privacy plays a role in the practice of camera surveillance if it is understood as a set of rights assigned to data subjects. The privacy policy does not include any rules concerning data subjects' rights to access, correction and removal (as articles 12 and 14 in de EU Directive describe data subjects' rights). What's more, the privacy guidelines say that access to the control room is permitted only for personnel responsible for monitoring the cameras, system administrators, police, and the proprietor and his representatives (see section 4.2.1); copies of processed data will only be given to police and judiciary for law enforcement purposes; and removal of data takes place automatically after seven days. In other words, the privacy policy does not mention any provisions for data subjects to access or remove their personal data, nor do the observed populations' rights with regard to data protection seem to be expressed in any other way in the practice of centralised CCTV.

To sum up, my case analysis suggests that data protection issues unmistakably came to the fore in the practice of centralised video surveillance in Dutch railway stations. Yet different elements of data protection figured in this practice in different ways. While mechanisms for data quality were firmly put in place, considerations concerning the lawfulness, fairness and purposes of data processing were less visible, whereas data subjects' rights seemed even more absent.

The low level of visibility of some of these principles regarding the permissibility of data processing could be the result of the fact that they are likely to play a role in the context of CCTV *prior* to the introduction of video surveillance schemes rather than *during* their operation. That is, studying the day-to-day practice of a system of camera surveillance probably cannot easily reveal the principles relating to permissibility, because these have generally been dealt with during its implementation phases. In this respect, the high visibility of data quality regulations might not come as a surprise, as such issues could be likely to be a major focus once

the video surveillance system is in use and questions regarding, for instance, its legality, lawfulness and purposes have already been addressed. The apparent disregard of data subjects' rights in the centralised CCTV system might be more surprising, given the low-cost, easy-to-implement possibilities for setting up provisions that allow data subjects to exert their rights (such as providing copies of privacy policies at customer service desks, or posting privacy policies on the company's website). Of course, as a result of data protection law in the Netherlands and Europe, regulations regarding the permissibility of data processing systems and data subjects' rights do exist, and data subjects therefore have ample means of recourse to exert their rights—even if these rights are largely indiscernible in the practice of video surveillance.

Conclusion

This paper aimed to explore approaches to data protection in the everyday use of a system of railway station camera surveillance. The case study shed light on the ways in which actors involved in the operation of CCTV referred to privacy and addressed data protection issues. Also, the case study suggested how data protection principles were translated in practical measures, and which mechanisms and techniques for privacy protection were visible applied.

It should be noted that this analysis did not intend to evaluate compliance with data protection regulations or to assess the adequacy of data protection legislation. Rather, it was meant to reveal how in a specific practice of camera surveillance the general norms for data protection (such as those laid down in the EU Directive) were applied and gained shape.

As I argued, data protection played a role in the operation of centralised video surveillance in various guises. Issues concerning data protection and privacy that were addressed in the everyday practice of railway station CCTV appeared to have different meanings, ranging from principles with regard to access authorisation to technical measures for system security.

That is, the notion of data protection that is often invoked in the context of video surveillance systems did not simply refer to an undifferentiated set of regulatory principles. Rather, norms concerning data protection had different meanings in the practice of centralised CCTV, most of which related to organisational and technical arrangements for data quality and system security, while some others were concerned with regulations pertaining to the permissibility of visual surveillance systems as such. Only a few mechanisms were introduced with a view to data subjects' rights.

The variety of meanings assigned to data protection in the operation of video surveillance in railway stations can be seen to imply that robust analyses of the privacy implications of video surveillance practices need to recognise the diversity of features that data protection issues come to display in the day-to-day operation of CCTV.

In addition, this paper suggests that a satisfactory and adequate analysis of privacy in the context of camera surveillance cannot be limited to a consideration of specific elements of data protection, such as the existence of technical arrangements for system security. For instance, in

their 2002 study of London CCTV McCahill and Norris solely reported on the legality of signage of these systems when they discussed the requirements for data protection laid down in British data protection legislation (McCahill and Norris, 2002: 44). Yet the UK Data Protection Act, like the EU Directive that it was based on, includes a variety of data protection principles, and is not limited to requirements concerning transparency of data processing systems. A comprehensive privacy analysis of video surveillance practices would need to consider various data protection principles, and explore how their different elements and features come to the fore in practice.

Finally, it should be noted that data protection alone might not be a sufficient framework for coming to understand privacy issues and implications of CCTV systems, as other aspects of privacy, such as bodily integrity, could also bear relevance (see note 1). Future studies of CCTV will benefit from including these types of issues in their discussion of data protection and privacy.

Of course, as the results of this paper suggest, more research on the impact and management of privacy in video surveillance practices is desirable. This paper reported on an explorative study, which does not allow for generalisations or comparisons between CCTV systems in different countries. Making generalisations with respect to the nature, extent and impact of CCTV systems is problematic as it is (see McCahill and Norris, 2003: 44), and privacy studies of camera surveillance are no exception. Therefore, we'd better hope for a wealth of future studies that will empirically explore approaches to privacy in specific visual surveillance systems.

References

- ACLU (1999) 'ACLU calls on law enforcement to support privacy laws for public video surveillance', ACLU. 08 April 1999. <http://www.aclu.org/news/1999/n040899b.html> [Accessed: 05 March 2004]
- Armitage, R. (2002) *To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime*. London: NACRO.
- Baas, N. J. and C. Cozijn (1996) *Toezicht met camera's: toepassing, effectiviteit en juridische aspecten*. Den Haag: WODC/Ministerie van Justitie.
- BCCLA (1999) *Video surveillance in public places*. BCCLA. June 1999. <http://www.bccla.org/positions/privacy/99videosurveillance.html> [Accessed: 05 March 2004]
- Bennett, C. J. (1992) *Regulating privacy: data protection and public policy in Europe and the United States*. Ithaca/London: Cornell University Press.
- Bennett, C. J. and R. Grant (1999) 'Introduction', in C. J. Bennett and R. Grant (eds.) *Visions of privacy: policy choices for the digital age*. Toronto: University of Toronto Press, 3-15.
- Blok, P. H. (2002) *Het recht op privacy: een onderzoek naar de betekenis van het begrip privacy in het Nederlandse en Amerikaanse recht*. Meppel: Boom Juridische Uitgevers.
- Blok, P. H. and A.H. Vedder (2002) 'Privacy in ontwikkeling', in J. E. J. Prins and J. M. A. Berkvens (eds.) *Privacyregulering in theorie en praktijk*. Deventer: Kluwer, 5-31.
- Camera's op de werkplek* (2002) Den Haag: College Bescherming Persoonsgegevens.

- Cavoukian, A. (2001) *Guidelines for using video surveillance cameras in public places*. Toronto: Information and Privacy Commissioner/Ontario.
- CCTV: looking out for you* (1994) London: Home Office.
- Coleman, R. and J. Sim (2000) 'You'll never walk alone: CCTV surveillance, order and neo-liberal rule in Liverpool city centre', *British Journal of Sociology*, 51(4): 623-639.
- Davies, S. G. (1998) 'CCTV: A new battleground for privacy', in C. Norris, J. Moran and G. Armstrong (eds.) *Surveillance, closed-circuit television and social control*. Aldershot: Ashgate, 243-254.
- Dodd, V. (2002) 'Still life: for your eyes only', *The Guardian*, 14 September.
- Dubbeld, L. (2004) *The regulation of the observing gaze: privacy implications of camera surveillance*. Enschede: PrintPartners Ipskamp.
- Dyer, C. (2003) 'Suicide bid on CCTV may herald new privacy law', *The Guardian*, January 29.
- EPN and Telindus (2001) *EPN Dossier: cameratoezicht in de openbare ruimte*. Den Haag: Electronic-Highway Platform Nederland.
- Flaherty, D. (1999) 'Visions of privacy: past, present, and future', in C. J. Bennett and R. Grant (eds.) *Visions of privacy: policy choices for the digital age*. Toronto: University of Toronto Press, 19-38.
- Gray, M. (2003) 'Urban surveillance and panopticism: will we recognize the facial recognition society?' *Surveillance & Society*, 1(3): 314-330.
[http://www.surveillance-and-society.org/articles1\(3\)/facial.pdf](http://www.surveillance-and-society.org/articles1(3)/facial.pdf)
- Gutwirth, S. (2002) *Privacy and the information age*. Boston: Rowman & Littlefield.
- Hempel, L. and E. Töpfer (2002) *Inception report (Urban Eye working paper no. 1)*. Berlin: Technical University Berlin.
- Hert, P. de and S. Gutwirth (1995) 'Cameratoezicht, veiligheid en de Wet Persoonsregistraties: juridische denkoefeningen naar aanleiding van de Franse wet van 21 januari 1995 inzake veiligheid', *Recht & Kritiek*, 21(3): 218-250.
- Hoek, A. van, A. van Pel et al. (2000) *Focus op veiligheid: lessen en ervaringen van negen Nederlandse gemeenten*. Amsterdam/Den Haag: Van Dijk, Van Soomeren en Partners/Esyink Smeets & Etman.
- Homburg, G. H. J. and S. Dekkers (2003) *Cameratoezicht in de openbare ruimte*. Den Haag: College Bescherming Persoonsgegevens.
- Koops, B.-J. and A. Vedder (2001) *Opsporing versus privacy: de beleving van burgers*. Den Haag: SDU.
- McCahill, M. (2002) *The surveillance web: the rise of visual surveillance in an English city*. Devon: Willan.
- McCahill, M. and C. Norris (2002). *CCTV in London (Urban Eye working paper no. 6)*. Hull: University of Hull, Centre for Criminology and Criminal Justice.
- McCahill, M. and C. Norris (2003) *CCTV systems in London: their structures and practices (Urban Eye working paper no. 10)*. Hull: University of Hull, Centre for Criminology and Criminal Justice.
- Neyland, D. (2000) *Closed circuits of interaction? Representation and spatiality in high street CCTV*. Unpublished PhD thesis, Brunel University, UK.

- Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society: the rise of CCTV*. Oxford/New York: Berg.
- Opinion 4/2004 on the processing of personal data by means of video surveillance* (2004) Brussels: European Union, Article 29 Data Protection Working Party.
- Prins, J. E. J. (1998) Wet bescherming persoonsgegevens: agenda voor een discussie, *Privacy geregistreerd: visies op de maatschappelijke betekenis van privacy*. Den Haag: Rathenau Instituut, 213-245.
- Regan, P. M. (1995) *Legislating privacy: technology, social values, and public policy*. Chapel Hill/London: University of North Carolina Press.
- Regan, P. M. (2003) 'Safe harbors or free frontiers? Privacy and transborder data flows', *Journal of Social Issues*, 59(2): 263-282.
- Registratiekamer (1997) *In beeld gebracht: privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging*. Den Haag: Registratiekamer.
- Registratiekamer (2001) *Jaarverslag*. Den Haag: Registratiekamer.
- Smink, C. and A. Hamstra (1998) 'Burgers over privacy: beoordeling van privacy in relatie tot persoonsgegevens en informatietechnologie', *Privacy geregistreerd: visies op de maatschappelijke betekenis van privacy*. Den Haag: Rathenau Instituut, 187-212.
- Vedder, A. (2001) 'KDD, privacy, individuality, and fairness', in R. A. Spinello and H. T. Tavani (eds.) *Readings in cyber ethics*. Boston: Jones and Bartlett Publishers, 404-412.
- Weitenberg, A.I.M., E.J.M. Jansen et al. (2003) *Cameratoezicht: de menselijke factor*. Zeist/Apeldoorn: Politie & Wetenschap.
- Zoom: dossier cameratoezicht* (2000) Amsterdam: Buro Jansen & Janssen.