

# Social Sorting in the Early 21<sup>st</sup> Century

## Video Surveillance and Governance

VOLKER EICK

It goes without saying that consolidating state power surveillance is on the agenda of the ruling classes.<sup>1</sup> Elaborating techniques of social control has always been of high importance. While enhancing efficiency and productivity, surveillance also focusses on a functioning bureaucracy to maintain power and control. Furthermore, functioning surveillance systems are even more important in times of economic crisis and during times of war.<sup>2</sup>

It is the rise of new technologies that has enhanced the opportunities for the main aims of surveillance such as control and discipline. Technology does both: enabling globalisation processes and widening the opportunities for social control. With the ongoing fragmentation of advanced industrialised societies due to the “neoliberal project”,<sup>3</sup> a new trend emerges, from ‘simple’ control and discipline of people to identifying and classifying them: the social sorting of people.

Developments in technology such as innovations in transportation, information and (tele)communication have led to an increasing free flux of capital, goods and (enabled, forced, or prevented) the migration of people. Under neoliberal conditions, this globalisation process is to be described as both uneven and unjust on different scales – global, national, regional and local. While the ‘global’ meets the ‘local’ and vice versa, globalisation is a more precise term. Video surveillance started its career on the local level trying to improve traffic (and crowd) control. At the present time, video surveillance (CCTV: Closed Circuit Television) is on all scales one of the most prominent instruments to control, discipline, identify and sort people.

“She uses a scale of 100 to 2 to make it easier to transcribe the information. Each sector has its own command and its own surveillance system. Small cameras are fixed to the ceiling. Elena imagined the circuit and the surveillance room. Once she had seen the surveillance centre at New York’s Penn Station. All the commuters were screened in corridors and platforms, and a grease-painted, blue-dressed policewoman with black glasses (a real policewoman) worked alone in a white basement ring rounded by TV screens; sitting in a swivel-chair she monitored the screens covering the walls. A microphone pinned at her blouse transmitted her voice and her breath. In the toilets perverts cooled down to their perversions; she supervised and informed the police squads in action one floor above. Three policemen were kicking a junkie who lay in a corridor leading to platform six.”

(*Die abwesende Stadt* Ricardo Piglia 1994, p. 99)

### **Neoliberalisation: The Fordist Big Brother and his Post-Fordist Sisters<sup>4</sup>**

Faced with the decline of profitability of the Fordist mass-production industries and the crisis of the Keynesian welfare system, Western industrialised nation-states began to dismantle the basic institutional components of the postwar structures and pushed forward – first ideologically than practically – extended market discipline, competition, and commodification throughout all sectors of society. This process of neoliberalisation is neither monolithic in form nor universal in effect; instead it is highly uneven both socially and geographically. This is why the management of (in)security, (dis)order and (crowd) control is not the same in every nation-state (or even locality). Although it is obvious that for the last twenty years the neoliberal project has failed to establish a coherent basis for sustainable capitalist growth, it nonetheless transformed the institutional infrastructures upon which the Keynesian welfare state and its Fordist structure was grounded.

“In short, in this North Atlantic zone [North America and Western Europe] at least, there seems to have been a shift from the pattern of deregulation and dismantlement so dominant during the 1980s, which might be characterised as ‘roll-back neoliberalism’, to an emergent phase of active state-building and regulatory reform – an ascendant moment of ‘roll-out neoliberalism’” (Peck and Tickell 2002, p. 384).

Or, as Lea (1997, p. 49) puts it, “Post-Fordism’ can be another name for the fact that in order to restore the conditions for profitable accumulation, capital must intensify its attack on the working class”. This intensified attack comes with a new model of regulation; first focussing on the local level and second introducing governance instead of government. In order to effectively deal with the complexity of contemporary social problems on the local level, stakeholders from all spheres of local society are brought together to cooperate with the municipality as well as with each other. With the devolution of welfare production, the blurring of borders between traditional policy fields such as labour market policies, economic development, social and security policies is obvious. In all sectors that are involved in welfare and, increasingly, security production (public, private, voluntary and nonprofit), shifts in values, habits and organisational structures (e.g. an increasing market orientation) can be identified. All this is happening in an environment increasingly defined by devolution, leading to a workfare governance model (Eick 2002).

The ongoing commercialisation and competition that comes with “roll-out neoliberalism” in a glocalising world also leads to the blurring of borders between commercial, police and military activities that now appear as a “criminal justice military industrial complex”. Video surveillance started within the Keynesian welfare state by defining the “citizen as a security risk” (Narr 1977). The second wave of CCTV takes into account the disruption of society that forces all individuals to take risks in areas such as labour, welfare, health, safety and tries to reconfigure and readjust its outcomes.

“MetaCops Unlimited is the official peacekeeping force... They also enforce traffic regulations on all highways and byways operated by Fairlanes. Inc.... MetaCops’ main competitor, WorldBeat Security, handles all roads belonging to Cruiseways, plus has worldwide contracts... WorldBeat is smaller than MetaCops, handles more upscale contracts,

supposedly has a bigger espionage arm – though if that's what people want, they just talk to an account rep at the Central Intelligence Corporation.

And then there's The Enforcers – but they cost a lot and don't take well to supervision. It is rumoured that, under their uniforms, they wear T-shirts bearing the unofficial Enforcer coat of arms: a fist holding a nightstick, emblazoned with the words SUE ME."

(*Snowcrash* Neal Stephenson 1992, p. 41-42)

### **No Need to Smile: Digital Discrimination and the Biometric Back Office**

Closed circuit television has a history of almost fifty years now. In Germany, the first cameras in public space were installed in the late 1950s – firstly in Munich in 1958 followed a year later by Hanover, where the government eventually installed the first 25 pan-tilt-zoom cameras in a city-centre pedestrian zone in 1976. While most of the cameras that were installed in the period between the late 1950s and mid-1960s focussed on traffic management, they have been used to target 'marginalised' groups since then. Nowadays, they are conquering the whole range of everyday life. In 1976, special police squads started surveillance of demonstrations; the so-called "Action Paddy" run by the Federal Office of Criminal Investigation (BKA), the secret services Federal Intelligence Service (BND) and the Office for the Protection of the Constitution (BFV) tried to identify members of the so-called terrorist group Red Army Faction (RAF) in the surroundings of the NATO headquarters in Heidelberg. The attempt failed and the project was stopped after a period of six months. Meanwhile there are countless video surveillance projects all over Germany: playing grounds are monitored as well as welfare centres, public employment offices as well as schools, public transport systems as well as residential areas, and workplaces as well as shopping malls. Obviously, this list is incomplete (Hempel and Töpfer 2002; Eick 2003).

While this development was pushed forward by the federal government and commercial security companies during the 1960s and 1970s, since the early 1990s video surveillance has been promoted, consumed or advertised by almost every part of current society,<sup>5</sup> and thus has invaded all its fields, including private and public spaces as well as the Internet, which itself has to be seen as a surveillance tool.

The relations between CCTV and interventions in urban space are both economic and political. In the UK, for example, the introduction of video surveillance into the public spaces of (inner) cities and towns has been an attempt to support these areas in the face of growing competition with out-of-town retail parks that have been seen as relatively safer than the inner city areas (Fyfe and Bannister 1998). The now-privatised German railway company DeutscheBahn organises social sorting by means of video surveillance both to exclude marginalised groups and to compete with airlines that connect almost every major city in Germany and surrounding countries since the early 1990s. Nowadays, Germany's main railway stations are high security zones designed like the current panoptical airports (Eick 1998). In the US, the configuration of the tightly managed, security-conscious corporate plazas reflects concerns that the presence of social difference will have a negative financial impact. As Flusty notes, "A plaza's white-collar user mix adulterated by vagrants or a janitor's family on a picnic [means] a loss of prestige before the 'business community' and a resulting loss of clientele" (1997, p. 58). Evidently, city streets that have been sites and

symbols of (democratic) protest and politics since the beginning of city building continue to be a source of anxiety to the leading class fearful of challenges to the very social order and power structures they want to sustain. According to managers and watchers of CCTV systems, we can easily describe video surveillance as a masculine or patriarchal technology. A gender structure is to be identified, not only because women use more time for shopping than men; a majority of them also use public transport, whereas men – whether police or private guards – are the watchers behind the camera. And even more, as Koskela states, “Women do not rely on those behind the camera because of the reproduction of patriarchal power. In urban space women are likely to be the ones who are looked at, the objects of the gaze. Furthermore, one of the very reasons for women’s insecurity is their ‘exaggerated visibility’. Paradoxically, women are marginalised by being at the centre (of the looks). Surveillance can be a way of reproducing and reinforcing male power. It is opening up new possibilities for harassment. Surveillance can be understood as the ‘re-embodiment’ of women, as an ‘extension of male gaze’” (1999, p. 13).

Therefore, categorisation – social sorting – by video surveillance and related technologies is not only particularly prejudicial, relegating ‘some’ to second-class citizens because of their social status, color, ethnic background or religion, but reproduces patriarchal structures as well.

“After this he might have to get out of the city for a while and live somewhere else. Somewhere simple, where the only smart building was the local library... Busiest of all was the Marounuchi, the financial district and electronic Mecca, where crowds of screen gazers jostled their way along the communications thoroughfare like so many holiday makers heading for the beach. He liked this place most of all, for here the luminous world reached its apogee and here was most for him to steal – whole batches of files of patents, statistics, research, analyses, sales figures and marketing plans – a seemingly limitless store of weightless wealth.”

(Gridiron Philipp Kerr, p. 407-408)

### **From Suspicion to Seduction: The Conversion of Mixed Interests**

One has to highlight the very different spaces that are covered by CCTV in order to understand that its existence is not only to guarantee the ruling class’ power, but also for profit: while it is true that political fears are an important driving force in introducing CCTV, it is also obvious that the current multi-stakeholder use of CCTV develops – following and transforming Jessop’s (2001, 2002) arguments – what can be described as a shift from a Keynesian ‘security state’ to a Schumpeterian ‘panic regime’. The multi-stakeholder use leads to what David Garland (2001) calls a “culture of control”.<sup>6</sup>

In the UK, it is already estimated that with respect to camera surveillance in public and private spaces there is one camera for every eight persons. One can estimate that for ‘developed’ countries, at least for the UK as Steve Graham (1998) argues, video surveillance will become “the fifth utility” of the networked utilities – following gas, electricity, water, and telecommunication systems. Another aspect is noteworthy: although, after World War II the responsibility for computer development and CCTV was turned over to the

commercial sector, it continues to be shaped by military interests, imperatives and funds. Thus, overseen militarily, a convergence between state and commercial surveillance is obvious. To the extent that technologies – such as communication, biometrics (the use of data extracted from the body),<sup>7</sup> manual and automated CCTV and new ‘low-intensity’ weapons – have their origins in military research and development, they have moved into policing and customer tracking businesses largely on the ‘trickle down’ model of dispersion. As Haggerty and Ericson note, “There has been a change towards a more ‘directed’ approach to technology transfer”, which they relate to “broader political transformations, the most important one being the disintegration of the Cold War threat” (2001, p. 54). This approach has been fuelled by 9/11, says David Carey, a former high-ranking CIA officer and, since November 2001, the head of the Information Assurance Centre at Oracle Corporation, the world’s largest database manufacturer: “In some ways, September 11 made business a bit easier. Previously, you pretty much had to hype the threat and the problem”. His boss, Larry Ellison, proposes to reconstruct America’s national security strategy along the lines of Oracle’s business model:

“The Oracle database is used to keep track of basically everything. The information about your banks, your checking balance is stored in an Oracle database. Your airline reservation is stored in an Oracle database. What books you bought on Amazon is stored in an Oracle database. Your profile on Yahoo is stored in an Oracle database. We already keep track of where you work, how much you earn, where your kids go to school, were you late on your last mortgage payment, when’s the last time you got a raise” (cited in Rosen 2002).

These separate commercial data are centralised in large databases maintained by credit card companies, whereas government data are mainly stored in disconnected databases: “The huge problem is the fragmented data. I really don’t understand”, states Ellison, who wants to consolidate the hundreds of state and federal databases into a single Oracle database (*ibid.*). Part of this data registration and collection in the US as well as in other countries is workplace surveillance. Mainly used to assure further exploitation and minimise profit losses, more than one-third of the 40 million American workers with Internet access are under constant surveillance very easily, because every computer leaves behind a trail of breadcrumbs. As the American Management Association (AMA) summarises in its workplace testing survey in 2000:

“Nearly three-quarters of major US firms (73.5%) record and review employee communications and activities on the job. The figure has doubled since 1997, when AMA inaugurated its annual survey. Video surveillance for security purposes grew from 32.7% in 1998 to 35.3%. The sample accurately mirrors AMA’s corporate membership, who together employ one-fourth of the US workforce” (AMA 2000, p. 2, 4).

The combination of algorithm, biometrics and CCTV opens up fields like customer tracking, profiling and relationship management – monitoring and channelling the shopping habits of customers, and the ability to monitor, store, exchange, cross-index and retrieve digital information grows each year. Like the UK company Clickstream Technologies Plc. that invented the monitoring of mouse click streams on web sites to target online shopping behaviour, in January 2002 the US company Brickstream Corp. introduced a system that pursues customers, collecting data about their ‘real life’ shopping habits. Advanced

Interface Technologies introduced a pattern identification program, combining voice and face recognition with CCTV that allows gender identification in shopping centres to optimise customer conduction; plans are under way to connect customer tracking systems with data mining (Sietmann 2002, p. 150-153).

"The train whistle blew, softly this time, almost whispering for them to please leave quietly. There were no TV cameras, no Minicams to be seen. No footage of American citizens being herded onto cattle cars for future historical re-interpretationists to throw in their faces. The great lesson of Watergate: Never leave a paper trail. The lesson of Rodney King: Minimise video opportunities."

(21st Century Manzanar Perry Miyake 2002, p. 3)

### **The Rise of a New Digital ABC: Algorithms, Biometry, Cameras**

The conventional way of verifying an alarm is to send a response either from the private security company or the police. Due to the high rate of false alarms and limitations on resources, the need for visual verification has increased, and the growth of CCTV, remote and on-site monitoring systems allowed the introduction of Automated Video Surveillance (AVS). Scholars argue that this is for operator concentration, saving of space, reduction of manpower, and enhancement of CCTV functions (Waring and Glendon 1998). It is obvious that AVS enables governments and commercial companies to reduce manpower and allows automatic responses, assisting human response and improving efficiency. In short, as Hesse (2002, p. 72) states, if "we consider the principles of protection as deter, detect, delay and respond, then the two objectives of CCTV and video motion detection are being continuously improved by the increases of technological advances". This is especially true when we think about the integration of biometrics into CCTV systems.

Advanced Video Motion Detection systems (VMD) like the Advanced Exterior Sensor project (AES) developed by Sandia National Laboratories in Albuquerque (New Mexico) and Livermore (California), combines the three sensor technologies of thermal infrared waveband, visible waveband and microwave radar with cameras and algorithms. Sandia is a research centre run by the Department of Energy (DoE) and the armaments company Lockheed Martin to "establish a permanent screen search system within global sensor networks. Conventional border control is to be supplemented by a system of monitoring security zones in the fore-field of the US' own borders" (Sietmann 2002, p. 95). As Sandia's project manager, Dave Nokes, states, "the long-term objective for the next years is to connect hundreds of sensor nodes that will be able to identify and pursue people in urban areas" (cited in Sietmann 2002).

The British QinetiQ Plc., a privatised subsidiary of the DERA (Defence Evaluation and Research Agency), developed a new personnel scanner out of a military all-weather camera; the system, displaying people naked on the monitors, will be able to screen 60 persons per minute from a distance of 30 meters to detect weapons and explosives (*Ibid.*).

Biometrics measure bodily life attributes (bios: life) and value them by characteristic (distinctive) features on the basis of a defined survey (metric: surveying). Biometry methods either work as verification systems (a user's identity has to match the implemented refe-

rence measure, i.e. one-to-one comparison) or as identification systems (the system compares the implemented reference measure with acquired forms and discovers the most similar measure) focussing on minutiae of or in the human body. As the 'best match' in the latter system needs to have a defined minimum similarity, algorithms come into play. Whereas authentication systems with a PIN code are bit-precise 'right' or 'wrong', biometry systems have to work with a blunt reference-value. Therefore, the probability distribution of a system's decision-taking has to be categorised into 'true acceptance' and 'true rejections' (both the desired outcomes), and the 'false acceptance rate' (FAR) and 'false rejection rate' (FRR), both causing identification problems.

What needs to be highlighted here is that biometrics, including CCTV, both disembeds and de-couples information from its nexus – the whole human being. Secondly, while electronic legal and business transactions will increase, necessary authenticity mechanisms will lead to an unforeseeable exchange of biometry data, making re-identification and one-to-one marketing an easy task. Thus, the human being is being transformed into a data flow – for social sorting and profit generating purposes.

CCTV and biometrics are combined in several fields: the state-run prison in Mannheim (Germany) uses biometry terminals to monitor the movement of the 850 prisoners and their working hours, using their fingerprints. As the manager of the prison's financial department, Bernhard Ruland, states, the aim is to be sure at any time that "the correct prisoner is at the correct time at the correct place" (cited in Ziegler 2002, p. 38).<sup>8</sup>

Biometry is also used at several airports around the globe while using facial recognition systems and iris scanners. Schiphol Airport in Amsterdam uses the iris scan system Privium that checks the eyes to see if they match the ones recorded on a smart card before; Boston Logan Airport uses the FaceIt system (Lyon, 2003); the Berlin Tegel Airport uses the ZN-Vision Technologies facial system to monitor their staff; the Sydney Airport uses the German system Cognitec to control its 6,000 personnel (Eick 2003); Keflavik Airport in Iceland too uses equipment from ZN-Vision Technologies, the world's leading German company in facial recognition situated in Bochum (Lucius 2002).

Expected to come are combinations of biometrics and CCTV with geographical profiling systems, like in the sniper case in Washington, D.C. in November 2002 (Grote 2002), and Global Information and Positioning Systems (GIS and GPS), expert systems and artificial neural networks (Hesse 2002). Boston began its Urban Neighbourhood Information System in the early 1990s, now using GIS. Data collected on block, group, tract and zip code level contributed by Boston public schools, Boston police, Department of Health, Business Directory, and others have led to a database including over 1,000 neighbourhood indicators (Pattavina *et al* 2002).

"Japanese television", he explained.

"That's nice", she said, not sure what response he was looking for.

"And not just Japanese. Chinese, Russian, every movie station in creation – I can get them all with this. My brother is in the Navy, works in electronics. He fixed me up with a special satellite dish that will pick up signals others can't. I can watch movies or TV shows from almost anywhere."

"You speak Japanese?"

"Nope, but if I ever learn, I'll have something to watch."

(24/7, Jim Brown, 2001, p. 2-3)

### **Breathing-space: Re-scaling the Surveillance of Injustice**

There are only a few evaluations, but current field research in Germany, Europe and the US shows that FA and FR rates are much higher in the field compared to those in controlled environments, such as companies' research areas or presented in computer fairs (Sietmann 2002; Hesse 2002). This is also true for CCTV systems, as Clive Norris and others have noted (Graham 1998; Lyon 2003).

Although there is evidence that biometric, genetic and video data may now be processed and cross-checked against each other, up to now this does not function on the level of everyday life. Even commercial research institutes and companies sometimes agree that it might take some more time to come forth with everything. An expert group of the US Federal Aviation Administration (FAA) concluded that the biometry industry "is not prepared to meet the demands of the FAA". Due to incomplete evaluations, it might take five to ten years "to have the maturity needed". TeleTrust, an NGO funded by the German Department of Commerce, admitted error rates in fingerprint and facial recognition systems between 2 to 20 percent,<sup>9</sup> and adds: "Biometric systems on a large scale will function within five, maybe even ten years" (cited in Sietmann 2002, p. 148).

Whether one wants to see these processes as 'Orwellian' or in the sense Foucault discussed Bentham's 'Panopticon', what needs to be highlighted is that most of the systems do not function properly and many are more or less easy to fool and overcome (Busch and Daum 2002; Costello 2002; Thalheim *et al* 2002; Ziegler 2002). But while algorithms, biometrics and neural networks are improving along with CCTV, GIS and GPS, the transformation of human beings into a set of parameters within given bandwidths is more than likely.

### **NOTES**

1. Surveillance, as I use it here, refers to the increasingly routine use of personal data and systematic information in the administration of agencies, businesses and institutions. Surveillance, i.e. watching from above, at the same time implies a dominant position of the observer shaping the observed.
2. For example, since the sixteenth century technological innovations and the restructuring of the respective welfare systems have gone hand in hand, leading to administrative centralisation and transparency (Gilliom 2001, p. 22-37); ID-card systems have been introduced during times of war in several countries, in which they either remained in place or were dismantled (Torpey 2000).
3. Following Moody (1997, p. 119-120), I refer to the neoliberal project as a mixture "of neoclassical economic fundamentalism, market regulation in place of state guidance, economic redistribution in favour of capital (known as supply-side economics), moral authoritarianism with an idealised family at its centre, international free trade principles (sometimes inconsistently applied) and a thorough intolerance of trade unionism".
4. Playing together the 'minutiae game' with the human body (see below).
5. (Autonomous) media, artists and the (off-)culture industry are part of this promotion – somehow 'playing' with the panoptic and synoptic parts of the 'game' (see among others <http://www.made.org> and <http://www.panix.com>).

6. The notion of 'control' refers to an ongoing debate on whether or not current societies are shifting from 'disciplinary societies' to 'control societies'. Any detailed discussion of this complex picture would require a separate research paper (see Deleuze 1993). What can be said is that hidden CCTV systems focus more on 'control', whereas open systems clearly attempt to strengthen 'discipline'.
7. Biometrics: Individual attributes such as fingerprints, irises, retinas, hand geometry, vein patterns, voices, faces and of course DNA; for an overview see Lyon 2003.
8. It is clear, of course, that like welfare centres and refugee camps, homeless shelters and prisons are most likely to be covered by CCTV; indeed, as an internal report from the Berlin Senate notes: "The surveillance by CCTV and sensor systems within and outside of the establishment [state prison Tegel, V.E.] is, due to worn out material and malfunctions, no longer guaranteed. The sensors have been switched off because of non-repairable malfunctions" (Expertenkommission 1995, p. 53); in some cases of surveillance, 'dummies' and illegal systems are in operation (Reichert *et al* 2002, p. 6-7; Ziegler 2002, p. 38; Eick 2003).
9. To compare: an error rate of only 0,1 = (per mille) out of ten million flight passengers will lead to about 1,000 false alarms: given current worldwide travel, an unacceptable number.

## REFERENCES

1. Busch, Christoph and Henning Daum "Frei von Zweifel? Biometrische Erkennung: Grundlagen, Verfahren, Sicherheit" (*c't* No. 5, 25 February 2002) p. 156-161.
2. Costello, Sam "Japanese researcher gums up biometrics scanners" (*Infoworld* <http://www.infoworld.com/articles/hn/xml/02/05/16/020516hngums.xml>, 16 May 2002).
3. Deleuze, Gilles "Postskriptum über die Kontrollgesellschaften" (*Unterhandlungen 1972-1990* 1993, Frankfurt/M.) p. 254-262.
4. Eick, Volker "Der deutsche Bahnhof – Zentrale oder Filiale der panoptischen Stadt des 21. Jahrhunderts? Aktuelle Sicherheitsdiskussionen – strategien und praxen bei und im 'Umfeld' der Deutschen Bahn AG" (<http://www.bigbrotherawards.de/2000/.gov/add.html>, 1998, Frankfurt/M.).
5. Eick, Volker "New strategies of 'policing' the poor: Berlin's neo-liberal security system" (Paper presented at the conference *Urbanising War/Militarising Cities: Cities as Strategic Sites* November 6-9 2002, Manchester, <http://www.surf.salford.ac.uk/documents/strategicsites.htm>).
6. Eick, Volker "We call it hard technology for a hard world" (*Surveillance in Germany and its Industry* unpublished, 2003, Berlin).
7. Expertenkommission (ed.) "Bericht der unabhängigen Expertenkommission für eine Sicherheitsanalyse der Berliner Justizvollzugsanstalten des geschlossenen Männervollzugs" (Internal paper, May 1995, Berlin).
8. Flusty, Steven "Building Paranoia" (in Ellin, Nan (ed.) *Architecture of Fear* 1997, New York) p. 47-59.
9. Fyfe, Nick R. and Jon Bannister "The eyes upon the street: Close-circuit television surveillance and the city" (in N. R. Fyfe (ed.) *Images of the Street: Planning, Identity and Control in Public Space* 1998, London) p. 254-267.
10. Garland, David *The Culture of Control* (2001, Oxford).
11. Gilliom, John *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (2001, Chicago/London).
12. Graham, Steven "Towards the Fifth Utility? On the Extension and Normalisation of Public CCTV" (in Norris, Clive, Jade Moran and Gary Armstrong (eds) *Surveillance, Closed Circuit Television and Social Control* 1998, Aldershot) p. 89-112.
13. Grote, Andreas *Algorithmus zur geografischen Lokalisierung von Straftätern* (<http://www.telepolis.de>, 12 October 2002).

14. Haggerty, Kevin D. and Richard V. Ericson "The Military Technostructures of Policing" (in Kaska, Peter B. (ed.) *Militarising the American Criminal Justice System* 2001, Boston) p. 43-64.
15. Hempel, Leon and Eric Töpfer *Inception Report* (Working Paper No. 1, <http://www.urbaneye.net>, 2002, Berlin).
16. Hesse, Layne "The Transition from Video Motion Detection to Intelligent Scene Discrimination and Target Tracking in Automated Video Surveillance Systems" (*Security Journal* Vol. 15, No. 2, 2002) p. 69-78.
17. Jessop, Bob "Globalisation, Entrepreneurial Cities and the Social Economy" (in Hamel, Pierre, Henri Lustiger-Thaler and Margit Mayer (eds) *Urban Movements in a Globalising World* 2000, London/New York) p. 81-100.
18. Jessop, Bob *The Future of the Capitalist State* (2002, Cambridge).
19. Kerr, Philip *Gridiron* (1995, London).
20. Koskela, Hille "The Gaze without Eyes: Video Surveillance and the Changing Nature of Urban Space" (in Koskela, H. (ed.) *Fear, Control & Space: Geographies of Gender, Fear of Violence, and Video Surveillance* 1999, Helsinki) p. 1-23.
21. Lea, John "Post-Fordism and Criminality" (in Jewson, Nick and Susanne MacGregor (eds) *Transforming Cities, Contested Governance and New Spatial Divisions* 1997, London/New York) p. 42-55.
22. Lucius, Robert V. "Das Profil der Masse" (*Frankfurter Allgemeine Zeitung* 1 August 2002) p. 13.
23. Lyon, David (ed.) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (2003, London/New York).
24. Miyake, Perry *21<sup>st</sup> Century Manzanar* (2002, Los Angeles).
25. Moody, Kim *Workers in a Lean World* (1997, New York).
26. Narr, Wolf-Dieter (ed.) *Wir Bürger als Sicherheitsrisiko* (1977, Reinbek).
27. Pattavina, April, Glenn Pierce and Alan Saiz "Urban Neighbourhood Information Systems: Crime Prevention and Control Applications" (*Journal of Urban Technology* Vol. 9, No. 1, 2002) p. 37-55.
28. Peck, Jamie and Adam Tickell "Neoliberalising Space" (*Antipode* Vol. 34, No. 3, 2002) p. 380-404.
29. Piglia, Ricardo *Die abwesende Stadt* (1994, Köln/Le Bois).
30. Reichert, Andreas, Andreas Zirngibl and Robert Kotok "Videoempirie" (*Videoüberwachung in Berlin TU Berlin*, WS 2001/2002).
31. Ronneberger, Klaus, Stephen Lanz and Walter Jahn *Die Stadt als Beute* (1999, Bonn).
32. Rosen, Jeffrey "Silicon Valley's Spy Game" (*The New York Times Magazine* <http://www.nytimes.com/2002/04/14/magazine/14techno.html>, 14 April 2002).
33. Sietmann, Richard "Die ultimative Überwachung. Personen-, Objekt- und Raumkontrolle mit neuartigen Techniken" (*c't* No. 17, 12 August 2002) p. 94-95.
34. Stephenson, Neal *Snowcrash* (1992, London).
35. Thalheim, Lisa, Jan Krissler and Peter-Michael Ziegler "Körperkontrolle Biometrische Zugangssicherungen auf die Probe gestellt" (*c't* No. 11, 21 May 2002) p. 114-123.
36. Torpey, John *The Invention of the Passport. Surveillance, Citizenship and the State* (2000, Cambridge).
37. Waring, Alan and Ian Glendon *Managing Risk* (1998, London).
38. Ziegler, Peter-Michael Katzenjammer "Biometrie: eine Branche in Erklärungsnot" (*c't* No. 12, 3 June 2002).

