Christoph Müller and Daniel Boos
University of Zurich, Switzerland

«Zurich main railway station: A typology of public CCTV systems»

Presentation at the Conference
«CCTV and Social Control:
The politics and practice of video surveillance
– European and Global perspectives»
8th / 9th January 2004 in Sheffield (UK)

revised pre-print version for
«Surveillance & Society»

If we will find time and contemplation in the next future,
we will prepare a HTML version with pictures for <http://www.socio5.ch/ctrl/>

Abstract:

   Railway stations have become places between «public» and «private». In this exploratory case study, we are looking at the CCTV system at the Zurich main station, the largest railway station in Switzerland. This railway station is used by train passengers, by customers frequenting the station's shopping area, and by persons trespassing the station.

   Looking at different types of CCTV systems, we examine the motivations that have been leading to the installation of the cameras, about their functionality and their effects on passengers and customers. Based on our observations, we are going to present a typology of different uses of CCTV systems: (1) access control, (2) conduct control, (3) registering evidence, (4) flow control and the planning of deployment.

   As a conclusion, we will have a look at some future trends in the use of CCTV in railway stations, focussing on (a) individualization, (b) automatization, and (c) commodification. In the last part of our presentation, we are going to ask about the limits of the spreading of CCTV systems in railway stations, focussing on the efficiency on one hand and on several possibilities for opposition on the other hand.

Contact:

   Christoph Müller, sociologist <muellerc@socio5.ch>
   Daniel Boos, sociologist <boos@sociology.ch>

1. Introduction

In this exploratory study, taking the Zurich main railway station as an empirical starting point, we are going to develop a typology of video surveillance systems. The background of our presentation of the CCTV system in the Zurich main railway station is our involvement in the organization of so-called «Big Brother Awards» in Switzerland. Since 1998, such ironic «awards» are given every year to organisations or to individuals who are promoting surveillance and control. The idea is spreading quickly: Meanwhile, more than 30 «Big Brother Awards» ceremonies have taken place in more than a dozen countries.[1] In Switzerland, «Big Brother Awards» have been given away since the year 2000. When collecting nominations for these «Awards», we usually receive a lot of proposals regarding CCTV or single video camera systems for surveillance, e.g. in churches, on streets, in shops or on public places.

Awarding such prizes is mainly a *political statement*: We are focussing on clear cases where basic human rights are violated. The style is *parody*, the language is *irony*. While we still believe that such events are important, and we will continue awarding such prizes and «watching the watchers», things are usually more complex than they appear at first sight. As sociologists, we are also interested in the more complex backgrounds and relationships of surveillance and of control. That's why in spring 2001 we started to add another series of events to the «Big Brother Awards» ceremonies, by organizing discussions, panels, excursions, workshops etc. to discuss and to debate topics concerning surveillance and control. Within the scope of these events, we organized several public excursions to the Zurich main railway station, with some fifty persons joining us every time, including print media and radio.

We usually start our excursion right outside of the main station, next to the Swiss National Museum. As most cities, Zurich is famous for several reasons – one of the negative reasons being the so-called «needle park» located right behind the National Museum (Platzspitz). During the 1980s this park has been known as one of Europe's most important centres for the traffic and consumption of illegal drugs. It is said that, back then, the police used to observe the scene from a window of the museum, using a video camera.

Back then, the target for observation was *a specific group of people* (a minority, a stigmatized group), and *a specific problem* (trafficking, dealing and consuming illegal drugs). The observation was *covered* and its purpose was (a) to get an idea of «what is going on», on the social organisation and the social structure of the «scene», as well as (b) collecting evidence, and (c) planning and coordinating interventions: It was an *investigative tool*.

Today we find cameras all around the museum: Next to the entrance or in the court. They are *observing everybody*, not just some «specific social groups» or «subcultures» – and not for a specific reason, but for a *generalized prevention*.

---

[1] For an overview of international «Big Brother Awards» see <http://www.bigbrotherawards.org>.

2. Between private and public

Zurich is the largest railway station in Switzerland, frequented every day by about 350'000 persons. The station is an important «node» in the Swiss railway network, especially in the network of suburban trains, bringing commuters from and to work. About 1200 trains leave the station every day. But the station is not only a station: It is also a shopping centre with 117 shops, a «transit zone», a meeting point, even a «living room» for some people. One part of the station, constructed in the early seventies is called «Shop-Ville» (opened in 1970). This part has been modernized this year (2002/2003) and renamed to «Shop-Ville – RailCity».[2]

The railway station is a «functional space», a «transit zone» with a low level of «neighbourhood control». In sociological terms, as well as in legal terms, the Zurich main railway station is a place neither public nor private, but *semi-public*. Like in other semi-public places, and especially in stations, CCTV surveillance and control systems have been installed.[3]

A short history of privatization

At the beginning of the «railway age», about 150 years ago, all railway companies in Switzerland were owned by private enterprises and promoted by private «pioneers». Building and operating railway lines was not regarded as a duty of the new nation, founded in 1848. However, the private railway companies were not very successful in economic terms. A lot of them failed or even went bankrupt. Therefore, at the end of the 19th century, the nation-state (the Swiss «Confederation») bought these companies and began to operate them itself, with the national «Swiss Federal Railway Company» (SBB, CFF). Since the 1990s however, about 100 years after becoming a public enterprise, the SBB has been partly privatized, in the context of a general move to «market liberalism».[4]

---

[2] The largest part of the station is owned by the Swiss Federal Railway Company (SBB, CFF), including a shopping area called «Shop-Ville», opened in 1990. There is an older «Shop-Ville» part, opened in 1970, owned by the municipality of Zurich. During the planning of the renovation of this older «Shop-Ville», in the early 2000s, some shop owners asked the municipality to install a CCTV system. But the data protection commissioner of the municipality opposed these requests – mainly because the shop owners did not present convincing arguments for the necessity of such a CCTV system. Therefore, there are no cameras in the publicly accessible part of this older shopping area. However, there are video cameras inside some shops and all the cables for a CCTV system have been laid out – to be prepared.

[3] At the Zurich main railway station, a CCTV system of 46 black-and-white cameras has been installed in the early 1990s by the cantonal police (Kapo), called «Kapo-Cams», still operated today by the Kapo. In addition, there is a CCTV system with about 20 color cameras installed and operated by the Swiss national railway company (SBB), installed later, observing the underground railway tracks, and a system with 16 cameras in the business area of the SBB (Bahnreisezentrum). The systems are linked in one network, all wires leading to a central monitoring room inside the main station, with about 20 monitors. In addition, the wires are leading to the operating room of the SBB and to two police headquarters. The black-and-white images of the first system («Kapo-Cam») are not recorded, although – in principle – an old, analog system for recording would be available at the station's police headquarter, but this possibility has never been used (source: Regierungsrat). By contrast, the images of the newer CCTV network in the «Bahnreisezentrum» are systematically recorded. A map of the CCTV system as well as of other cameras in the Zurich main railway station will (soon) be available at http://www.bigbrotherawards.ch/kameras/.

[4] 100 years ago, the Swiss railways became a «Regiebetrieb» of the Swiss Confederation, in analogy to the «Post, Telephone and Telegraph» Company (PTT). Railways owned and operated by nation-states were common in other states in Europe as well, e.g. in Germany (Deutsche Bundesbahn, DB), in Italy (Ferrovie dello Stato, FS), or in France (Société Nationale des Chemins-de-Fers, SNCF). Today – unlike in some other states in Europe – the Swiss

The same process of privatization concerned the Railway Police («Bahnpolizei»), being responsible for the security in trains and stations and of the railway infrastructure in general.[5] In 2001, the functions of the «Bahnpolizei» have been given over to a new company called «Securitrans – Public Transport Security AG», which is a PPP (public private partnership) with the Federal Railway Company holding 51% of the shares and the private company «Securitas», the largest Company for Security in Switzerland, holding the other 49% of the shares.

3. A typology of CCTV surveillance

In order to understand the CCTV-system observing the publicly accessible space of the railway station, we first mapped the cameras and then started to order and to classify them, according to a grid of several *dimensions*:

- dummies or real cameras?
- focussing on private or on public space?
- used for prevention or for interventions?
- visible or hidden?
- recorded or not recorded?
- real-time observation or not?
- single cameras or networked systems?
- focussing on individuals or on collectives?
- with a systematic analysis or not? (i.e. «filtered» or not?)
    - matched with a data base?
        - as individuals or as a collective / crowd?
            - based on identity markers or on behaviour?
    - automated or «manual» matching with database?

Obviously, this multi-dimensional «room» of classification is rather complex.[6] For heuristic reasons, we classified the cameras in a next step in *four types*[7]. In doing so, we are following a *functional*

---

government still owns the majority of the shares. Since 1998, the SBB is organized as a company under special laws («spezialgesetzliche Aktiengesellschaft mit Sitz in Bern», see Bundesgesetz über die SBB, SR 74.231). In this context, different divisions of the Railway company have been separated, and the access to the rail infrastructure has been liberated. In addition to traditional private railway companies like the BLS or the «Mittelthurgaubahn» (now failed), there are only some few private companies operating trains on the Swiss railway network (like «Cisalpino» or «CityNightLine»).

[5] The Railway police (now officially called Public Transport Police PTP), based on a law of 1878, is a special case in the legal system of Switzerland, as it is the only Federal (State) Security Police. The last effort to introduce a Federal Security Police (BUSIPO, Bundessicherheitspolizei), has been rejected in December 1978 by 56% of the voters. However, there is an investigative Federal Police (FedPol), and some functions of a Security Police are performed by Military Police (Festungsschutz), Border Police (Grenzschutz), and supra-cantonal police forces, e.g. to protect the private «World Economic Forum» in Davos.

[6] Some of these dimensions are of importance in the legal framework: The Data Protection Commissioner of the Canton Zurich distinguishes three forms of video surveillance: (1) observing (without individualization; flow control), (2)

approach, asking «what could these cameras be good [be meant] for?».[8] By presenting this typology, we hope to deepen our understanding of the functioning of CCTV systems.

Generally speaking, we are considering cameras as a specific kind of «sensor». They are «sensoring» situations and movements: What are they sensoring? What for? We distinguish four types of camera use (see the summarizing flow-diagram at the end of the paper).

3.1. Type 1: Access control

One of the oldest purposes for the installation of cameras watching the «public space» is based on *access control*: Are you allowed to enter this door, this house, this area? Typically, such cameras are placed at entrances – of a house, of a bank, of a high-risk environment like a prison or a nuclear plant – or at the borders of a nation. They can be visible or hidden. They may register all movements or they may be used «on demand», when a «client» is asking permission for entering a special area.[9] In most cases, images of such an access control are not registered. The procedure is executed simultaneously. However, if the images of an access control are being registered, they may be used later on as an evidence for law enforcement (when something «went wrong», e.g. unauthorized access or stealing, see type 3 below).

Of course, cameras are not the only way of controlling access. Other systems include human solutions (personal bouncers) or material, hard-constructed solutions (e.g. doors, locks, ticketing systems).[10] Access may be controlled on the basis of the mere *appearance* of a person (e.g. as signalled by clothes), of his or her *behaviour* (e.g. drunken) or of personal *identity markers* or «tokens» (like passports, credit card batches, etc.).

During daytime, access to the main part of the Zurich railway station is controlled by personal means, that is: by guards and by police officers, as well as by social control in general, but not by

---

dissuasive (on special locations, persons are – at least in principle – indentifiable), (3) invasive (with a concrete target, collecting evidence), see BAERISWYL 2002, also EDSB O.J. A lot of other authors have pointed at the difficulties in ordering the various kinds of CCTV systems in different dimensions. For other typologies see NOGALA 2002, ARMITAGE 2002, COLEMAN / NORRIS (2000), POST 2002, and the 27 dimensions of «old and new surveillance» outlined by Gary T. MARX 2003.

[7] In starting from an empirical basis, we are more concerned with «real types» than with «idealistic» ideal types (Idealtypen) in the sense of the German sociologist Max WEBER. However, the distinctions between the different types are still following *analytical* purposes: In reality, it is more likely to find mixed forms than to find «pure» types.

[8] This does not imply that a certain camera «is functional» in the sense of «it is working», neither in relation to a CCTV system nor in relation to society in general. It can be dysfunctional or non-functional as well.

[9] A prototypical example is described by LOMELL, SAETNAN AND WIECEK 2003 (*urbaneye working paper nr. 9*): In the city of Copenhagen, video cameras are observing the entrance area of four public toilets, specifically to avoid the toilets (for the handicapped) being occupied by homeless people as shelters: «If a visibly handicapped person seeks to enter the toilet, he/she must signal for the operator's attention. The operator then signals the remote-controlled lock and buzzes the person in.» (p.58)
At least in Switzerland, there are more and more small cameras installed at the entrances of houses to control who is asking for entrance, often in addition to voice control and intercom. A traditional system is to look out of the window or to go downstairs to look who's knocking at the door.

[10] For an overview of human-object-chains and embedded «programs» in door opening systems, see LATOUR 1996 (in English: «The Berlin Key») – Cameras can be regarded as one element in a general process of «distancing» (Distanzierung), described by Norbert ELIAS as a «figuration» of modern life.

technical means.[11] In semi-public places, like railway stations, the rules of access regulation are not clearly fixed: definitions are «fluid» and open for interpretation. Therefore, enforcements of access blocking depend on assessments and judgements of the observants.[12] At the Zurich main railway station, there is an informal, not written «house rule» stating that visitors of the station have to own a valid train ticket. But at least for the shopping area, this access rule is too restrictive, because it would inhibit the possibility of someone just going to buy some goods in a shop. Yet, the rule is sometimes applied by security patrols, mostly as a formal argument to enforce the expulsion of «unwanted persons», mostly young people or alcohol addicts «hanging around».[13]

It is important to note that the cameras we observed do not enforce nor block access by themselves. They act partly (a) *as a tool* to support some monitoring personnel in their decisions to allow or to deny access, and/or mainly (b) *as a symbol* for a self-selection of access. The cameras may indeed have a dissuasive function, that is deterrence: Most observed cameras are visible, their presence is marked by signs.[14] The effect may be a self-selection of who is entering an area and who is not. The message of these cameras-as-signs is: «Watch out: If you are not allowed to enter this area, you better leave...»[15] The main function of this type of access control is a symbolic one: *These cameras are symbols and signs*. For this purpose, however, they *could be dummies* as well.[16]

It is interesting to note that most of the cameras in the (semi-) public space of the Zurich railway station are obviously not intended to control access: They are not specifically placed at strategic «obligatory passage points» like entrances, doors, or stairways. Instead, most cameras of the CCTV systems are placed in order to overview large areas, while some are focussing on smaller «hot spots» meant for special attention, but not entrances or exits.

3.2. Type 2: «conduct control»

Once access is allowed, cameras may be used in order to remind users of certain «rules of conduct» in the area. As explained in the context of access control, such rules are often not very clear in the case of semi-public areas. When entering the main railway station, there are some rather small signs informing about the rules of the station, especially the «do-not's»: Do not play, do not hang around, do not

---

[11] This is unlike to a lot of underground (metro) stations. During late night times however, the railway station is locked with material gates.

[12] There is a lot of literature on stereotypes influencing CCTV operator's attention, e.g., NORRIS 1997 or LOMMELL ET AL. 2003. Often, adolescent males are among the most observed, even more when their skin color is black and when they appear «scuffy». Another focus, as well based on stereotypes, is voyeuristic: targeting young women.

[13] However, in most cases, they do have a valid ticket, often a monthly or yearly ticket. Still, according to a newspaper report, there are about 100 persons expulsed from the main railway station every month (*Tages-Anzeiger 12/12/2001*).

[14] In autumn 2001, the Swiss Federal Data Protection Commissioner visited the main railway station, had a look at all the cameras, and suggested that the cameras should be marked with signs (EDSB 2002). Two years later, in autumn 2003, such signs have been placed at the entrances of the railway station. In addition, a specific regulation has be created as a legal framework for the use of surveillance cameras in stations and in trains (Videoüberwachungs-verordnung VüV-SBB, SR 235.742.2).

[15] If the images are registered, the additional message could be «..., else you will be registered ...».

[16] In fact, in a lot of other places we observed in the city of Zurich, some cameras are dummies indeed.

beg, do not...».[17] Cameras may be used for the same *symbolic* purpose, especially when they are visible and marked. This is an important «social control aspect» of cameras: They are reminding people that they are watched – or, to be precise: the cameras *give people the impression* that they are watched – and that they have to behave «nice». It is important to note that this «prevention effect» of cameras is not only focussing on drunken people, dropouts, beggars etc. – but it is *focussing on everybody*, including security guards and the police! So for example, the cameras in the ticket selling area of the station are not only intended to prevent robberies, but they are also directed towards the sales assistants: To remind them that they are not allowed to steal as well, and more generally that they have to behave nice and polite.

There are various reasons why companies are observing their customers and/or their employees:[18]

> (1) to create a «safe atmosphere» for customer relations;
> (2) to remind customers and employees of discipline;
> (3) to prevent and to detect criminal activities;
> (4) to check out workplaces and workers for efficiency;
> (5) to plan processes and to optimize procedures, especially
> to promote consumption and to reduce delay times.

Although some of these purposes require monitoring or even recording the images, for the purposes (1) and (2) it is sufficient to make customers and employees *believe that* they are observed. People tend to do things in private they would not do in public (and vice versa!). «In public» means: when they believe that other persons are (possibly) observing them. This social regulation of behaviour is not performed by cameras, but it is based on complex cultural rules and norms. Therefore, it varies in different settings as well as in history. Although cameras do not regulate social conduct in public by themselves, they may expand the number of situations where people believe that they are observed.

In a broader approach, crime prevention can be seen as just one special case of «social order prevention» in general. Every regulation of what is appropriate or not has to be based on distinctions between «good» and «bad», between «normal» and «abnormal». This evaluation is not done by cameras, and it is done only in exceptional cases recurring to written laws. There are a lot of situations where social behaviour at a specific place and time may be valued in a negative way, although not being «criminal» in the sense of the law – e.g., kissing, talking aloud or running.

Although the cameras *do not define* what is appropriate or not, and although they *do not enforce* good conduct nor block bad conduct by themselves, they may have effects on social conduct: As a positive,

---

[17] A previous version of these rules was headed «So ist es richtig:» – which means «these are the rules:». The starting sentence «Willkommen im Bahnhof» (Welcome to the station) is meant to mark the ownership and the power to define the rules of a certain area: Who else would welcome other people if not the owner or the host? However, the legal base for this type of «house law» (Hausrecht) is quite small.

[18] In the strict sense of the law, surveillance of employees on their workplace is against the workers' rights. However, there are exceptions, e.g. for people working in dangerous or in in highly sensitive areas.

«encouraging» effect, cameras may reinforce attempts to behave as socially desirable persons, while as a negative, «discouraging» effect, they may *reinforce self-restrictions and self-discipline.* This is in accordance with the mechanism of the Panopticon as described by Michel Foucault: In the Panopticon, prisoners are aware of the fact that they may constantly be observed, but they never know if they are really observed.[19] This may lead to a raised awareness and maybe to adaptations of behaviour. As long as customers of the railway station *believe* that they may be observed, they may adapt their behaviour *as if* they were observed. This is a general form of «deterrence» and of «controlling conduct».[20]

In most cases, cameras with the purpose of «controlling conduct» are functioning by way of *self-control* and *self-restriction*, following an «appellative approach»: They *remind* people to behave in a certain way and not in another way. In this sense, as reminders, they have – as in the case of access control – a *symbolic value*. Cameras-as-signs raise awareness in public spaces and remind people of «appropriate behaviour» *by symbolical means*.

Sub-type 2bis: «Feeling safe» and raising awareness

Successful «social order prevention», resulting in reductions in «risks» of unexpected behaviour, may lead to a general feeling of being in a safe environment. This can be regarded as a subtype of «conduct control»: If social discipline is successfully appealed to by cameras-as-signs, and awareness is risen, then customers and employees may «feel safe», because, if people act «nice», that is: in the way they are socially expected to act at this place and time, the space is perceived as controlled, «quiet» and protected. Of course, cameras-as-signs are not the only means potentially leading people to «feel safe». Other means include architectural design, lightening, the use of «friendly» and bright materials, as well as other symbols and signs.[21]

Reminding people of being observed, and thus appealing to good conduct does not only affect potential offenders, who may become more aware of the «threat of potential surveillance», of potential detection and intervention, but also potential victims, who may become more aware of potential danger and therefore may try to present themselves as «inoffensive» to each other. Consequently, the area makes a friendly and inoffensive impression.

---

[19] Until the renovation of the older shopping area in the Zurich main railway station («Shop-Ville», renovated 2002/ 03), a prototype of a simple «panoptic» surveillance system was installed: A one-way mirror allowing the staff of a «control room» to watch the customers while they could not see the staff. Ironically, the one-way mirror was installed right in front of the station's public toilet, which was a well known meeting point for male homosexuals and for male prostitutes. However, the mirror has not been installed by the police, but by the technical services of the municipality, and the reason was probably not to target the toilet (users).

[20] Again: This is not to say that the functions are fulfilled in reality. Cameras may lead to various forms of displacement. For an overview of six forms of displacement, see COLEMAN / NORRIS p.156ff.

[21] At the Zurich railway station, there is a huge sculpture hanging in the main hall, called «L'ange protecteur» (i.e. protecting angel or guardian angel) by the sculptor Nikki DE SAINT-PHALLE. Ironically, this sculpture has been sponsored by «Securitas», the largest private security company in Switzerland. Yet, we personally never felt very much protected by this «Angel», on the contrary: we were more afraid of the risk that the wires fixing the angel at the top of the hall could suddenly tear...

However, this type of symbolic CCTV function is based on a range of *assumptions*: Cameras only work as a means of «conduct control» as long as people believe that the cameras are real (and not dummies), that they are working properly, that they are being monitored by someone, that this «someone» would organize an intervention, if necessary, or at least that the images would be recorded and could be used as evidence for ex-post sanctions.[22]

It is important to repeat that the cameras do not directly *enforce* discipline! As in the case of «access control», cameras used for «conduct control» often act as *signs or symbols*. To enforce discipline, or to block access, humans are needed, be they professional guards or «neighbours» intervening.

3.3. Type 3: «registering evidence»

Both in regards to *access control* (type 1) and to *conduct control* (type 2), «wrong conduct» may be sanctioned, e.g. when entering an area without permission, or when behaving in an «inappropriate way», maybe even in a criminal way. In order to sanction such behaviour, proofs or evidence are needed.[23] If the images of a camera are recorded, then these images may be used as evidence or even as proofs, eventually leading to sanctions like punishment. If they are not recorded but have been monitored by humans, then these humans may act as witnesses.[24]

One well-known example of registering evidence are cameras placed at or near Automatic Teller Machines (ATM, «Bancomaten»): At least with some ATMs, every time someone starts an interaction or a transaction with the machine, a picture of the user is taken and recorded. In cases of fraud, this picture may be used as evidence.

Another example are cameras on railway tracks. One argument for installing them could be to prevent suicides, as some psychologists have noted that people intending to commit suicide are often strolling around for some time and hesitating before «doing it». If this kind of «abnormal behaviour» is detected, security guards may become aware of such suicide attempts and may organize an intervention. The general argument here is «caring for another».[25] Yet, there could be another reason for the installation of cameras on railway tracks: Given the relatively easy possibility to push someone in

---

[22] «Increased perceptions of safety in CCTV areas might increase people's presence, deterring potential offenders.- CCTV may also remind people to be more cautious so that they are less easily targeted by crime.» (POST 2002) On the other hand, people may feel insecure in places with CCTV surveillance, as they may interpret cameras as a marker for an unsafe area. Further, as a parallel effect of an increased subjective impression of «feeling safe» at places with CCTV observation, there may be a decrease in the same subjective impression in places without CCTV: People may get the impression that every place without a camera is an insecure place.

[23] However, this is not always the case, as we know, e.g. in regards to the last intervention in Afghanistan or in Iraq.

[24] As noted in the UK POST-Report, there are several problems using CCTV images as evidence, i.e. (a) poor image quality, (b) difficulty to locate evidence from (analog) CCTV, (c) technical difficulties, because of different formats, and (d) the problem of authenticity of CCTV images. Further, is seems that CCTV images have a poor reliability in identification of persons: Witnesses are often confusing people seen on CCTV images. «Despite this, people tend to be confident in their decisions, even when incorrect.» (POST 2002).

[25] Similar types of «caring surveillance» can be found in hospitals, especially at «intensive-care units», where patients are surveilled by video cameras and a range of others sensors. In most cases the sensors and cameras are used as a tool helping to decide about interventions (see type 4 below).

front of a train, the images may be used as evidence to find out if someone really committed suicide or has been murdered.[26]

A lot of cameras are used for collecting evidence, especially when recording images without watching them in real-time. Typical examples of cameras for collecting evidence are targeting on (a) theft, robberies and fraud, (b) vandalism, damage to property, (c) personal attacks, (going up to killing), (d) «terror» (in the sense of: threatening the public). In such cases, cameras are more than simple signs, more than reminders: They are *instruments, tools*. The evidence may be used for planning an intervention (see below) or for ex-post sanctions.[27]

Cameras of this type are not excluding the first two types, on the contrary: They may be used to reinforce the symbolic, appellative aspect of the cameras-as-signs: As people may expect that the images are being recorded, they may avoid the area observed or adapt their behaviour.

3.4. Type 4: «flow control» and deployment

The fourth type is about planning interventions. This is maybe the oldest form of video surveillance of public places. It is used since the early 1950s in order to control street traffic of cars, especially in tunnels. When, in a certain setting, «something goes wrong» or goes «out of order», cameras and CCTV systems may be useful instruments in planning interventions. This seems to be the main pur-pose of the «Kapo-Cam»-CCTV system in the Zurich main railway station – and it is also the main reason the persons responsible themselves are presenting for the system:[28] Especially the underground parts of the station are characterized by a restricted visibility, their architecture is rather confusing. When something special happens, e.g., a major accident or a fire, then it is important to know which accesses are to be closed, which accesses are open for intervening fire brigades or ambulances – to inform and to conduct both helpers and other people. Other examples of «unusual events» are terrorist attacks (or even warnings and threats), demonstrations, fights etc. One typical effect of unusual events, when something is going «out of the normal order» and «out of control», is a public «panic». From the perspective of intervening forces, public panics are calling for *crowd control* or at least for *crowd monitoring*.

Cameras of the fourth type can be used in a *preventive* way as well, e.g., to observe the flow of a group of Hooligans or of demonstrating people. The basic principle of CCTV-cameras used for

---

[26] There is another parallel to hospitals, e.g., in regards to maternity rooms, in order to obtain evidence in cases of child abduction, or, – more general – of murdering by nursing staff, by relatives or by enemies. One classical case of cameras-for-collecting-evidence is the abduction of James Bulger near Liverpool in February 1993, where an image from a surveillance camera of a shopping centre became an «icon», see WEAVER 2001.

[27] There is a trend to install cameras inside the coaches of public trains as well, in order to record evidence. According to the recommendations of the Swiss Data Protection Commissioner, such camera images may be stored for up to 24 hours, in special cases up to 48 hours (EDSB oJ, see also BAERISWYL 2002). Except in some small pilot studies, there are no results on the efficiency of such cameras. Given the relatively easy possibilities to manipulate digital images, the value of camera images as «proofs» may be contested. In most legal cases, they have been used merely as evidence, often convincing a defendant to confess.

[28] Sources: REGIERUNGSRAT_ZUERICH 2001, EDSB 2002 and interviews with security officers of the main railway station.

this type is «*flow control*».[29] The monitoring does not have to lead to interventions in every case, but is to be seen as *a command and control tool for planning interventions and sanctions.* Once incidents are detected, the cameras may be used to coordinate police response.

A minor example for intervention planning are the *emergency posts* («Notrufsäulen») in the station: Almost every post is watched by a «Kapo-Cam». When someone pushes the alarm button, the operator may switch on the camera to see what is going on. The operator then may decide on the necessity to send a patrol or not. Is someone offended or in danger? Is someone just asking a simple question? What does it mean if the button has been pushed but nobody is talking? Are there children playing or is it a mute person? Is someone about to die? Similar to the case of mass interventions, the CCTV system is used in order to support the intervention planning of the security guards, the police, ambulances and fire brigades: Where should the patrols go to? How many patrols should be directed to these places? From the perspective of deployment, this use of cameras as auxiliary decision tools is useful to avoid sending patrols because of «false alarms».

Correspondingly, this type of cameras can be used *to assure that no intervention is needed*, that «everything is working fine». In another, smaller railway station in Zurich, the cameras observing the railway track are routinely used as «additional, remote eyes»: As the railway track follows a curve, the cameras are a working tool for the controllers to check if the trains are ready to leave the station.

In order to be able to plan and to coordinate an intervention, the first important feature is a real-time transmission of the images collected by CCTV cameras.[30] The images do not have to be recorded in order to make the system work, indeed, in the case of the Zurich main railway station, images of the «Kapo-Cam»-System are not recorded. The focus is mainly on *collectives*, on *crowds*, not on individuals.[31]

As Müller (2002) noted, there is an important drawback of such CCTV systems working as «additional eyes» for police forces: While allowing them to plan their interventions, these systems may at the same time increase the public's expectance that the police will intervene every time when the public believes that there is a necessity for an intervention. This may result in a increased pressure on police forces to intervene (otherwise, they may loose credibility) – one of several reasons why police forces could have a low interest in «seeing everything».

---

[29] In this context, we use the term «flow control» for flows of persons, not of data. This is a much narrower use of the term than the one presented by DELEUZE 1990 and by HAGGERTY / ERICSON 2000, respectively.

[30] If the images are recorded, they may be used at a later stage to evaluate the interventions, to learn from errors etc.

[31] In our interviews, the operators reassured us that they were not at all interested in singular, individual persons. However, the system, in principle, allows for the possibility *to follow a specific person* through the area of the station and maybe to plan an intervention at a specific location, e.g., an arrest.

3.5. Additional types

The typology we presented so far is not complete. Additional types of CCTV not considered here include:

(a) Forms of recording images without an immediate intervention, mainly for purposes of planning, like counting and flow statistics of car traffic or of customer traffic in a shopping centre, analyzed *ex post*, mostly for marketing strategies and other optimizing schemes.

(b) Forms of collecting and archiving images of individuals, like pictures collected by automated passport-cameras, or by the Swiss Railway Company in order to produce «seasons tickets».

(c) Forms of tracking information on the basis of individuals, and «data mining». (In general, we did not consider the merging of images and other types of data in databases.)

(d) Forms of commodification and of commercialization of images (e.g., selling CCTV footage to TV-stations).

4. Summary, trends and limits

From our observation of the CCTV-system at the Zurich main railway station, we distilled four types of functionalities of surveillance cameras. All these types are about «flow control» and about regulation. We summarized the different types in the flow diagram in table 1. A lot of cameras and CCTV systems are not «pure», but mixed types.

The main function of a lot of cameras is «signing» – they are a special kind of «sign» or «symbol». This is the case for the types 1 (*access control*) and 2 (*conduct control*). However, some types have additional features, especially when the images are recorded (as for *collecting evidence*, type 3) or when the cameras are used as «remote eyes», e.g. for *planning interventions* (type 4). Thus, we can describe some types as *cameras-as-signs*, while others are *cameras-as-eyes*.

Thus far, we tested our typology in three case studies: (a) for the CCTV-system at the Zurich main railway station, (b) for about 50 cameras observing semi-public areas in a selected part of the city of Zurich (Langstrasse, Kreis 4), as well as (c) for the case of car traffic control including number plate recognition. We believe that the typology is useful both for camera systems targeting collectives (crowds) as well as for systems targeting individuals.

In general, we identify *three future trends* in the use of CCTV systems (as well as of data collection in general): *(a) individualization, (b) automatization,* and *(c) commodification*. Applying these trends to our typology, we expect a *merging* of the four distinguished types for the future, and feedbacks from one type to another. Cameras and CCTV systems are becoming more and more *multifunctional*. This is especially true when images are getting digitized and combined with indivi-

dualizing and automated software systems and databases. Cameras then become elements in a broader network of sensoring devices. This could take the form of automated face recognition, car licence plate recognition, or any other automated sensoring system, like tracking by cell mobile phones, by RFID or similar chip systems.[32] The merging and feedbacking may take different forms:

Firstly, a simple system could consist in an automated *merging of flow control and access control,* resulting in an emergency system for subways or tunnels: If a fire is detected, access will be denied.

Secondly, on an individualized base, *access control can be linked with registering evidence and intervention planning*: A specific person entering an area may be triggering an intervention. One example is the face recognition system installed in Newham, with a «watch list» of «special persons». Similarly, if a car without the proper permission to enter the inner city ring of London is singled out, an automated intervention may happen, like blocking the car's electronic system or sending the owner an invoice, at the same time registering the car owner in a database. Interventions and sanctions may be deployed only *ex post*, or immediately, like stopping a person not allowed to enter a specific area, by using appropriate techniques.[33]

Similarly, *using pattern recognition, a detected «abnormal behaviour» may lead to an alarm and trigger interventions* (as used in test cases for the observation of parking lots). Or a person not respecting the «rules of good conduct» may be marked for a later intervention – e.g., applying a «three strikes» sanctioning system. Conversely, «inappropriate conduct» may lead to the recording of CCTV images as evidence.[34]

And finally*, flow control may get coupled with conduct control.* When adding audio channels to the video system, a person or a group of persons behaving in an «inappropriate way» may be warned by a guard: «Please keep to the right!» – thus reminding the local «rules of conduct».

In all these cases: The norms against which a person is checked may be *based on individual markers*, registered in data bases, or on *behavioural markers*, as compared with algorithms against a defined «normality». Every checking must be based on a reference, a «norm» in the sense of a «normality»: If behaviour is not normal, it is filtered out. Although the technical systems for pattern recognition are not very reliable yet, this may change quickly.

We may therefore ask about the *limits* of spreading surveillance systems. Taking the CCTV system in the Zurich main railway station as an example, we identity the following *restraining*

---

[32] For a tracking system of railway travellers: Until recently, the Swiss Federal Railway Company intended to introduce a contactless, automated, individualized ticketing system using a (RFID-) chip card called «EasyTicket». This would have allowed the company to track the passengers, registering their movements and billing them accordingly. For the moment, however, the Swiss part of the project has been postponed.

[33] A simple technique is a «unit separator for persons» (Personenseparator); a more sophisticated one could be a net. Examples for automated access control by references to data bases are iris scans in «high security areas», at the Airport Schipohl in Amsterdam (since October 2001, for «frequent flyers») or even in a discotheque in Zurich (for «members only»). At the Zurich Airport, there is a pilot project running on biometrical face recognition (Farec). However, such systems still tend to be unreliable – see the failure in Tampa / Florida (STANLEY / STEINHARDT 2002, ACLU-Report).

[34] According to the UK POST report, police patrols observing the British Parliament sometimes ask CCTV operators to record images of a specific camera in order to collect evidence in the case of «dubious events» (POST 2002).

elements: (a) technical limitations and «failures», (b) opportunity limits («feeling safe» vs. «feeling observed»), (c) inefficiency («CCTV does not resolve problems»), (d) costs (including opportunity costs) and (e) finally opposition, by customers, consumer protections organisations, trade unions, data protection commissioners or sabotage activists.

5. Future research

Having identified four functional types of CCTV systems and extrapolated some future trends and limits, we propose the following questions for further research:

– *What is new with CCTV systems* – compared to «traditional» social control in semi-public spaces? What exactly are the new elements of the four functions performed by camera systems? How have these functions been performed before the rise of CCTV systems?

– *What elements are changing* if CCTV-systems are getting more and more automatized and are including more and more individualizing features? – Which of the observed types are going to be merged in what way?

– *How are CCTV systems going to be merged* with other surveillance systems, especially with automated, individualized tagging systems as implemented in mobile telephones or with RFID and other chip cards?

References

Armitage, Rachel (2002) "To CCTV or not to CCTV? A review of current research into the effective-ness of CCTV systems in reducing crime." London: Nacro (Report – «Community safety practice briefings»). online: http://www.nacro.org.uk/data/briefings/nacro-2002062800-csps.pdf

Baeriswyl, Bruno (2002) "Videoüberwachung durch öffentliche Organe. Grundlagen." Zürich: Datenschutzbeauftragter des Kantons Zürich, online: http://www.datenschutz.ch/bericht_videoueberwachung_2002_07_v_2.pdf

BBA-CH, Big Brother Awards Switzerland (2002) "A Map of Surveillance Cameras in the Zurich inner city district 'Kreis 4'.", prepared for *http://www.bigbrotherawards.ch/kameras/*.

BBA-CH, Big Brother Awards Switzerland (2003) "A Map of Surveillance Cameras in the Zurich Main Railway Station." prepared for *http://www.bigbrotherawards.ch/kameras/*.

Coleman, Clive, and Clive Norris (2000) "CCTV and crime prevention: questions for criminology (= Chapter 6)." Pp. 146-175 in *Introducing Criminology*, edited by Clive Coleman and Clive Norris. Cullompton and Portland: William Publishing.

Deleuze, Gilles (1990) "Post-scriptum sur le sociétés de contrôle." *L'autre journal*.

EDSB (2002) "Videoüberwachung im Hauptbahnhof Zürich (= Kap.3.2.2. des 9. Tätigkeitsberichts)." Bern: Eidgenössischer Datenschutzbeauftragter, online: http://www.edsb.ch/d/doku/jahresberichte/tb9/kap4.htm#322

EDSB (o.J.) "Leaflet on video surveillance by private individuals." Berne: Eidgenössischer Datenschutzbeauftragter, online: http://www.edsb.ch/e/doku/merkblaetter/video.htm

Haggerty, Kevin D., and Richard V. Ericson (2000) "The surveillant assemblage." *British J. of Sociology* 51:605-622.

Latour, Bruno (1996) *Der Berliner Schlüssel*. Berlin: Akademie-Verlag.

Lomell, Heidi Mork, Ann Saetnan Rudinow, and Carsten Wiecek (2003) "Flexible Technology, Structured Practices: Surveillance operations in 14 Norwegian and Danish organisations (urbaneye wp9)." RTD-Project "Urbaneye", online: http://www.urbaneye.net/results/ue_wp9.pdf.

Marx, Gary T. (2002) "What's New About the 'New Surveillance'? Classifying for Change and Continuity." *Surveillance and Society* 1:9-29. online: http://www.surveillance-and-society.org

McCahill, Michael, and Clive Norris (2003) "CCTV in London (urbaneye wp6)." RTD-Project "Urbaneye". online: http://www.urbaneye.net/results/ue_wp6.pdf

Müller, Henning Ernst (2002) "Zur Kriminologie der Videoüberwachung." *Monatsschrift zur Kriminologie* 85:33-46.

Nogala, Detlef (2002) "Ordnung durch Beobachtung: Videoüberwachung als urbane Einrichtung." Pp. 33-54 in *Jahrbuch StadtRegion 2002. Schwerpunkt: Die sichere Stadt*, edited by Christine Hannemann, Werner Petrowsky, and Jörg Pohlan. Opladen: Leske+Budrich.

Norris, Clive (1997) "Surveillance, Order and Social Control. End of Award Report." Hull: http://www.aclu.org/issues/privacy/CCTV_Norris.pdf.

Norris, Clive, and Gary Armstrong (1999a) "CCTV and the Social Structuring of Surveillance." Pp. 157-178 in *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*, edited by Kate Painter and Nick Tilley. Monsey (NY): Criminal Jurstice Press.

Norris, Clive, and Gary Armstrong (1999b) *The maximum surveillance society. The rise of CCTV*. Oxford (UK): Berg.

Norris, Clive, Jade Moran, and Gary Armstrong (Eds.) (1998) *Surveillance, closed circuit television and social control*. Aldershot: Ashgate.

POST (2002) "CCTV – postnote nr. 175." London: POST – Parliamentary Office of Science and Technology, online: http://www.parliament.uk/post/pn175.pdf

Regierungsrat_Zürich (2001) "Überwachungskameras der Kantonspolizei im Zürcher Hauptbahnhof – Antwort vom 28.11.2001 auf die Anfrage (Motion) von Bettina Volland und Anna Maria Riedi vom 10.9.2001 (KR-Nr: 284/2001)." Zürich: Kantonsrat des eidgenössischen Standes Zürich. (= Response of the Cantonal Government of Zurich to a parliamentary question on the CCTV system in the Zurich main railway station), http://kantonsrat.zueri.ch/task/geko/k01/gk01284.htm)

Stanley, Jay, and Barry Steinhardt (2002) "Drawing a Blank: The failure of facial recognition technology in Tampa, Florida." ACLU, online: http://archive.aclu.org/issues/privacy/drawing_blank.pdf

Weaver, Thomas (2001) "The Eye of the Genius. Notes on Bentham and the Bulger case." in *http://nachdemfilm.de/no3/wea01eng.html*.

Appendix: Table 1:

A typology of CCTV systems
Christoph Müller, Daniel Boos
Zürich, Switzerland, January 2004

1) access control

allowed

not allowed

2) conduct control

exit

appropriate

not appropriate

2b) (self-)discipline, «awareness»

3) collecting proofs / evidence

«feeling safe»

4) interventions, c&c, sanctions