7/QUIS CUSTODIET IPSOS CUSTODES

Stand up to
close scrutiny.
Raymond
98200900042

Standing up to close
scrutiny (Bombay/Abu Dhabi)
Pair of photographic prints,
each 120 x 84 cm
(Manu Luksch, 2005)

back at work:
the daily grind
at the Daily Myth
Ma Nu shapes worldviews
by shuffling old data
into new news

THE SPECTRAL CHILDREN

london, 2033

new towers mark the skyline
glass facades flashing code
to the central watchtower
a holographic web
of risk and trade
woven through the data cloud
of radioactive smog
that chokes those overlooked
by the optical revolution

far below, in the nether city
in the pavlovian underbelly
familiar patterns repeat
ad infinitum

except... look:
Ma Nu is moving home
in an anarchic break
from the everyday drone

–

back at work:
the daily grind [...]

Manu Luksch & Mukul Patel
2006

Excerpt from intertitles text of *Faceless: The Spectral Children* (multiple DVD players and monitors, 15 min looping video installation, 2006)

First shown at GBK Gallery Barry Keldoulis as part of the Sydney Biennale 2006

The Spectral Children
Installation view at* Digitally Yours, *Aboa Vetus & Ars Nova Museum, Turku (Finland, 2007)
Curated by Andy Best

12 March 2005

[redacted]
Store Manager
Kmart store [redacted]

[redacted]

Dear [redacted]

During the preceding 6 months our security staff has been monitoring your husbands activities while in our store. The list below details his offences, all of which have been verified by our surveillance cameras and we have retained copies on tape.

We have repeatedly given your husband verbal warnings while he is in this store and he has subsequently ignored them. He replied to these warning with rudeness and the response "while the wife shops here I will come here too". We are therefore forced to ban you, your husband and your family from this store.

The following list details your husbands activates in this store over the past six months.

June 15: Took 24 boxes of condoms and randomly put them in people's carts when they weren't looking.

July 2: Set all the alarm clocks in House wares to go off at 5-minute intervals.

July 7: Made a trail of tomato juice on the floor leading to the rest rooms.

July 19: Walked up to an employee and told her in an official tone, 'Code 3' in house wares and watched what happened.

August 4: Went to the Service Desk and asked to put a bag of M&M's on lay-buy.

September 14: Moved a 'Caution - WET FLOOR' sign to a carpeted area.

September 15: Set up a tent in the camping department and told other shoppers he'd invite the in if they'll bring pillows.

September 23: If any staff offers him assistance he begins to cry and asks, "Why can't you people just leave me alone?"

October 4: Looked right into the security camera; used it a mirror, and picked his nose.

November 10: While in the gun department, asked the clerk if he knows where the antidepressants are.

December 3: Darted around the store suspiciously loudly humming the "Mission Impossible" theme.

December 6: In the auto department, practiced his "Madonna Look" using different size funnels.

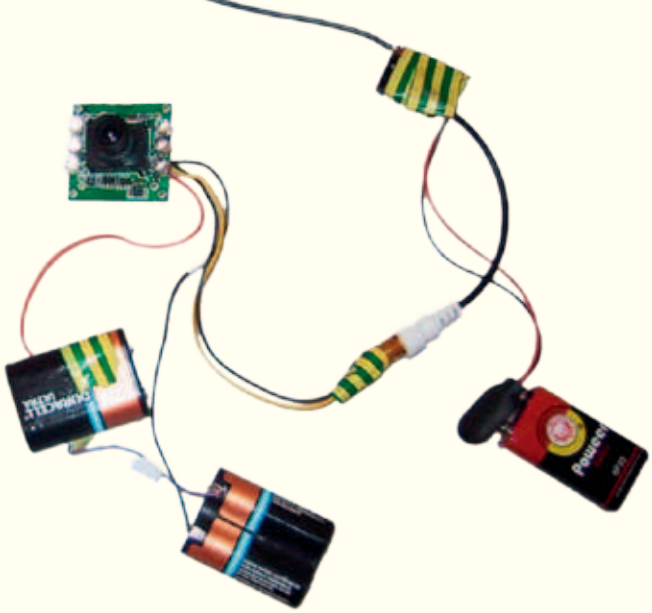
December 18: Hide in a clothing rack and when people browse through, yelled "PICK ME!" "PICK ME!"

December 21: When an announcement came over the loud speaker, he assumes the fetal position and screams "NO! NO! It's those voices again!"

December 23: Went in the fitting room, shut the door and waited a while; then yelled, very loudly, "There is no toilet paper in here!

[redacted]

[redacted]
Store Manager



THE SPY SCHOOL

The Spy School scrutinises the public–private borderline of post–9/11 daily life in a climate where the ethic of surveillance is in the ascendancy and the development of its technologies in overdrive.

Exercise #1: Tel Aviv, Israel, November 2002
Exercise #2: Hull, UK, January 2003
Exercise #3: Tallinn, Estonia, June 2003
Exercise #4: The *Faceless* project, London, 2002–07
Exercise #5: Who Is Watching The Watchers?, 2004

Exercise #1: Tel Aviv, Israel, November 2002

For *VideoZone*, the first video art biennale in Israel, *The Spy School* traveled to Tel Aviv to intervene in the opening night party at the Digital Art Lab, Holon, Tel Aviv.

Raiding the spectrum, *The Spy School* gathers information, throws it in to the mix, and sends it back out through the airwaves. Radio-talk, phone-talk, CCTV, your whispered conversations and surreptitious glances, captured, reconfigured, rebroadcast. You arrive at the party to find yourself already there, echoed in the soundtrack and projections. *The Spy School* infiltrates scenes with its human avatar, wired for sound and image and feeding the DJ and VJ with angles on the party-goers. And there's a performer on the floor, ranging through moves and masks – but no one's quite sure who's watching who.

---

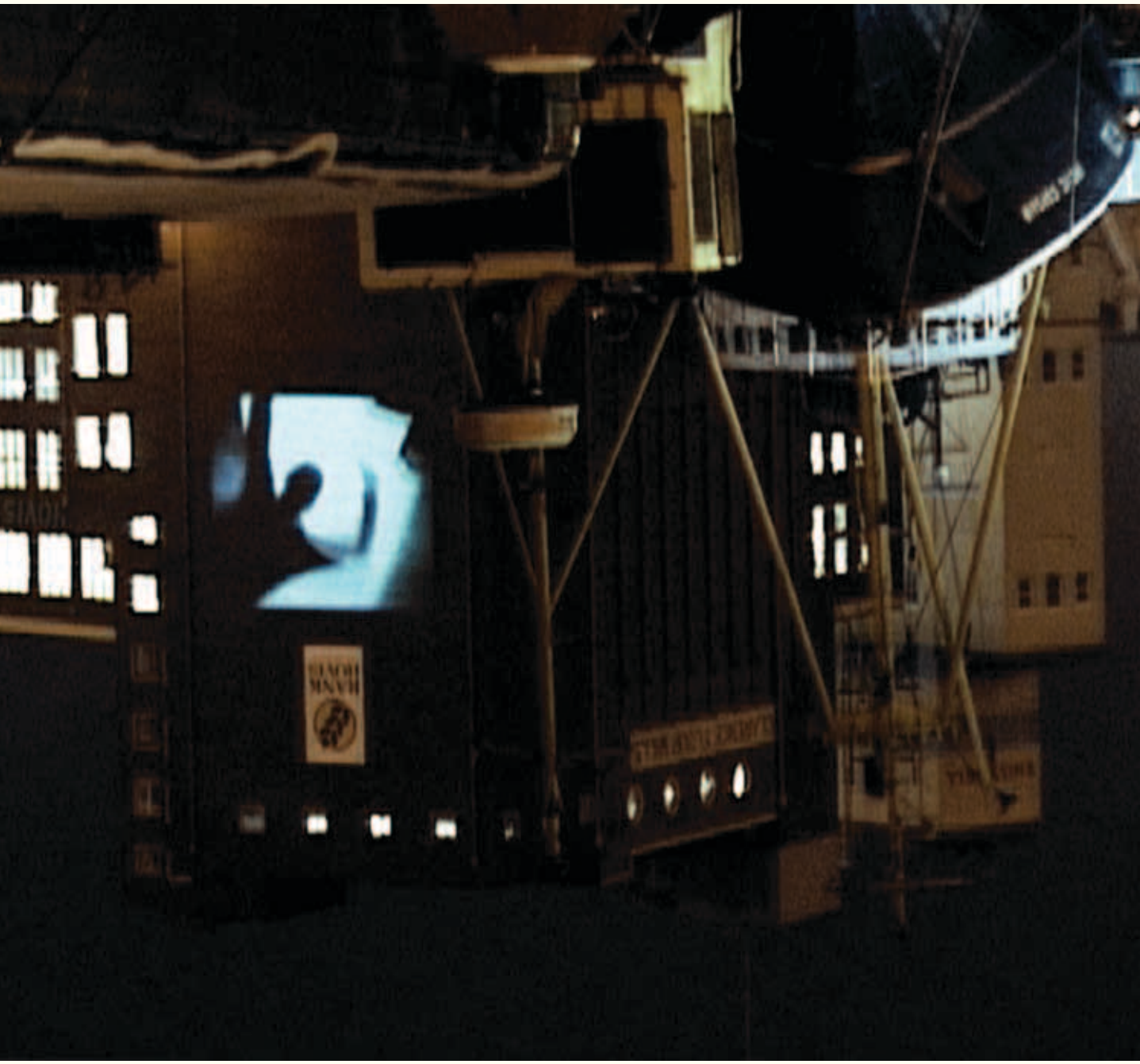
ambientTV.NET
2002–07

The Spy School Exercise #1
party intervention
piece by Manu Luksch &
Mukul Patel, with Michael
Uwemedimo, Gavin Starks
and support by Jaromil
[dyne.org]

The Spy School Exercise #2
realisation + video:
Manu Luksch
performance: Michael
Uwemedimo, Lizzie Tuckey
sound: Mukul

***Above: Miniature wireless cameras used for* Spy School Exercise #2**

Left: Letter forwarded to Manu Luksch by a visitor to Gallery Barry Keldoulis while* The Spectral Children *was on show



Exercise #2: *Hull, UK, January 2003*

Commissioned by Hull Time-Based Arts, *The Spy School Exercise #2* took place outside the house of William Wilberforce, a leader of the Abolitionist movement, in the important British slave trade harbour of Kingston upon Hull.

Two capoeiristas, Michael Uwemedimo and Lizzie Tuckey, play outdoors, in the dark in front of the Wilberforce House Museum on the River Hull. Their costumes incorporate wireless, miniature, night-vision-enabled cameras that trace and transmit their movements. The work is a thematic exploration of the contradictions and conjunction of spectacle and surveillance, and a demonstration of the ruses by which 'data-subjects' can slip their shadows, masking their movements and intentions, while remaining highly visible. The capoeiristas were 100 m from the receivers, at the limit of the useful range, where the signal was seasoned with noise.

Capoeira is a discourse of dissimulation and resistance. Drawing on martial, musical, religious and dance forms from communities along the slave routes that reached from coast to coast across the Atlantic, deep into the African and Brazilian interiors, its martial implications had to be disguised as recreational, quasi-religious dance forms. It is a ruse, a camouflage, double-talk. When capoeira was outlawed, the stakes were raised – execution and amputation were among the penalties for playing – it became a form that had to hide itself, emerge, take shape, and disperse. Strategies of dissimulation characterise the encounter between participants as well as those between the form and structures of societal authority. Each dancer is a shadow that traces the motion of the other, suddenly to slip out of synch, to surprise and trip the body that cast it.

A video recording of *Exercise #2* was shown on cable TV (Kingston Interactive, Timebase Channel) and projected in public space. Behind the projection surface, the huge south-facing facade of the Rank Hovis Building, Lord Rank had carried out early media experiments. A filmmaker and mogul, among his fascinations were the possibilities of the production and exhibition of 'religious films'.

Exercise #2 ***screening on the Rank Hovis Building, Hull, 2003***

Exercise #3: *Tallinn, Estonia, June 2003*

MA students at the E-Media Centre of the Eesti Kunstiakadeemia developed new works over four days of intensive tactical media workshops led by Manu Luksch and Mukul Patel. The workshops focussed on the boundaries between the public and the private, and the mediation that occurs all the time, everywhere in an age of increasing surveillance and data mining by states and corporations. The artists used surveillance technologies including miniature wireless cameras. Works were displayed on the large electronic billboard on the EKA building at Tartu mnt. 1, and streamed online.

Exercise #4: *The* Faceless *Project, London, 2002–08*

The *Faceless* project is a series of works that intervenes in the quotidian recording and processing of CCTV (closed-circuit television) surveillance camera images in the UK, and probes the laws surrounding these images – particularly the UK Data Protection Act (DPA) 1998. Apart from a 50 minute sci-fi film produced under the constraints of the *Manifesto for CCTV Filmmakers*, the project has resulted in works including

- an online DIY toolkit for making 'subject access requests' under the DPA
- an archive of research materials, records of communication with data controllers, and other documentation
- *The Eye* (a choreography workshop for surveilled space, led by the Ballet Boyz, Billy Trevitt and Michael Nunn)
- *I wish to apply, under the Data Protection Act, for any and all CCTV images of my person held within your system. I was present at [place] from approximately [time] onwards on [date].* (lightboxes with letters received from data controllers)
- *The Spectral Children* (a multiple-screen video installation for galleries), and
- *FRAMED* (a series of large-scale photographic prints).

FACELESS (MANU LUKSCH, 2007, UK/AUSTRIA)
The film is an assemblage of recordings from existing CCTV surveillance cameras in London – the most heavily surveilled city on Earth – obtained under the terms of the DPA (1998). The process of accessing these images also activated other layers of legislation concerning the recordings, including Article 8 of the Human Rights Act (1998), the Freedom of Information Act

(2000), and aspects of copyright and image rights. In *Faceless*, the CCTV image is treated as a 'legal readymade' – an *objet trouvé* (after Duchamp) that has been annexed and redacted according to the law.

The scenario of *Faceless* reflects and renders visible the formal qualities of the images both as image, and as legal readymade: the RealTime calendar of the film derives from the time-lapse nature of the recordings and the often multiple, conflicting timecodes embedded within the frames, while the facelessness of the world is rooted in the erasure of the faces of third parties in the footage (as stipulated by law for the protection of privacy). In its fictive aspect, the scenario resembles that of Yevgeny Zamyatin's dystopian novel *We* (1924), although in *Faceless* it is derived under real-world constraints.

Plot development was an open process, in parallel with and parasitical upon the process of image acquisition. Since CCTV cameras are not permitted to record sound, there is no dialogue; only music, and a voiceover by Tilda Swinton in hommage to Chris Marker's *La Jetée*.

SUBJECT ACCESS REQUESTS FOR CCTV RECORDINGS
Many corporations and organisations (data controllers) collect and store personal information about others (data subjects) on computer or in paper files. This information can be used to make decisions that significantly affect the data subjects. The Data Protection Act (DPA) allows you to find out what information is held on you as a data subject in computer and some paper records.

In 1998, CCTV systems were brought into the remit of the DPA. In order to obtain copies of any CCTV recordings in which you feature, you must determine the identity of the relevant data controller and address a 'subject access request' letter to them. The DPA stipulates that the contact details of data controllers be displayed in the zone covered by CCTV. Data controllers are obliged to store any recordings for a declared retention period, and to release a copy to a data subject who requests them and pays the statutory fee (£10).

Note: the DPA (1998) has recently been reinterpreted in the light of court rulings in, notably, *Peck vs The United Kingdom* (2003) and *Durant vs Financial Services Authority* (2003). This has placed an onus of proving the 'biographical relevance' of the recordings on the data subject.

1

[1] www.darpa.mil

Exercise #5: Who Is Watching The Watchers?, *2004*

A POST-9/11 T-SHIRT COLLECTION

Ambient Information Systems (AIS) launches its September 11 collection in hommage to the recently discontinued Total Information Awareness (TIA) logo of the US Defence Advanced Research Projects Agency (DARPA)[1].

The TIA logo, a potent symbol of security and freedom, would have been lost to history were it not for its timely appropriation by AIS.

TIA is a program of DARPA's Information Awareness Office (IAO), its mission to integrate 'innovative information technologies for detecting and pre-empting foreign terrorist activities against Americans.' The original logo was discontinued because it had 'become a lightning rod' and was 'needlessly diverting time and attention from critical tasks.' The Total Information Awareness program has now been renamed Terrorism Information Awareness Systems. DARPA runs numerous other research programs, including FutureMAP (a futures market where traders were invited to gamble on political events).

The original TIA logo features an eye that 'scans the globe for evidence of terrorist planning and is focused on the part of the world that was the source of the attacks' of 9/11. The Ambient Information Systems T-Shirt features a slightly modified version of the TIA logo. Notably, the eye is refocused and the motto 'Scienta est potentia' – Knowledge is power – is replaced by 'Quis custodiet ipsos custodes' – *Who is Watching the Watchers?*

1
Watchers-watchers-watcher
Photo: Peter Grech

2
Original TIA logo

3
TIA logo as modified by AIS

Right: Excerpt from a DARPA public information document

Following pages, left: Subject access request letter

Right: Faceless *film poster*

2

3

Question 14: When is it anticipated that TIA will be ready for use?

Answer: Research under the TIA program is planned for several years. An operational prototype TIA network is the goal of this multiyear effort. During the first 36 months, a range of ideas will be developed via limited demonstrations and preliminary prototypes. During the final 24 months, the most promising research avenues will be extended to support transition of a scalable, leave-behind network prototype. At the end of the multiyear program, Congress will have decided if and how the TIA network will be deployed or further matured.

Question 15: What does the IAO logo mean? Why has it disappeared from the web site?

Answer: DARPA offices have traditionally designed and adopted logos. However, because the IAO logo has become a lightning rod and is needlessly diverting time and attention from the critical tasks of executing that office's mission effectively and openly, we have decided to discontinue the use of the original logo.

For the record, the IAO logo was designed to convey the mission of that office; i.e., to imagine, develop, apply, integrate, demonstrate, and transition information technologies, components, and prototype, closed-loop information systems that will counter asymmetric threats by achieving total information awareness useful for preemption, national security warning, and national security decision making. On an elemental level, the logo is the representation of the office acronym (IAO); the eye above the pyramid represents "I," the pyramid represents "A," and the globe represents "O." In the detail, the eye scans the globe for evidence of terrorist planning and is focused on the part of the world that was the source of the attacks on the World Trade Center and the Pentagon. *Scientia est potentia* means "Knowledge is power." With the enabling technologies being developed by the office, the United States will be empowered to implement operational systems to thwart terrorist attacks like those of September 11, 2001.

The unfinished pyramid and the eye depicted in the logo were taken directly from the reverse side of the Great Seal of the United States of America (for a history of the seal, see http://www.heraldica.org/topics/usa/usheroff.htm). Both sides of the seal also appear on the back of the U.S. $1 bill.

Question 16: How was John Poindexter selected as the Director of DARPA's Information Awareness Office?

Answer: Dr. Poindexter was selected as the Information Awareness Office Director based on a number of factors: his prior experience with DARPA's Project Genoa and the national security

RECEIVED
-2 SEP 2003

MANU LUKSCH
[redacted]

28 August 2003

The security and safety manager,
[redacted]

Dear Sir / Madam,

I wish to apply, under the Data Protection Act, for any and all CCTV images of my person held within your system. On 27 August 2003, I was present at the ATM 254 Seven Sisters Road, at approx. 20.15 p. m.

For ease of identification, I enclose a photo of myself below. I was wearing white trousers and a white T-Shirt with aqua blue sleeves.

IN AN EERILY FAMILIAR CITY, A CALENDAR REFORM HAS DISPENSED WITH THE PAST AND THE FUTURE, LEAVING CITIZENS FACELESS, WITHOUT MEMORY OR ANTICIPATION. UNIMAGINABLE HAPPINESS ABOUNDS – UNTIL A WOMAN RECOVERS HER FACE...

LONDON HAS THE HIGHEST DENSITY OF CCTV SURVEILLANCE CAMERAS ON EARTH. *FACELESS* USES RECORDINGS FROM THESE CAMERAS, OBTAINED UNDER THE UK DATA PROTECTION ACT, AS 'LEGAL READYMADES' TO CONSTRUCT A STRANGE YET PLAUSIBLE WORLD.

«Il y a deux façons de concevoir le cinéma du réel. La première est de prétendre donner à voir le réel. La seconde est de se poser le problème du réel. De même il y avait deux façons de concevoir le cinéma-vérité. La première était de prétendre apporter la vérité. La seconde était de se poser le problème de la vérité.»

«Or nous devons le savoir, le cinéma de fiction est dans son principe beaucoup moins illusoire, et beaucoup moins menteur que le cinéma dit documentaire, parce que l'auteur et le spectateur savent qu'il est fiction, c'est-à-dire qu'il porte sa vérité dans son imaginaire. Par contre, le cinéma documentaire camoufle sa fiction et son imaginaire derrière l'image reflet du réel. Or, nous devons le savoir de plus en plus profondément, la réalité sociale se cache et se met en scène

d'elle-même, devant le regard d'autrui et surtout devant la caméra. La réalité sociale s'exprime à travers des rôles. Et en politique, l'imaginaire est plus réel que le réel. C'est pourquoi, c'est sous le couvert du cinéma du réel qu'on nous a présenté, proposé, voire imposé les plus incroyables illusions, c'est que, dans les contrées merveilleuses dont on ramenait l'image exaltante, la réalité sociale était mise en scène et occultée par le système politique régnant et transfigurée dans les yeux hallucinés du cinéaste.»

«C'est-à-dire que le cinéma qui se pose les plus graves et les plus difficiles problèmes par rapport à l'illusion, l'irréalité, la fiction, est bien le cinéma du réel, dont la mission est d'affronter le plus difficile problème posé par la philosophie depuis deux millénaires, celui de la nature du réel.»

Edgar Morin, from his 1980 introduction to* Cinéma Vérité *at Centre Pompidou

7/QUIS CUSTODIET
IPSOS CUSTODES

ANGSTBILDER GEGEN DIE ANGST

Angst löscht die Gegenwart aus. Sie speist sich aus einer Vergangenheit, die sich unkontrolliert über die Gegenwart hinweg ausbreitet und von der Zukunft Besitz ergreift. Diese Angst zu bannen, indem man Vergangenheit und Zukunft ausschaltet, das ist das Versprechen des Überwachungsstaates. Ein Versprechen, das die permanente Observation des öffentlichen Raums zu legitimieren scheint und den Traum vom sorgenfreien Dasein im abgeschotteten Jetzt in einen real gewordenen Alptraum verkehrt.

Manu Luksch erzählt von diesem Alptraum im Vokabular des Science Fiction Films – und mit dem Bildmaterial, das sie den Betreibern von Londoner Videoüberwachungsanlagen unter Berufung auf ein Datenschutzgesetz abgerungen hat. In fantastisch-poetischer Verkettung lässt sie beklemmend vertraute Stadtansichten zum Schauplatz eines Schicksalsszenarios werden, in dem eine Frau den schockhaften Ausbruch aus der existenziellen Verfasstheit der „Echtzeit"-Erfassung erlebt.

Gesichts- und geschichtslos wie die Menschen, die auf den realen, von der Betreibergesellschaft CCTV herausgegebenen Videoaufnahmen (aufgrund eines Gesetzes zum Schutz der Privatheit) unkenntlich gemacht wurden, taucht die Protagonistin von *Faceless* mit ihrem plötzlich wiedererlangten Gesicht aus einem Datendasein hervor und in eine vergessen geglaubte Geschichte ein.

In spiegelbildlicher Umkehrung des Befreiungsakts, in welchem das Trauma dieser Bewusstwerdung letztlich mündet, traumatisiert *Faceless* über die ebenso stimmungsvoll wie unheimlich bebilderte Metaerzählung einer Gesellschaft, deren Selbstbewusstsein im Zerrbild ihrer medialen Hyperpräsenz zu verblassen droht.

Robert Buchschwenter
2007

English Translation:
Steve Wilder
Traduction Français:
Françoise Guiguet

IMAGES OF FEAR, AGAINST FEAR

Fear blots out the present. It feeds on a past that spills over uncontrollably into the present; it takes possession of the future. Vanquishing this fear by erasing past and future is the promise of the Big Brother state. This promise is contrived to legitimise the constant observation of public space, which turns the dream of carefree existence in an isolated present into a nightmarish reality.

Manu Luksch employs the vocabulary of science fiction film to draw us into this nightmare. Crucially, she uses only images obtained from the operators of CCTV video surveillance systems in London, under the terms of a British law governing access to data. In a fantastic and poetic concatenation, she transforms oppressively familiar views of the city into locations of a fateful scenario, in which a woman is thrust into a startling escape from the perpetually administered present of 'RealTime'.

At first as faceless and devoid of history as the other individuals anonymised in the recordings by the CCTV operators (to comply with privacy legislation), the film's protagonist abruptly regains her face, and casts off her former existence as a Bit of data to dive into her stolen past.

In a mirror image of the failed act of liberation that the trauma of this realization incites, *Faceless* succeeds in traumatising its viewers by means of an equally atmospheric and weirdly illuminated metanarrative – that of a society whose self-understanding is occluded by its dazzling media hyperpresence.

DES IMAGES DE LA PEUR POUR VAINCRE LA PEUR

La peur anéantit le présent. Elle se nourrit d'un passé qui, sans crier gare, submerge le présent et prend possession de l'avenir. Conjurer cette peur en abolissant passé et avenir, telle est la promesse de l'État de surveillance. Une promesse qui tend à légitimer l'observation permanente de l'espace public et transforme le rêve d'une existence sans problème dans un immédiat étanche en cauchemar devenu réalité.

Manu Luksch nous conte ce cauchemar en utilisant le vocabulaire des films de science fiction – et le matériau visuel qu'elle a réussi à acquérir auprès des contrôleurs du système londonien de vidéo surveillance, en vertu de la loi britannique sur la protection des données. Dans un enchaînement fantastico-poétique, elle transforme des vues de la ville, d'une familiarité troublante, en théâtre d'un scénario fatidique: une femme est brutalement projetée hors du «monde du temps réel» qui était soumis au contrôle absolu d'un système anonyme.

D'abord sans visage et sans vécu, comme les personnes rendues non identifiables sur les enregistrements vidéo authentiques fournis par la société de contrôle CCTV (conformément à la loi britannique sur la protection de la vie privée), la protagoniste de *Faceless*, retrouvant soudain son visage, se trouve rejetée hors de son existence de donnée et plongée dans une histoire qu'on pensait oubliée.

Quand la prise de conscience traumatique conduit finalement au renversement en son contraire de l'acte libérateur, *Faceless* bouleverse en faisant, par le biais d'images aussi évocatrices qu'angoissantes, le métarécit d'une société dont l'identité est en passe de disparaître dans l'image déformée de son hyperprésence médiatique.

---

the filmmaker as symbiont:

opportunistic infections of the surveillance apparatus

Manifesto for CCTV filmmakers declares a set of rules, establishes effective procedures, and identifies issues for filmmakers using pre-existing CCTV (surveillance) systems as a medium in the UK. The manifesto is constructed with reference to the Data Protection Act 1988 and related privacy legislation that gives the subjects of data records access to copies of the data. The filmmaker's standard equipment is thus redundant; indeed, its use is prohibited. The manifesto can be adapted for different jurisdictions.

* * *

MANIFESTO FOR CCTV FILMMAKERS

1. GENERAL

The filmmaker is not permitted to introduce any cameras or lighting into the location.

2. SCRIPT

A protagonist ("data subject") is required to feature in all sequences.

Data Protection Act 1998; 1998 Chapter 29; Part II Section 7(1).
[A]n individual is entitled –
(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,
(b) if that is the case, to be given by the data controller a description of –
(i) the personal data of which that individual is the data subject,
(ii) the purposes for which they are being or are to be processed, and
(iii) the recipients or classes of recipients to whom they are or may be disclosed,
(c) to have communicated to him in an intelligible form –
(i) the information constituting any personal data of which that individual is the data subject, and
(ii) any information available to the data controller as to the source of those data,
(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

The documented activity of the protagonist must qualify as personal or sensitive data. The filmmaker is to establish this by locating a CCTV camera and circumscribing the field of action for the actors relative to it, so that incidents of biographical relevance (i.e., that reveal personal data) occur in the frame.

ICO CCTV systems and the Data Protection Act JB v.5 01/02/04
2. The court decided that for information to relate to an individual (and be covered by the DPA) it had to affect their privacy. To help judge this, the Court decided that two matters were important: that a person had to be the focus of information, the information tells you something significant about them.

The provisions of the 1998 Act are based on the requirements of a European Directive, which at, Article 2, defines, personal data as follows:
"Personal data" shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
The definition of personal data is not therefore limited to circumstances where a data controller can attribute a name to a particular image. If images of distinguishable individuals' features are processed and an individual can be identified from these images, they will amount to personal data.

All people other than the protagonist ("third parties") will be rendered unidentifiable on the data obtained from the CCTV operators. Typically, operators blur or mask out faces of third parties. The filmmaker is to consider the visual impact of this manipulation, and to establish a rule for the handling of footage delivered with ineffectual masking or blurring – for example, reporting the offence.

Right to Privacy in Article 8 of the Human Rights Act 1998:
RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE
1. Everyone has the right to respect for private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights or freedoms of others.

DPA1998
4. On the other hand, the disclosure of third party information in compliance with a subject access request may also expose the data controller to complaint or action by the third party, for example [...] for breach of confidence.
6. The data controller should consider to what extent it is possible to communicate the information sought without disclosing any third party information [...] This might be achieved by editing the information to remove names or other identifying details.

3. LOCATION

The filmmaker is to choose locations covered by multiple cameras operated by a large business, private security firm or public authority – or, if operated by a small retailer, cameras that can be panned or zoomed remotely. Locations may be mobile (e.g., public bus).

ICO CCTV systems and the Data Protection Act JB v.5 01/02/04
If you have just a basic CCTV system your use may no longer be covered by the DPA.
[...] Small retailers would not be covered who
– only have a couple of cameras,
– can't move them remotely,
– just record on video tape whatever the camera picks up,
– only give the recorded images to the police to investigate an incident in their shop.

For every camera, the operator's name and contact details are to be noted.

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
7. Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.
The signs should contain the following information:
Identity of the person or organisation responsible for the scheme.
The purposes of the scheme.
Details of whom to contact regarding the scheme.
(First Data Protection Principle).

4. FOOTAGE REQUESTS

After each shoot, the filmmaker is to send a written request ("subject access request letter") to the CCTV operator ("data controller") to ensure that the data recovery process can be initiated while the recordings are still archived. (Mandatory retention periods vary.)

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
1. Once the retention period has expired, the images should be removed or erased (Fifth Data Protection Principle).

The subject access request letter is to state the place and time of the recording and include a picture of the protagonist (wearing the same clothes if possible) and a cheque for £10 (the maximum fee chargeable). Letters should be sent by a secure system that provides

evidence of delivery. (Some data controllers may require the notarisation of the letter to legally establish identity.)

Data Protection Act 1998; 1998 Chapter 29, Part II Section 7(2)
A data controller is not obliged to supply any information under subsection (1) unless he has received –
(a) a request in writing, and
(b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

The filmmaker is to allow a maximum 40 days after sending the data request for an initial response.

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
A data controller must comply with a subject access request promptly, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of: the information required (i.e. to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks); and the fee.

The filmmaker is to establish a set of rules for handling the various formats in which the data may be sent (video tape, DVD-video, digital files encoded with proprietary codecs, hard copies of frames, etc.).

5. SOUND

CCTV systems are not permitted to record sound. The filmmaker is to establish a set of rules for the soundtrack (if any) of the movie.

6. DISTRIBUTION

Footage received is subject to complex copyright issues. The filmmaker is to take legal advice and establish a strategy.

* * *

Manu Luksch & Mukul Patel
2007

CHASING THE DATA SHADOW

First published in Stocker, G. & Schöpf, C., eds., *Goodbye Privacy: Ars Electronica 2007* (Ostfildern: Hatje Cantz Verlag, 2007)

Stranger than fiction

Remote-controlled UAVs (Unmanned Aerial Vehicles) scan the city for anti-social behaviour. Talking cameras scold people for littering the streets (in children's voices). Biometric data is extracted from CCTV images to identify pedestrians by their face or gait. A housing project's surveillance cameras stream images onto the local cable channel, enabling the community to monitor itself.

These are not projections of the science fiction film that this text will discuss, but techniques that are used today in Merseyside, Middlesborough, Newham and Shoreditch in the UK. In terms of both density and sophistication, the UK leads the world in the deployment of surveillance technologies. With an estimated 4.2 million CCTV cameras in place, its inhabitants are the most watched in the world[1]. Many London buses have five or more cameras inside, plus several outside, including one recording cars that drive in bus lanes.

[1] 'A Report on the Surveillance Society'. For the Information Commissioner by the Surveillance Studies Network, September 2006, p.19. Available from www.ico.gov.uk

But CCTV images of our bodies are only one of many traces of data that we leave in our wake, voluntarily and involuntarily. Our vehicles are tracked using Automatic Number Plate Recognition systems, our movements revealed via location-aware devices (such as cell phones), the trails of our online activities recorded by ISPs, our conversations overheard by Echelon, shopping habits monitored through loyalty cards, individual purchases located using RFID tags, and our meal preferences collected as part of PNR (flight passenger) data. Our digital selves are many-dimensional, alert, unforgetting.

Increasingly, these data traces are arrayed and administered in networked structures of global reach. It is not necessary to posit a totalitarian conspiracy behind this accumulation — data mining is an exigency of both market efficiency and bureaucratic rationality. Much has been written on 'the surveillance society' and 'the society of control', and it is not the object here to construct a general critique of data collection, retention and analysis. However it should be recognised that, in the name of efficiency and rationality — and, of course, security — an ever-increasing amount of data is being shared (or leaked)

DIE JAGD NACH DATENSCHATTEN

Manu Luksch & Mukul Patel
2007

Aus dem Englischen von
Martina Bauer

Seltsamer als jede Fiktion

Ferngesteuerte, unbemannte Luftfahrzeuge überfliegen die Stadt auf der Suche nach unsozialem Verhalten. Sprechende Kameras rufen (mit Kinderstimmen) Menschen zur Ordnung, die Abfälle auf die Straßen werfen. Bildern der Videoüberwachung werden biometrische Daten entnommen, um Passanten über ihr Gesicht oder ihren Gang zu identifizieren. Die Überwachungskameras einer Wohnanlage werden im internen Kabelfernsehen ausgestrahlt, und ermöglichen den Bewohnern, sich selbst zu kontrollieren.

Das sind keine Szenen aus dem Science Fiction Film, der Anlaß dieses Textes ist, sondern Techniken, die heute in Großbritannien in Merseyside, Middlesborough, Newham und Shoreditch zum Einsatz kommen. Mit einer geschätzten Anzahl von 4,2 Millionen CCTV-Kameras sind die Einwohner Großbritanniens die meist beobachteten der Welt[1]. Viele Londoner Busse sind im Inneren mit fünf oder mehr Kameras bestückt, weitere sind außen angebracht, wobei eine die Autos aufnimmt, die die Busspur benützen.

Doch die Bilder der Überwachungskameras sind nur eine der vielen Datenspuren, die wir – freiwillig oder unfreiwillig – hinterlassen. Unsere Autofahrten werden mittels Nummernschilderkennung aufgezeichnet, dank der location-awareness der Endgeräte (wie etwa Mobiltelefone) werden unsere Bewegungen registriert, die Spuren unserer Online-Aktivitäten von Internetdienstanbietern aufgezeichnet, unsere Gespräche von Echelon abgehört, Einkaufsgewohnheiten per Kundenkarten überwacht, individuelle Einkäufe über RFID-Kennungen (Radio Frequency Identification, Identifizierung über Radiowellen) und unsere Ernährungsgewohnheiten mit den Fluggastdaten erfasst. Unsere digitalen Alter Egos sind mehrdimensional, wachsam und vergessen nie etwas.

Diese Datenspuren werden zunehmend in global vernetzten Datenbanken gehortet und verwaltet. Man muss nicht unbedingt eine totalitäre Verschwörung hinter dieser Datenakkumulation vermuten – die Auswertung von Daten ist sowohl ein Erfordernis der Markteffizienz als auch der bürokratischen Rationalität. Über die „Überwachungsgesellschaft“ und die „kontrollierte

[1] Surveillance Studies Network „A Report on the Surveillance Society“ (ICO: September 2006), S. 19. Zu beziehen über www.ico.gov.uk

1

between the keepers of such seemingly unconnected records as medical histories, shopping habits, and border crossings. Legal frameworks intended to safeguard a conception of privacy by limiting data transfers to appropriate parties exist. Such laws, and in particular the UK Data Protection Act (DPA, 1998), are the subject of investigation of the intermedia project *Faceless*.

From Act to Manifesto

I wish to apply, under the Data Protection Act, for any and all CCTV images of my person held within your system. I was present at [place] from approximately [time] onwards on [date].[2]

For several years, ambientTV.NET conducted a series of exercises to visualise the data traces that we leave behind, to render them into experience and to dramatise them, to 'watch those who watch us'. These experiments, scrutinising the boundary between public and private in post-9/11 daily life, were run under the title *The Spy School*. In 2002, *The Spy School* carried out an exercise to test the reach of the UK Data Protection Act as it applies to CCTV image data.

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. The DPA gives individuals certain rights regarding information held about them. It places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual[3].

The original DPA (1984) was devised to permit and regulate access to computerised personal data such as health and financial records. A later EU directive broadened the scope of data protection and the remit of the DPA (1998) extended to cover, amongst other data, CCTV recordings. In addition to the DPA, CCTV operators must comply with other laws related to human rights, privacy, and procedures for criminal investigations, as specified in the *CCTV Code of Practice*[4].

As the first 'subject access request' letters were successful in delivering CCTV recordings for *The Spy School*, it then became pertinent to investigate how robust the legal framework was.

[2] From the template for 'subject access requests' used for Faceless.

[3] Data Protection Act Factsheet available from the UK Information Commissioners Office www.ico.gov.uk

[4] See www.ico.gov.uk

1
Transport for London Poster, 2002

2
Manifesto for CCTV Filmmakers, *Broadway Market, London 2008*
Photo: Mukul Patel

Gesellschaft“ wurde bereits viel geschrieben, und es ist nicht unsere Absicht, in diesem Rahmen eine allgemeine Kritik von Datensammlung, –vorratsspeicherung und –analyse zu leisten. Doch sollten wir nicht die Augen davor verschließen, dass im Namen von Effizienz und Rationalität – und natürlich der Sicherheit – eine ständige wachsende Datenmenge zwischen den Bewahrern scheinbar nicht vernetzter Aufzeichnungen wie unserer Krankengeschichten, Einkaufsgewohnheiten und Grenzübertritten ausgetauscht wird. Es gibt gesetzliche Rahmenbedingungen zum Schutz der Privatheit, die Datenübertragungen auf die zugehörigen Parteien beschränken. Es sind diese Gesetze und insbesondere das britische Datenschutzgesetz (DPA 1998), die der Films *Faceless* durch seine Machart untersucht.

Vom Gesetz zum Manifest

Ich möchte gemäß DPA 1998 sämtliche Videobilder meiner Person, die von Ihrer Videoüberwachungsanlage aufgezeichnet wurden, beantragen. Ich war am [Datum] um [Zeit] in [Ort] anwesend.[2]

Unter dem Namen „ambientTV.NET“ betrieb Manu Luksch mehrere Jahre lang eine Reihe von Workshops zur Visualisierung von Datenspuren, um diese in dramatisierter Weise erfahrbar zu machen und „jene zu beobachten, die uns beobachten“. Diese Experimente, in denen die Grenze zwischen Öffentlichkeit und Privatheit im Alltagsleben nach 9/11 eingehend untersucht wurde, liefen unter dem Titel *The Spy School*. Im Jahr 2002 wurde in *The Spy School* ein Experiment durchgeführt, um die Wirksamkeit des UK Data Protection Act in Bezug auf CCTV-Bilddaten zu testen.

Der Data Protection Act 1998 versucht, eine Balance zwischen den Rechten des Einzelnen und den mitunter konkurrierenden Interessen jener herzustellen, die legitime Gründe haben, personenbezogene Daten zu verwenden. Der DPA gesteht Einzelpersonen gewisse Rechte hinsichtlich der über sie gesammelten Daten zu. Er erlegt jenen, die Daten verarbeiten (den verantwortlichen Stellen) Verpflichtungen auf, während er jenen, deren Datenprofil erstellt wird (die Betroffenen), Rechte zugesteht. Personenbezogene Informationen umfassen sowohl Fakten als auch Meinungen über Einzelpersonen[3].

Der DPA (1984) wurde ursprünglich ausgearbeitet, um den Zugang zu computerisierten personenbezogenen Daten, wie

2

[2] Aus dem für *Faceless* verwendeten Vordruck „Antrag eines Betroffenen um Zugriff auf Videodaten“.

[3] Der Gesetzesauszug zum DPA ist über das UK Information Commissioner’s Office (ICO) zu beziehen: www.ico.gov.uk
Der vollständige Text des DPA (1998) ist zu beziehen über www.opsi.gov.uk/ACTS/acts1998/19980029.htm

1

The *Manifesto for CCTV Filmmakers* was drawn up, permitting the use only of recordings obtained under the DPA. Art would be used to probe the law.

A legal readymade

Vague spectres of menace caught on time-coded surveillance cameras justify an entire network of peeping vulture lenses. A web of indifferent watching devices, sweeping every street, every building, to eliminate the possibility of a past tense, the freedom to forget. There can be no highlights, no special moments: a discreet tyranny of 'now' has been established. 'Real time' in its most pedantic form.[5]

[5] Ian Sinclair *Lights out for the territory* (London: Granta 1998), p. 91

Faceless is a CCTV science fiction fairy tale set in London, the city with the greatest density of surveillance cameras on Earth. The film is made under the constraints of the *Manifesto* — images are obtained from existing CCTV systems by the director/protagonist exercising her rights as a 'surveilled person' under the DPA. Obviously the protagonist has to be present in every frame. To comply with privacy legislation, CCTV operators are obliged to render other people in the recordings unidentifiable — typically by erasing their faces, hence the 'faceless' world depicted in the film. The scenario of *Faceless* thus derives from the legal properties of CCTV images.

RealTime orients the life of every citizen. Eating, resting, going to work, getting married—every act is tied to RealTime. And every act leaves a trace of data — a footprint in the snow of noise...[6]

[6] *Faceless* (2007).

The film plays in an eerily familiar city, where the reformed RealTime calendar has dispensed with the past and the future, freeing citizens from guilt and regret, anxiety and fear. Without memory or anticipation, faces have become vestigial — the population is literally faceless. Unimaginable happiness abounds — until a woman recovers her face.... There was no traditional shooting script: the plot evolved during the four-year long process of obtaining images. Scenes were planned in particular locations, but the CCTV recordings were not always obtainable, so the story had to be continually rewritten.

Faceless treats the CCTV image as an example of a legal readymade (*objet trouvé*). The medium, in the sense of 'raw materials that are transformed into artwork', is not adequately

---

1
Still from* Faceless *(2007)

2
Still from* Faceless *(2007)

etwa medizinischen und buchhalterischen Aufzeichnungen, zu ermöglichen und zu regulieren. Durch eine spätere EU-Richtlinie wurden der Datenschutz und der Aufgabenbereich des DPA (1998) auf Aufzeichnungen von Videoüberwachungsanlagen ausgedehnt. Abgesehen vom DPA müssen Betreiber von Videoüberwachungsanlagen weitere Gesetze befolgen, die sich auf Menschenrechte, das Recht auf Privatheit und kriminalpolizeiliche Ermittlungen, wie sie im *CCTV Code of Practice*[4] festgelegt sind, beziehen.

Als die ersten Anträge für Zugriff auf Videodaten insofern erfolgreich waren, als CCTV-Aufzeichnungen für *The Spy School* freigegeben wurden, stellte sich die Frage, wie stabil die gesetzlichen Rahmenbedingungen denn waren. Das *Manifest für CCTV-Filmemacher* wurde verfasst, demzufolge lediglich die Verwendung von Aufzeichnungen gestattet ist, die mithilfe des DPA erlangt wurden. Das Gesetz sollte mit den Mitteln der Kunst überprüft werden.

2

[4] www.ico.gov.uk

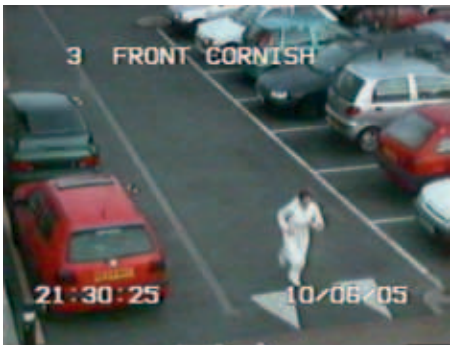
Ein gesetzliches Readymade

Undeutliche Schreckgespenster einer Bedrohung, die über zeitkodierte Überwachungskameras festgehalten wurden, rechtfertigen ein umfassendes Netz voyeuristischer Kameralinsen. Ein Netz teilnahmsloser Beobachtungsgeräte, die jede Straße, jedes Gebäude abtasten, um die Möglichkeit einer Vergangenheit, die freie Wahl, etwas zu vergessen, auszuschalten. Glanzpunkte, besondere Augenblicke kann es nicht mehr geben: Eine diskrete Tyrannei des „Jetzt" ist im Entstehen. „Realzeit" in ihrer pedantischsten Ausprägung.[5]

[5] Sinclair, Ian *Lights out for the territory* (London: Granta 1998), S. 91

Faceless ist ein CCTV-Science Fiction Märchen, das in London, der Stadt mit der weltweit größten Dichte an Überwachungskameras, spielt. Der Film wurde nach den Vorgaben des *Manifests* produziert: die Bilder stammen aus bestehenden CCTV-Anlagen und wurden von der Regisseurin/Protagonistin beschafft, indem sie ihre Rechte als „überwachte Person" gemäß des DPA wahrnahm.

Begreiflicherweise ist die Protagonistin in jedem Bild präsent. Durch die gesetzlichen Auflagen zum Schutz der Privatheit sind die CCTV-Betreiber dazu verpflichtet, dafür zu sorgen, dass keine der anderen Personen in den Aufzeichnungen identifizierbar ist. Im Allgemeinen erfüllen sie diese Anforderung, indem sie deren Gesichter unkenntlich machen. Dies erklärt die



1

described as simply video or even captured light. More accurately, the medium comprises images that exist contingent on particular social and legal circumstances — essentially, images with a legal superstructure. *Faceless* interrogates the laws that govern the video surveillance of society and the codes of communication that articulate their operation, and in both its mode of coming into being and its plot, develops a specific critique.

Reclaiming the data body

Through putting the DPA into practice and observing the consequences over a long exposure, close-up, subtle developments of the law were made visible and its strengths and lacunae revealed.
I can confirm there are no such recordings of yourself from that date, our recording system was not working at that time. (11/2003)
Many data requests had negative outcomes because either the surveillance camera, or the recorder, or the entire CCTV system in question was not operational. Such a situation constitutes an illegal use of CCTV: the law demands that operators comply with the DPA by making sure that the equipment works properly[7].

In some instances, the non-functionality of the system was only revealed to its operators when a subject access request was made. In the case below, the CCTV system had been installed two years prior to the request:
Upon receipt of your letter [...] enclosing the required £10 fee, I have been sourcing a company who would edit these tapes to preserve the privacy of other individuals who had not consented to disclosure. [...] I was informed [...] that all tapes on site were blank. [...W]hen the engineer was called he confirmed that the machine had not been working since its installation. Unfortunately there is nothing further that can be done regarding the tapes, and I can only apologise for all the inconvenience you have been caused. (11/2003)

Technical failures on this scale were common. Gross human errors were also readily admitted to:
As I had advised you in my previous letter, a request was made to remove the tape and for it not to be destroyed. Unhappily this request was not carried out and the tape was wiped according with the standard tape retention policy employed by [deleted]. Please accept my apologies for this and assurance

[7] *CCTV Systems and the Data Protection Act 1998*, available from www.ico.gov.uk

---
1
Still from* Faceless *(2007)

2
Still from* Faceless *(2007)

„gesichtslose“ Welt des Films. Das Drehbuch von *Faceless* lässt auf die gesetzlichen Eigenschaften der Bilder zurückschliessen.

EchtZeit bestimmt das Leben aller Bewohner. Arbeiten, ruhen, essen, heiraten – jede Handlung passiert im Takt der EchtZeit. Und jede Handlung hinterlässt eine Spur – einen Fußabdruck am Strand des Datenmeeres.[6]

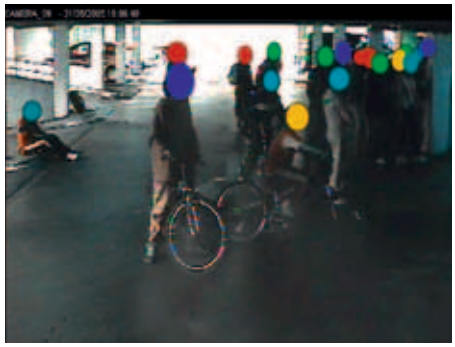
Der Film spielt in einer geradezu unheimlich vertrauten Stadt, in der ein neu eingeführter Echtzeitkalender Vergangenheit und Zukunft abschafft. Die Bürger sind endlich von Schuldgefühlen und Zukunftsangst befreit. Ohne Gedächtnis oder Erwartung verblassten die Gesichtszüge und die Bevölkerung wurde sprichwörtlich gesichtslos. Eine Zeit unvorstellbaren Glücks begann – bis eine Frau ihr Gesicht wiedererlangt …

Es gab kein Drehbuch im herkömmlichen Sinn: Der Plot entwickelte sich während des vierjährigen Prozesses der Bilderlangung. Einige Szenen wurden zwar geplant, doch die Aufzeichnungen aus der Videoüberwachung waren oft nicht erhältlich, weshalb die Geschichte ständig umgeschrieben werden musste.

Faceless definiert das CCTV-Bild als Beispiel für ein rechtliches Readymade (*objet trouvé*). Das Medium ist nicht einfach als Video oder fixiertes Licht adäquat zu beschreiben. Genauer gesagt, besteht das Medium aus Bildern, die kontingent unter bestimmten gesellschaftlichen und gesetzlichen Bedingungen existieren – im Wesentlichen aus Bildern mit einem rechtlichen Überbau. Der Film *Faceless* hinterfragt die Gesetze, die Datensammeln und -verwalten regeln, als auch die Kommunikationscodes, die mit der Umsetzung dieser Gesetze einhergehen, und ist sowohl durch seine eine Entstehungsweise als auch durch seinen Plot eine Form von Kritik.

Die Einforderung des Datenprofils

Da der DPA von der Filmemacherin über einen langen Zeitraum hinweg angewendet und seine Auswirkungen beobachtet wurden, konnten Veränderungen des Gesetzes, seine Stärken und Schwächen, im Detail aufgezeigt werden.
Ich kann bestätigen, dass es von Ihnen zum genannten Zeitpunkt keine Aufzeichnungen gibt. Unser Aufzeichnungsgerät war zu dieser Zeit außer Betrieb. (11/2003)
Die meisten Antworten fielen negativ aus, weil entweder die Überwachungskamera in Frage oder das Aufnahmegerät oder



2

[6] *Faceless* (2007)

1

that steps have been taken to ensure a similar mistake does not happen again. (10/2003)

Some responses were simply mysterious (data request made after spending an hour below several cameras installed in a train carriage):
We have carried out a careful review of all relevant tapes and we confirm that we have no images of you in our control. (06/2005)
Could such a denial simply be an excuse not to comply with the costly demands of the DPA?

Many older cameras deliver image quality so poor that faces are unrecognisable. In such cases the operator fails in the obligation to run CCTV for the declared purposes:
You will note that yourself and a indistinct in the tape, but the picture you sent to us shows you wearing a similar fur coat, and our main identification had been made through this and your description of the location. (07/2002)
To release data on the basis of such weak identification compounds the failure.

Much confusion is caused by the obligation to protect the privacy of third parties in the images. Several data controllers claimed that this relieved them of their duty to release images:
[…W]e are not able to supply you with the images you requested because to do so would involve disclosure of information and images relating to other persons who can be identified from the tape and we are not in a position to obtain their consent to disclosure of the images. Further, it is simply not possible for us to eradicate the other images. I would refer you to section 7 of the Data Protection Act 1998 and in particular Section 7 (4). (11/2003)
– even though the section referred to states that it is 'not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise'.

Where video is concerned, anonymisation of third parties is an expensive, labour-intensive procedure— one common technique is to occlude each head with a black oval. Data controllers may only charge the statutory maximum of £10 per request, though not all seemed to be aware of this:
It was our understanding that a charge for production of the tape should be borne by the person making the enquiry,

---

1
Rotakin test target developed by UK police for evaluating the performance of CCTV systems

2
Police surveillance van for combatting street crime and nuisance, Manchester, 2007
Photo: Mukul Patel

die gesamte CCTV-Anlage nicht funktionstüchtig war. Das entspricht einer illegalen Verwendung der Anlage: Das Gesetz schreibt vor, dass die Geräte funktional sein müssen[7].

In einigen Fällen bemerkten die Betreiber erst als sie das Ansuchen erhielten, dass das System nicht funktionierte. Im folgenden Fall war die CCTV-Anlage zwei Jahre vor der Anfrage installiert worden:
Nach Erhalt Ihres Schreibens [...] und der erforderlichen Gebühr von £10 habe ich eine Firma zur Bearbeitung dieser Bänder gesucht, um die Privatheit anderer Personen, die der Freigabe nicht zustimmten, zu gewährleisten. [...] Man teilte mir mit, [...] dass alle Bänder leer wären. [...] A]ls der Techniker beigezogen wurde, bestätigte er, dass das Gerät seit seiner Installation nicht in Betrieb war. Wir bedauern, dass wir in dieser Angelegenheit nichts für Sie tun können und ersuchen Sie um Nachsicht für die Unannehmlichkeiten, die Sie hatten. (11/2003)

Technische Ausfälle dieser Größenordnung waren nichts Seltenes. Auch grobes menschliches Versagen wurde immer wieder eingestanden:
Wie ich Ihnen in meinem vorangegangenen Schreiben mitteilte, hatten wir beantragt, das Videoband beiseite zu legen, damit es nicht gelöscht wird. Bedauerlicherweise wurde diesem Ansuchen nicht Folge geleistet und das Band wurde gemäß der bei [Name unkenntlich gemacht] üblichen Aufbewahrungsfrist gelöscht. Ich ersuche um Nachsicht und versichere Ihnen, dass Schritte unternommen wurden, um in Zukunft derartige Fehler zu vermeiden. (10/2003)

Einige Antworten konnte man nur als mysteriös bezeichnen (folgendes Ansuchen wurde nach einem einstündigen Aufenthalt vor mehreren Kameras in einem Zug gestellt):
Wir haben alle relevanten Bänder sorgfältig geprüft und versichern Ihnen, dass wir über keine Bilder von Ihnen verfügen. (06/2005)
Ist eine solche Verleugnung von Tatsachen möglicherweise nur ein Vorwand, um die kostspieligen Auflagen des DPA nicht erfüllen zu müssen?

Viele ältere Kameras liefern derartig schlechte Bilder, dass kein einziges Gesicht erkennbar ist. Abgesehen von anderen Konsequenzen, gilt auch dies als illegaler Betrieb einer Videoüberwachungsanlage:
Sie werden bemerken, dass die Gesichter von Ihnen und Ihrem

2

[7] CCTV Systems and the Data Protection Act 1998, www.ico.gov.uk

1

of course we will now be checking into that for clarification. Meanwhile please accept the enclosed video tape with compliments of [deleted], with no charge to yourself. (07/2002)

Visually provocative and symbolically charged as the occluded heads are, they do not necessarily guarantee anonymity. The erasure of a face may be insufficient if the third party is known to the person requesting images. Only one data controller undeniably (and elegantly) met the demands of third party privacy, by masking everything but the data subject, who was framed in a keyhole. (This was an uncommented second offering; the first tape sent was unprocessed).

One CCTV operator discovered a useful loophole in the DPA:
I should point out that we reserve the right, in accordance with Section 8(2) of the Data Protection Act, not to provide you with copies of the information requested if to do so would take 'disproportionate effort'. (12/2004)
What counts as 'disproportionate effort'? The 'gold standard' was set by an institution whose approach was almost baroque — they delivered hard copies of several hundred relevant frames from the time-lapse camera, with third parties' heads cut out, apparently with nail scissors. Two documents had (accidentally?) slipped in between the printouts — one a letter from a junior employee tendering her resignation (was it connected with the beheading job?), and the other an ironic memo:
And the good news — I enclose the £10 fee to be passed to the branch sundry income account. (Head of Security, internal communication 09/2003)

From 2004, the process of obtaining images became much more difficult:
It is clear from your letter that you are aware of the provisions of the Data Protection Act and that being the case I am sure you are aware of the principles in the recent Court of Appeal decision in the case of Durant vs Financial Services Authority. *It is my view that the footage you have requested is not 'personal data' and therefore [deleted] will not be releasing to you the footage which you have requested.* (12/2004)

Under British common law, judgements set precedents. The decision in the case *Durant vs Financial Service Authority* (2003) redefined 'personal data'; since then, simply featuring in raw video data does not give a data subject the right to obtain copies of the recording. Only if something of a 'biographical nature' is revealed does the subject retain the right.

1
Still from* Faceless *(2007)

2
Still from* Faceless *(2007)

Kollegen in dem Video ziemlich undeutlich sind. Auf dem Bild, das Sie uns schickten, tragen Sie jedoch einen ähnlichen Pelzmantel, sodass wir Sie hauptsächlich durch diesen Pelzmantel und Ihre Ortsangabe identifizieren konnten. (07/2002)
Daten, die auf Basis so vager Angaben ermittelt werden, dürften eigentlich nicht freigegeben werden.

Die Verpflichtung, die Privatsphäre abgebildeter Dritter zu schützen, stiftete große Verwirrung. Das führte mehrmals soweit, dass Betreiber sich der Pflicht, die Bildinformation zugänglich zu machen, enthoben glaubten:
[…W]ir können Ihnen die angeforderten Aufnahmen nicht aushändigen, da ansonsten Informationen über und Bilder von anderen Personen, die auf dem Video identifizierbar sind, preisgegeben würden. Es ist uns leider nicht möglich, deren Zustimmung zur Herausgabe der Bilder einzuholen. Außerdem ist es uns nicht möglich, diese Bilddetails zu löschen. Ich verweise auf den Abschnitt 7 des DPA 1998 und insbesondere auf Abschnitt 7 (4). (11/2003)
In dem genannten Abschnitt wird betont, dass Betreiber soviel der angesuchten Information wie möglich weiterzuvermitteln haben. Dabei muss vermieden werden, die Identität von Dritten, sei es namentlich oder durch andere indentifizierbare Besonderheiten preiszugeben.

Im Fall von Video ist die Anonymisierung Dritter ein kostspieliges, aufwändiges Verfahren. Eine weitverbreitete Methode besteht darin, jeden Kopf durch ein schwarzes Oval abzudecken. Die gesetzlich vorgeschriebene Pauschalgebühr pro Anfrage beträgt £10, obwohl das nicht alle zu wissen schienen:
Wir gingen davon aus, dass die Kosten für die Videonachbearbeitung von der ansuchenden Person übernommen werden, wobei wir diesen Punkt natürlich noch überprüfen werden. In der Zwischenzeit übermitteln wir Ihnen das Videoband mit den besten Grüßen von [Firmenname unkenntlich gemacht] – und zwar gebührenfrei. (07/2002)

Die anonymisierten Köpfe – visuell provokant und symbolisch aufgeladenen–, garantieren nicht unbedingt Schutz der Privatheit. Das Ausschwärzen eines Gesichts kann unzureichend sein, wenn die Drittperson demjenigen, der die Bilder anfordert, bekannt ist. Nur ein einziger Betreiber hat eine gültige Lösung gefunden, nämlich die “Schlüssellochmaske”, die alles ausser den erkennbaren Betroffenen abdeckte. (Es handelt sich dabei um ein vom Betreiber ohne Kommentar

2


BBC NEWS CHANNEL

Page last updated at 13:52 GMT, Wednesday, 11 June 2008 14:52 UK

E-mail this to a friend Printable version

Thief uses CCTV camera as mirror

A thief stole a chain from a teenager on a tram in south-east London and then tried it on - checking his reflection in the CCTV camera lens, police said.

Officers said the suspect snatched the chain and a bracelet from a 16-year-old boy in Bromley on 23 March.

The suspect threatened to stab the

1

Having considered the matter carefully, we do not believe that the information we hold has the necessary relevance or proximity to you. Accordingly we do not believe that we are obligated to provide you with a copy pursuant to the Data Protection Act 1988. In particular, we would remark that the video is not biographical of you in any significant way. (11/2004)

Further, with the introduction of cameras that pan and zoom, being filmed as part of a crowd by a static camera is no longer grounds for a data request:
[T]he Information Commissioners office have indicated that this would not constitute your personal data as the system has been set up to monitor the area and not one individual. (09/2005)

As awareness of the importance of data rights grows, so the actual provision of those rights diminishes:
I draw your attention to CCTV systems and the Data Protection Act 1998 (DPA) Guidance Note on when the Act applies. Under the guidance notes our CCTV system is no longer covered by the DPA [because] we:
– only have a couple of cameras
– cannot move them remotely
– just record on video whatever the cameras pick up
– only give the recorded images to the police to investigate an incident on our premises (05/2004)

Data retention periods (which data controllers define themselves) also constitute a hazard to the CCTV filmmaker:
Thank you for your letter dated 9 November addressed to our Newcastle store, who have passed it to me for reply. Unfortunately, your letter was delayed in the post to me and only received this week. [...]There was nothing on the tapes that you requested that caused the store to retain the tape beyond the normal retention period and therefore CCTV footage from 28 October and 2 November is no longer available. (12/2004)

Amidst this sorry litany of malfunctioning equipment, erased tapes, lost letters and sheer evasiveness, one CCTV operator did produce reasonable justification for not being able to deliver images:
We are not in a position to advise whether or not we collected any images of you at [deleted]. The tapes for the requested period at [deleted] had been passed to the police before your request was received in order to assist their investigations into various activities at [deleted] during the carnival. (10/2003)

1
An ingenious use for a CCTV camera, probably unintended by the manufacturer.
BBC News, 11 June 2008

2
Advertisement for a GPS car navigation system with a database of 'safety' (traffic enforcement) cameras.
Photo: Mukul Patel

übermitteltes zweites Band, nachdem das erste völlig unbearbeitet ausgehändigt worden war.) Ein CCTV-Betreiber entdeckte eine opportune Gesetzeslücke im DPA:
Ich sollte darauf hinweisen, dass wir uns – gemäß Abschnitt 8(2) des Data Protection Act – das Recht vorbehalten, Ihnen keine Kopien der angeforderten Daten zu übermitteln, da dies einen „unverhältnismäßigen Aufwand" impliziert. (12/2004)

Was gilt als „unverhältnismäßiger Aufwand"? Alle Rekorde diesbezüglich schlug eine Institution, deren Vorgangsweise fast als barock bezeichnet werden kann: hunderte von Einzelbildern wurden auf Papier ausgedruckt, und die Köpfe der Drittpersonen waren allem Anschein nach mit Nagelscheren ausgeschnitten worden. Zwei Dokumente waren (zufällig?) zwischen die Ausdrucke gerutscht – ein Brief einer jungen Angestellten, die ihre Kündigung einreichte (besteht womöglich ein Zusammenhang mit dem Job, Köpfe auszuschneiden?), und eine ironische Notiz:
Und die erfreuliche Nachricht – ich lege die Gebühr von £10 bei, damit sie auf das Konto Verschiedenes überwiesen werden kann.
(Sicherheitschef, interne Kommunikation 09/2003).

Ab 2004 wurde das Verfahren erheblich erschwert.
Aus Ihrem Brief geht hervor, dass Sie die Bestimmungen des Data Protection Act kennen, daher bin ich sicher, dass Sie auch über die Richtlinien des jüngsten Entscheids des Berufungsgerichts im Fall Durant versus Financial Services Authority *informiert sind. Meiner Ansicht nach fällt das von Ihnen verlangte Filmmaterial nicht unter „persönliche Daten", weshalb wir [Name unkenntlich gemacht] Ihnen das angeforderte Filmmaterial nicht aushändigen werden.* (12/2004)

Im britischen Rechtssystem, das auf dem Gewohnheitsrecht basiert, haben Urteile Präzedenzcharakter. Die Entscheidung im Fall *Durant versus Financial Services Authority* (Finanzdienstleistungsbehörde; 2003) hat den Begriff „personenbezogene Daten" neu definiert; seither hat ein Betroffener nicht mehr das Recht, Kopien der Aufzeichnungen zu erhalten, nur weil er auf den Originalaufnahmen zu sehen ist. Dieses Recht hat er nur, wenn Informationen „biografischer Art" preisgegeben werden:
Nach sorgfältiger Erwägung der Angelegenheit glauben wir nicht, dass die Information, über die wir verfügen, die nötige Relevanz bezüglich Ihrer Person haben. Demgemäß glauben wir nicht, dass wir verpflichtet sind, Ihnen entsprechend des Data Protection Act 1998 eine Kopie auszuhändigen. Insbesondere möchten wir anmerken, dass das Video keine in irgendeiner Weise aussagekräftigen biografischen Details über Sie enthält. (11/2004)

2

The Guardian | Friday April 11 2008

National

Council uses criminal law to spy on school place applicants

Couple's anger over surveillance admission

Officials accused of playing James Bond

have contacted us or come and kno on the door rather than opting for sur lance, which is completely underha The woman, who lived in the Parks area of Poole, said her daughter was ing trouble sleeping because she feare man outside watching us".

1

In the shadow of the shadow

There is debate about the efficacy, value for money, quality of implementation, political legitimacy, and cultural impact of CCTV systems in the UK. While CCTV has been vital in solving some high profile cases (e.g. the 1999 London nail bomber, or the 1993 murder of James Bulger), at other times it has been strangely impotent (e.g. the 2005 police killing of Jean Charles de Menezes).

The prime promulgators of CCTV may have lost some faith: during the 1990s the UK Home Office spent 78% of it crime prevention budget on installing CCTV, but in 2005, an evaluation report by the same office concluded that the CCTV schemes that have been assessed had little overall effect on crime levels[8].

The public perception is rather different. Attitudes remain generally favourable, though concerns have been voiced recently about 'function creep' (prompted, for example, by the disclosure that the cameras policing London's Congestion Charge remain switched on outside charging hours).

Confidence in the technology remains high; though as the realities of its daily operation become more widely known, this may be somewhat tempered. Physical bodies leave data traces: shadows of presence, conversation, movement. Networked databases incorporate these traces into data bodies, whose behaviour and risk are priorities for analysis (by business, by government). The securing of a data body is supposedly necessary to secure the human body (either preventively or as a forensic tool). But if the former cannot be assured, what grounds are there for trust in the promise of the latter?

The panopticon is not complete, yet. Regardless, could its one-way gaze ever assure an enabling conception of security?

{8} Gill, M. and Spriggs, A.: 'Assessing the impact of CCTV', pp. 60–61 (London: Home Office Research, Development and Statistics Directorate, 2005)

The full text of the DPA (1998) is at www.opsi.gov.uk/ACTS/acts1998/19980029.htm

---

1
Article in The Guardian, *11 April 2008*

2
Article in London Lite, *6 September 2008*

Die technische Möglichkeit per Schwenk und Zoomfunktion das Augenmerk auf eine Person zu richten, dient seitdem als Merkmal für personenbezogene Daten. Wurde man hingegen mit einer statischen Kamera etwa inmitten einer Menschenmenge gefilmt, qualifizeren sich die Aufnahmen nicht als Daten biografischer Natur:
[D]as Information Commissioner's Office bezeugte, dass es sich in diesem Fall nicht um personenbezogene Daten handelt, da das System eingerichtet wurde, um ein Gebiet und nicht eine Einzelperson zu überwachen. (09/2005)

Während das Bewusstsein der Öffentlichkeit gegenüber Datenrechte ansteigt, wird die Umsetzung derselben immer schwieriger:
Ich verweise auf den Text „CCTV Systems and the Data Protection Act 1998 Guidance Note on when the Act applies". Diesem Dokument zufolge fällt unsere Videoüberwachungsanlage nicht länger unter den DPA, [weil] wir: nur einige Kameras haben; diese nicht fernbedienen können; nur auf Video aufnehmen, was zufällig in das Blickfeld der Kamera kommt; die Aufnahmen lediglich der Polizei zur Untersuchung von Vorfällen auf unserem Gelände aushändigen. (05/2004)

Auch die Zeitspanne der Datenvorratsspeicherung (die von den verantwortlichen Stellen selbst definiert wird) ist für den CCTV-Filmemacher oft ein Unsicherheitsfaktor:
Besten Dank für Ihr an unser Geschäft in Newcastle adressiertes Schreiben vom 9. November, das an mich weitergeleitet wurde. Bedauerlicherweise erhielt ich den Brief durch eine Verzögerung auf dem Postweg erst diese Woche. [...] Es befanden sich keine der von Ihnen angeforderten Bilder auf den Videobändern, die Anlass gegeben hätten, die Videobänder über den üblichen Speicherungszeitraum hinaus aufzubewahren, weshalb das Filmmaterial der Videoüberwachungsaufnahmen vom 28. Oktober und 2. November nicht mehr verfügbar ist. (12/2004)

Inmitten dieser Litanei an Ausreden, die disfunktionale Geräte, gelöschte Bänder, verlorene Briefe oder legale Schlüpflöcher inkludieren, befand sich eine einzige verständliche Rechtfertigung, warum keine Bilder geliefert konnte:
Wir können Ihnen nicht mitteilen, ob wir im [unkennlich gemacht] Bilder von Ihnen aufnahmen. Die Bänder für den gewünschten Zeitraum wurden bereits vor Erhalt Ihrer Anfrage der Polizei übergeben, um deren Untersuchungen verschiedener Aktivitäten am [unkennlich gemacht] während des Karnevals zu unterstützen. (10/2003)


Councils recruit kids as 'spies'

● LONDON children as young as eight have been hired by councils to snoop on neighbours and report petty offences such as littering. Boroughs across the UK, including Ealing, Bromley, Enfield, Southwark and Waltham Forest, have hired 5,000 "covert intelligence sources".

2

Im Schatten des Schattens

Man diskutiert über Effizienz, Qualität der Ausführung, politische Legitimität und kulturelle Auswirkungen der CCTV-Anlagen in Großbritannien. Während Videoüberwachung bei der Lösung einiger Fälle, die grosse Beachtung in den Medien fanden, eine wesentliche Rolle spielte (z. B. 1999 beim Fall des Londoner Nagelbombers oder 1993 im Mordfall von James Bulger), erwiesen sie sich in anderen Fällen als seltsam nutzlos (z.B. 2005 als Jean Charles de Menezes von der Polizei ermordet wurde). Die eifrigsten Verfechter der Videoüberwachung scheinen bereits ihren Glauben an dieses Allheilzweckmittel verloren zu haben. In den 1990er Jahren investierte das britische Innenministerium 78 % des Präventivbudgets gegen Kriminalität in CCTV. In einem Evaluationsbericht aus dem Jahr 2005 kam dieselbe Stelle zu dem Schluss, dass die bewerteten CCTV-Modelle wenig Auswirkung auf die Kriminalitätsrate hatten[8].

Die öffentliche Wahrnehmung sieht anders aus. Überwiegend ist die Öffentlichkeit positiv eingestellt, obwohl in jüngerer Zeit Bedenken über Zweckentfremdung laut wurden (ausgelöst beispielsweise durch die Enthüllung, dass die Kameras, die in London die Bezahlung der Innenstadtmaut überwachen, auch außerhalb der gebührenpflichtigen Zeit eingeschaltet bleiben). Das Vertrauen in die Technologie ist zwar nach wie vor hoch, könnte aber schwinden, sollten die tatsächlichen Umstände des täglichen Betriebs bekannter werden.

Physische Körper hinterlassen Datenspuren: Schatten der Anwesenheit, Gespräche, Bewegung. Vernetzte Datenbanken verdichten diese Spuren zu einem „Datenkörper", dessen Verhalten und Risiko im Zentrum von Analysen (der Wirtschaft und der Regierung) stehen. Die Sicherstellung eines „Datenkörpers" ist angeblich notwendig, um den menschlichen Körper zu schützen (präventiv, oder als forensisches Hilfsmittel). Wenn Ersteres nicht gewährleistet werden kann, warum sollte man daran glauben, dass Letzteres funktioniert?

Das panoptische System ist (noch) nicht komplett. Es stellt sich aber die dringende Frage: Kann der Einwegblick jemals als Grundlage eines Sicherheitskonzeptes dienen, das vorgibt, die Betroffenen zu bevollmächtigen, sie zur Mitverantwortung und Teilnahme aufzufordern?

Ministry loses 45,000 secret files

By Christopher Hope

THE personal details of 45,000 people, including dates of birth, criminal records, National Insurance numbers and court information, were lost by a single Government department last year.

The Ministry of Justice's (MoJ) annual accounts show that the data was lost in nine separate incidents in the past financial year.

The worst loss, in June last year, saw civil servants lose the names, addresses and some bank details of 27,000 people working for suppliers to the MoJ.

Officials at the Ministry of Justice also violated an "inadequately protected" laptop containing the job applications of 13 people who were applying for judicial posts.

The losses are the latest in a list of data blunders by Government departments, which included the loss of two CDs containing the entire child benefit database of 25 million families. The CDs are still missing.

The police were informed about six of the nine latest losses while 39,000 of the 45,000 people affected were not told that the MoJ had lost their details.

The information was being held on "inadequately protected electronic storage devices", thought to be memory sticks.

There was another major error in January this year when officials lost an "inadequately protected" laptop in a secured Government office.

The computer contained the names, dates of birth, addresses and offence details of 16,000 "low defenders", including the National Insurance numbers in one fifth of the cases.

The Liberal Democrats' justice spokesman, David Howarth MP said: "Yet again the Government has shown that it cannot be trusted with citizens' personal data.

"How can ministers possibly argue for the introduction of a universal ID Card scheme when they can't even keep safe the data they already have."

An MoJ spokesman said: "Risk assessments were carried out to assess who, if anyone, should be notified and to ensure measures were in place to mitigate risk to individuals and to prevent a recurrence of the incident."

The Government is battling to restore people's trust over the way it handles private information of taxpayers."

Last month, the Ministry of Defence said it had lost 658 laptops over the past four years – more than twice an earlier estimate.

In April the Information Commissioner said he was notified of 94 data breaches since the loss last year of the child benefit database – two thirds were committed by the Government and other public sector bodies.

[8] Gill, M. und Spriggs, A. „Assessing the impact of CCTV" (London: Home Office Research, Development and Statistics Directorate 2005), S. 60–61

***Above:** Article in* The Telegraph*, 16 August 2008*

***Left:** FRAMED: THE MINISTRY, FRAMED: THE TRANSPORT, FRAMED: THE MONEY*
Unique edition of inkjet prints, each 300 x 91 cm (Manu Luksch 2003)
Image courtesy Gallery Barry Keldoulis, Sydney

As I had advised you in my previous letter, a request was made to remove the tape and for it not to be destroyed. Unfortunately this request was not carried out and the tape was wiped in according with the standard tape retention policy.
Please accept my apologies for this and assurance that steps have been taken to ensure a similar mistake does not happen again.
Yours sincerely
Upon receipt of your letter of the 27th September, enclosing the required £10.00 fee, I have been sourcing a company who would edit the tapes to preserve the privacy of other individuals who had not consented to disclosure. Having found a company to do this, I asked the site to forward the tapes to me and was informed that they had discovered that all tapes on site are blank. He advised me there was a technical fault with the CCTV machine and that when the engineer was called he confirmed that the machine had not been working since its installation.
Again please accept my sincerely apologies for not being able to assist you on this occasion. Should you wish to discuss this matter further with me, please do not hesitate to contact me.
Yours sincerely

Above: The Mistake
Chalk writings in public space
(Manu Luksch, 2008)
Adaptation of the Manifesto
by Joseph Beuys (1985)

Left: I wish to apply, under the Data Protection Act, for any and all CCTV images of my person held within your system. I was present at [place] from approximately [time] onwards on [date].
Set of three inkjet prints in light boxes, 150 x 37 cm
(Manu Luksch, 2006)

Charing Cross
Strand
Villiers St
Watergate Walk
Craven Passage
Craven St
Embankment
Northumberland Ave
Whitehall
Craig's Court
Great Scotland Yard
Whitehall Pl
Victoria Embankment
Horse Guards Ave
Downing St
Richmond Terrace
Parliament St
King Charles St
Derby Gate
Cannon Row
Westminster
Great George St
Bridge St

MAPPING CCTV IN WHITEHALL

Two-part exercise to map CCTV cameras around Whitehall, London, within a zone covered by SOCPA (Serious and Organized Crime Prevention Act). A map of the hundreds of cameras in the zone was made over two days of observation. The second part involved mapping the range of one of these cameras, no. 40 in Villiers Street, by intercepting its signal as it was transmitted wirelessly without encryption. As passers-by entered the marked area covered by camera no. 40, they were alerted to the camera's presence and handed a copy of the map of CCTV cameras in Whitehall.

Manu Luksch
2008

Video: DV, 3 mins

Left: Map of CCTV cameras in Whitehall

1
Using the intercepted signal of camera no. 40 to map its range (video still)

2
Marking the range of the camera with tape on the pavement (video still)

1

2

Mukul Patel

2007

FACELESS: NOTES ON SOUND

Sound for the film *Faceless* posed a particular challenge: while the image is clearly and precisely determined by concept and process, the surveillance cameras record no sound. With neither field ambience nor dialogue as a starting point, and no constraints equivalent to those determining the image, the sonic world of the film had to be created ex nihilo.

The soundtrack is composed in 5.1 (five full-frequency channels: left, centre, right, rear left, and rear right, plus subwoofer). I don't use the rear speakers just for special/spatial effects – as point sources, they are as important as the front speakers. For example, there is the 'pulse of RealTime', which ticks clockwise around the viewer throughout the film.

The surround soundtrack helps to overcome the spatial and temporal limitations of the CCTV footage:

– The immersive quality of the soundtrack compensates for the large depth of field and limited range of perspectives of the CCTV cameras, psychologically enlarging or compressing the space. There are no visual close-ups in this film – only sonic ones.

– The ability to move sound right around the audience carries movement in the picture over the chasms of time-lapse recording. (The full-frame-rate errors and jitter in the images also helps).

The 'dream space' in the film – passages are accompanied by Rupert Huber's solo piano – is further distinguished by being the only part in mono or stereo, without the rear speakers. Sonic textures are predominantly 'postindustrial ambient' – not industrial, not even 'light industrial', but more the throb of the service sector.

In late 2006, it became clear that the film needed a voiceover. An early project with the footage (*The Spectral Children*) used intertitles, but the plot grew too complex to be narrated elegantly in this way. It was not only the appropriateness of her voice, but also her longstanding commitment to critical art that made Tilda Swinton the ideal narrator for *Faceless*. Her

voice is placed, classically, in the centre speaker. (We recorded the narration in a couple of hours in a restaurant overlooking the Moray Firth, by her house in Scotland).

The other voices in the film – those of the choir led by Eva Königer, which sings the refrain of the New Machine – are treated in a way that they are difficult to locate, the lyric barely distinguishable, to add a spookiness to the world.

Until a few days before the mastering date, I had no sound for the dance of the Spectral Children. Then, I chanced across an old recording of Paul Zimmerman playing berimbau. Cut up to the image, this was the perfect sound for a dance of rebellion. (Today the berimbau is used in the favelas as a signal warning of police).

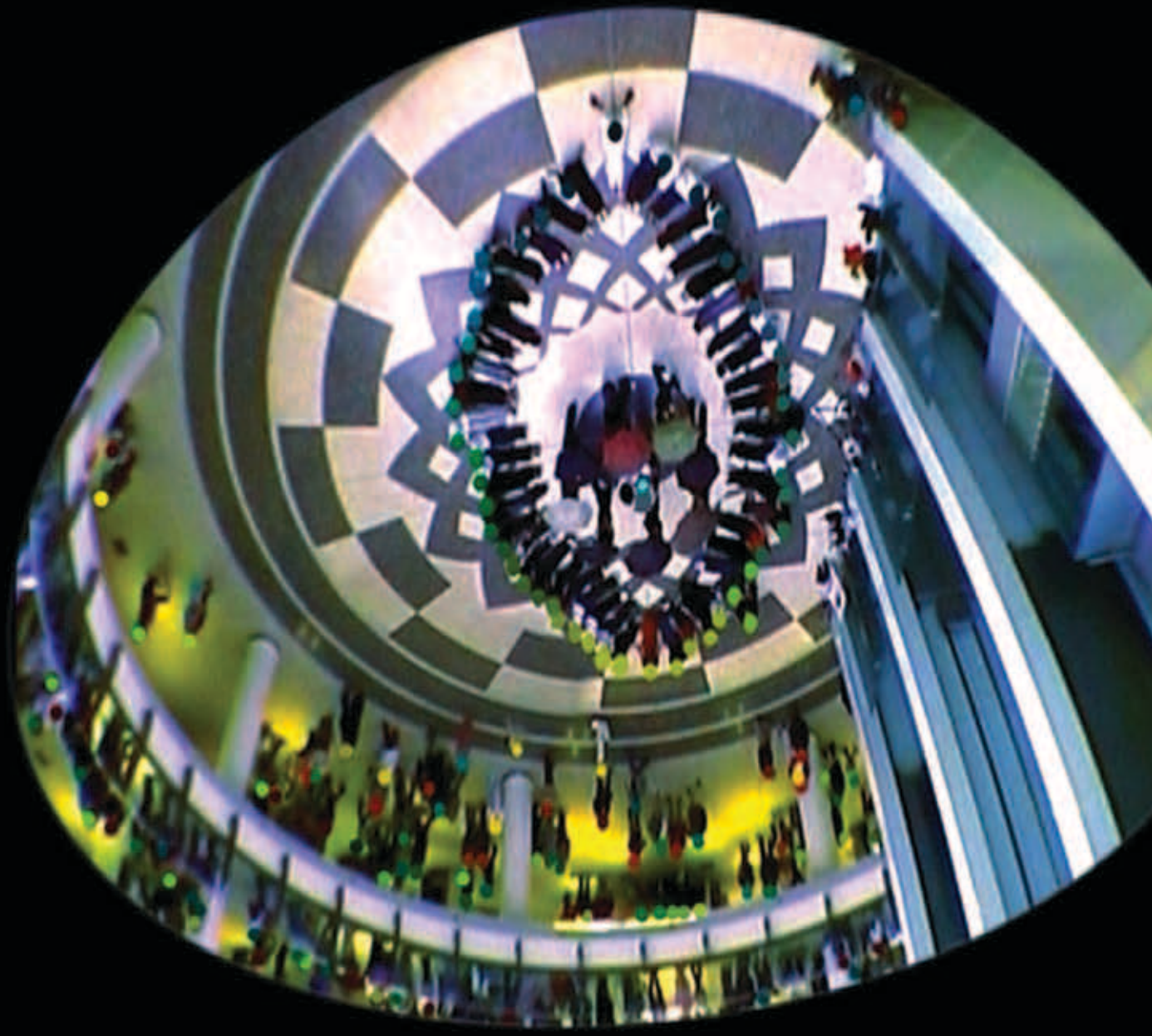
On a final note, there is only one moment of truly diegetic sound in the film – it's hard to miss.

SIDELONG GLANCES

4. The age of spiritual machines

Having elegantly spattered the surrounding surfaces, Rebecca Horn's painting machine – in the *Bodylandscapes* retrospective at the Hayward Gallery, 2005 – lay provocatively quiescent. Had it determined that the work was complete, or had it balked at the prospect of a lawsuit from a Prucci-clad visitor? Either way, Ray Kurzweill ought to be told.

Mukul Patel
2007



THE EYE

The Eye is a site-specific dance piece for 80 performers of all ages, developed as a humourous hommage to Busby Berkeley's Hollywood revue movies. The choreography is filmed from above by surveillance system operators whose vantage point is shared by the audience, and unfolds in kaleidoscopic patterns. The project took place in the atrium of Lakeside Shopping Centre, Essex. A subsequent piece, *The Eye 2*, was conducted with youth dance initiative Alluminae Project for public spaces in the Brentford Housing Estate, West London.

Manu Luksch
2005

Choreography for surveilled space, developed in collaboration with Billy Trevitt & Michael Nunn (The Ballet Boyz ⁄ George Piper Dances)

Far left: Still from **The Eye**

Left: Still from **The Eye 2**

ORCHESTRA OF ANXIETY

Manu Luksch & Mukul Patel
2005

Participatory installation. *Orchestra of Anxiety* was commissioned by Watermans Arts Centre in London.

The *Orchestra of Anxiety* is a collection of instruments that deploy security and surveillance technologies in unusual and playful contexts, prompting visitors to reflect on their personal sense of security and their relationship with public fears (of petty crime, terrorism, etc.). The first instrument to be built is a steel harp with strings of razor wire, which requires the harpist to wear protective gauntlets to play it.

Gallery visitors are invited to play the harp after donning protective chain mail gauntlets. The razor wire 'strings' trigger multiple projections and sound sources. A pedal enables the harpist to loop phrases for accompaniment. The installation has a game-like grammar that can be learned over a few minutes. Initially, a filmed guard dog patrols the walls of the installation space[1]. Touching strings at random triggers a ferocious attack. More musical playing calms the dog and makes him sing. Once the harpist has calmed the guard dog, the installation switches to a second theme: CCTV[2]. The object is to search the initially vacant housing estate grounds for children, and then to make them dance.

In mythology, the harp is regarded as a sacred or metaphysical instrument and is associated with tranquility, love, and goodness around the world. A Biblical story tells of how David exorcised Saul's bad spirit by playing a harp. The razor wire harp has similar powers to drive out evil and madness, but the harpist must first overcome the anxiety that the instrument provokes.

[1] A professional guard dog was directed to attack the camera during the film shoot.

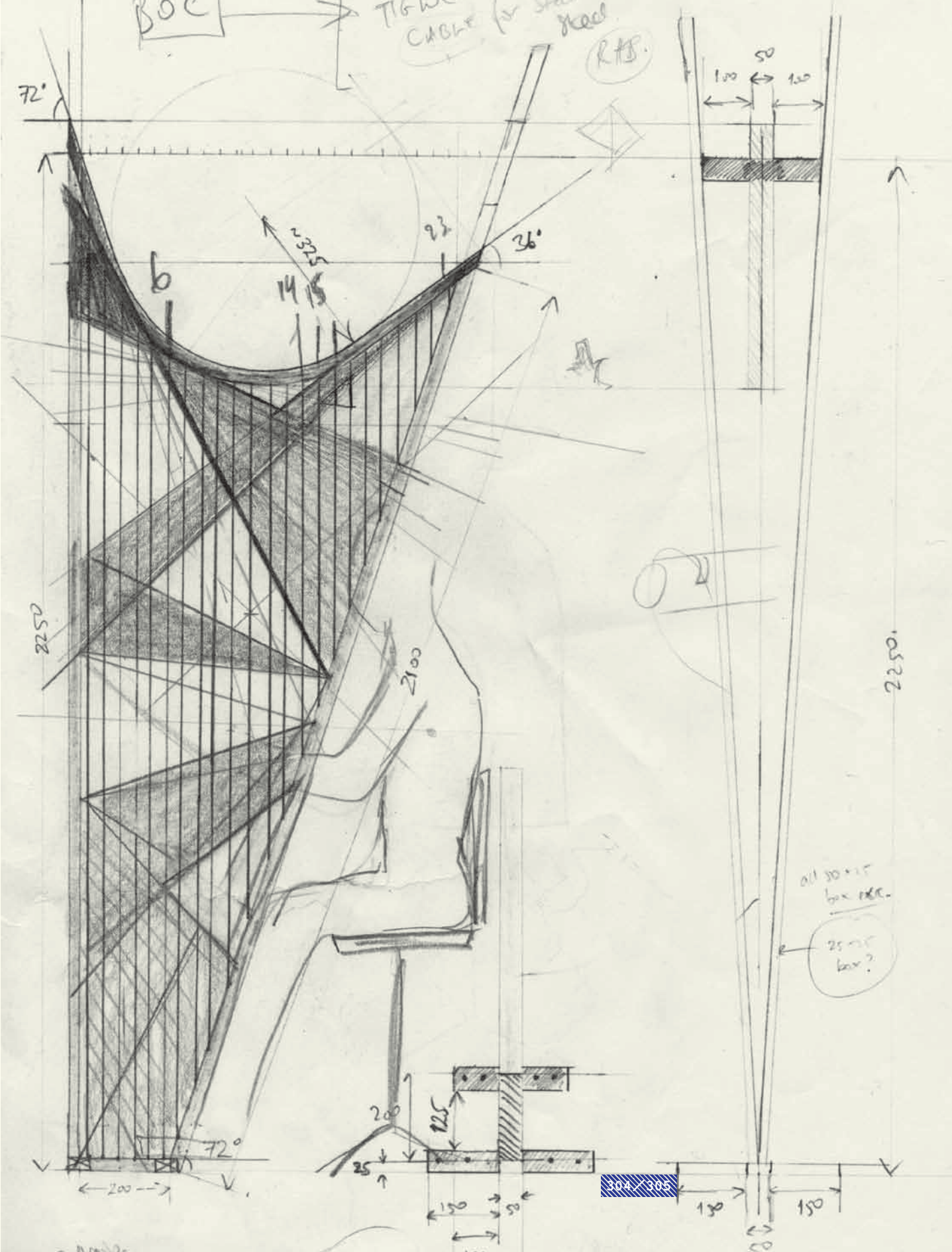
[2] Images were obtained from existing surveillance cameras in a London housing estate. A guerrilla choreography for the public spaces of the estate was developed in collaboration with a youth dance initiative.

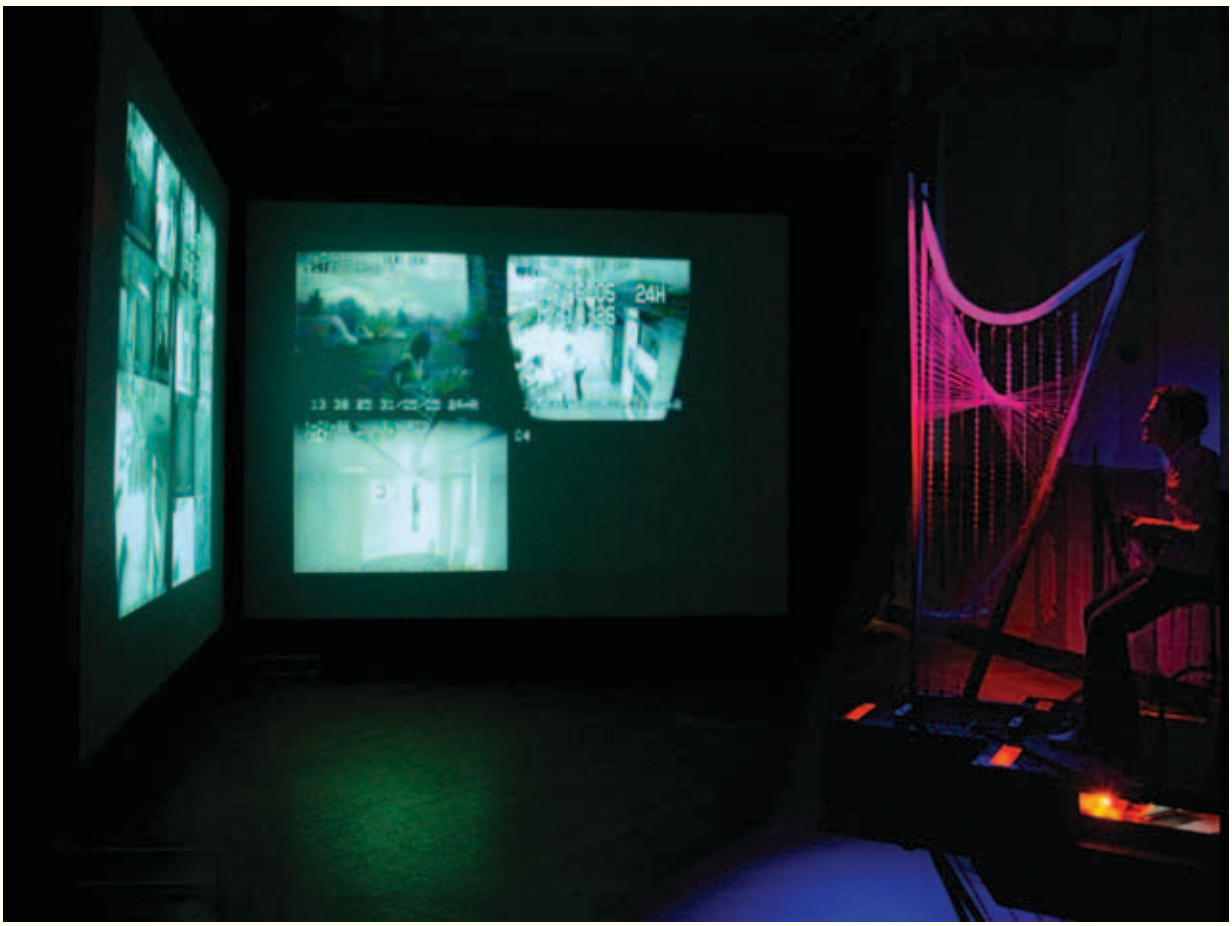
Crowd control

During the installation of the harp at Watermans, the gallery raised concerns over health & safety issues, citing the possibility of children or drunken visitors falling into the razor wire. The exhibition was allowed to open only on the condition that crowd control barriers were erected around it, and that visitors who wanted to play the instrument do so under the supervision of the artists.

Above: Stills from the video shoot with guard dog and handler Tony Heldt, of OmniSecurity. Tony directed the dog to approach, threaten, and attack the camera.

Right: Sketch for harp, with frame angles based on the shape of razor wire blades. Harp constructed in collaboration with engineer and sculptor John Ashworth.


72°
b
14
15
23
36°
2250
2100
200
72°
125
35
150
50
50
150
150
2250



Left: Orchestra of Anxiety *at* SOHO in Ottakring *Festival, Vienna 2006*

Above: Orchestra of Anxiety *at* databodies, *Paradiso, Amsterdam 2006*

The Order
100 portraits: video installation and photographic prints (Manu Luksch, 2009)