Manu Luksch, Mukul Patel

Faceless: Chasing the Data Shadow

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.

CCTV sculpture in a park in London

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. ("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).* Many London buses have five or more cameras inside, plus several outside, including one recording cars that drive in bus lanes.

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 Automated 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) 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 film *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].*
> (from the template for "subject access requests" used for *Faceless)*

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.*
> (Data Protection Act Factsheet available from the UK Information Commissioners Office, *www.ico.gov.uk)*

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 *(www.ico.gov.uk)*.
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. 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.*
> (Ian Sinclair: *Lights out for the territory,* Granta, London, 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.

Still from *Faceless,* 2007

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 ...
(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 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 [...] equipment works properly.*
> (CCTV Systems and the Data Protection Act 1998, available from *www.ico.gov.uk)*

Multiple, conflicting timecode stamps

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

Some responses, such as the following, were just 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 colleague's faces look quite 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.

The Rotakin test, devised by the UK Home Office Police Scientific Development Branch, measures surveillance camera performance.

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, 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:

Off with their heads!

> *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 each of the 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.

> *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)*

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

Still from Faceless, 2007

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 preventatively 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?

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

Manu Luksch, Mukul Patel

Faceless: Die Jagd nach Datenschatten

Seltsamer als jede Fiktion

Ferngesteuerte unbemannte Luftfahrzeuge überfliegen die Stadt auf der Suche nach unsozialem Verhalten. Sprechende Kameras rufen (mit Kinderstimmen) Menschen, die Abfälle auf die Straßen werfen, zur Ordnung. Bildern aus Videoüberwachungsanlagen werden biometrische Daten entnommen, um Passanten über ihr Gesicht oder ihren Gang zu identifizieren. Die Überwachungskameras einer Wohnanlage versorgen den lokalen Kabelkanal mit Bildern und ermöglichen den Bewohnern, sich selbst zu kontrollieren.
Dies sind keine Szenen aus dem Science-Fiction-Film, der Thema dieses Textes ist, sondern Techniken, die heute in Merseyside, Middlesborough, Newham und Shoreditch (GB) zum Einsatz kommen.

Plakat in London

Großbritannien ist heute führend, was die Dichtheit und Raffinesse der Überwachungstechnologien anbelangt. Mit einer geschätzten Anzahl von 4,2 Millionen CCTV-Kameras sind die Einwohner Großbritanniens die meist beobachteten der Welt. *(A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network2,* September, 2006, S. 19. Zu beziehen über http://www.ico.gov.uk). 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 ANPR-Systemen 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 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 dürfen wir nicht die Augen davor verschließen, dass im Namen von Effizienz und Rationalität – und natürlich der Sicherheit – eine ständige wachsende Datenmenge zwischen den Hütern scheinbar nicht vernetzter Aufzeichnungen wie Krankengeschichten, Einkaufsgewohnheiten und Grenzübertritten ausgetauscht wird. Es gibt gesetzliche Rahmenbedingungen zum Schutz der Privatheit, die Datentransfers 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.*
> *(Aus dem für* Faceless *verwendeten Vordruck „Antrag eines Betroffenen um Zugriff auf Videodaten")*

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 (Betroffenen) Rechte zugesteht. Personenbezogene Informationen umfassen sowohl Fakten als auch Meinungen über Einzelpersonen.*
> *(Der Gesetzesauszug zum DPA ist über das* UK Information Commissioner's Office *(ICO) zu beziehen, www.ico.gov.uk.)*

Der DPA (1984) wurde ursprünglich ausgearbeitet, um den Zugang zu computerisierten personenbezogenen Daten, wie 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 erfüllen, die sich auf die Menschenrechte, das Recht auf Privatheit und kriminalpolizeiliche Ermittlungen, wie sie im *CCTV Code of Practice (www.ico.gov.uk)* 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.

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.*
> Sinclair, Ian: *Lights out for the territory*, Granta, London 1998, S. 91

Faceless ist ein CCTV-Sciencefiction-Märchen, das in London, der Stadt mit der weltweit größten Dichte an Überwachungskameras, spielt. Der Film wurde nach den Vorgaben des Manifests gedreht – die Bilder stammen aus bestehenden CCTV-Systemen und wurden eingeholt, indem die Regisseurin/Protagonistin ihre Rechte als „überwachte Person" gemäß 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 andere Person in den Aufzeichnungen identifizierbar ist – im Allgemeinen erfüllen sie diese Anforderung, indem sie deren Gesichter unkenntlich machen. Dies erklärt die „gesichtslose" Welt des Films. Das Drehbuch von *Faceless* lässt sich somit auf die gesetzlichen Vorschriften für Bilder aus Videoüberwachungsanlagen zurückführen.

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 Daten-Meeres.
Faceless, 2007

Der Film spielt in einer geradezu unheimlich vertrauten Stadt, in der ein neu eingeführter Echtzeitkalender Vergangenheit und Zukunft abschafft, wodurch die Bürger von Schuld, Bedauern, und Zukunftsangst befreit sind. Ohne Gedächtnis oder Erwartung verblassten die Gesichtszüge und wurde die Bevölkerung sprichwörtlich gesichtslos. Eine Zeit unvorstellbaren Glücks beginnt – bis eine Frau ihr Gesicht wiedererlangt ...
Es gab kein Drehbuch im herkömmlichen Sinn: Der Plot entwickelte sich während des vierjährigen Prozesses der Bilderlangung. Szenen wurden zwar für bestimmte Orte geplant, doch waren die Aufzeichnungen aus der Videoüberwachung nicht immer erhältlich, weshalb die Geschichte ständig umgeschrieben werden musste.


Standbild aus *Faceless,* 2007

Faceless beschreibt das CCTV-Bild als Beispiel für ein rechtliches Readymade *(objet trouvé).* Das Medium, im Sinne eines „Rohmaterials, das Kunst wird", 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 die Videoüberwachung der Gesellschaft regeln, sowie die Kommunikationscodes, die ihre Umsetzung bestimmen, und ist sowohl durch seine eine Entstehungsweise als auch durch sein Plot eine Form von Kritik.

Die Einforderung des Datenprofils

Da der DPA 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 keine Aufzeichnungen von Ihnen für diesen Zeitpunkt gibt, unser Aufzeichnungssystem war zu dieser Zeit nicht in Betrieb. (11/2003)

Viele Datenanfragen wurden negativ beantwortet, weil entweder die betroffene Überwachungskamera oder das Aufnahmegerät oder das gesamte CCTV-System nicht funktionstüchtig war. Dies kommt einer illegalen Verwendung der Videoüberwachungsanlage gleich: Das Gesetz schreibt vor, dass Betreiber dem DPA Folge zu leisten heben, indem sie dafür sorgen, dass [...] die Geräte funktionieren.
(CCTV Systems and the Data Protection Act 1998, zu beziehen über http://www.ico.gov.uk)

Mehrfache, widersprüchliche Zeitstempel

In einigen Fällen bemerkten die Betreiber erst als ein Antrag gestellt wurde, dass das System nicht funktioniert. Im folgenden Fall war das CCTV-System erst 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 schützen. [...] 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 gang und gäbe. Auch grobes menschliches Versagen wurde bereitwillig eingestanden:

> *Wie ich Ihnen in meinem vorangegangenen Schreiben mitteilte, haben wir beantragt, das Videoband zu entnehmen, damit es nicht gelöscht wird. Bedauerlicherweise wurde diesem Ansuchen nicht Folge geleistet und das Band wurde gemäß der bei [Name unkenntlich gemacht] üblichen Bandspeicherungsvorgabe gelöscht. Ich ersuche um Nachsicht und versichere Ihnen, dass Schritte unternommen wurden, um in Zukunft derartige Fehler zu vermeiden. (10/2003)*

Einige Antworten, wie etwa die folgende, kann man nur als mysteriös bezeichnen (Datenanfrage nach einstündigem Aufenthalt vor mehreren Kameras, die an einem Zugabteil angebracht waren).

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. Auch in solchen Fällen erfüllt der CCTV-Betreiber seine gesetzmässig verankerten Verpflichtungen nicht.

> *Sie werden bemerken, dass die Gesichter von Ihnen und Ihrem 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.*

Daten, die auf Basis so vager Angaben ermittelt werden, dürften ebenfalls nicht freigegeben werden.
Die Verpflichtung, die Privatsphäre abgebildeter Dritter zu schützen, stiftete große Verwirrung. Das führte mehrmals dazu, dass Betreiber sich der Pflicht, Bildinformation zugänglich zu machen, enthoben glaubten.

Der Rotakin-Test, der von der Home Office Police Scientific Development Branch (GB) entwickelt wurde, misst die Effizienz einer Überwachungskamera.

> *[…W]ir können Ihnen die angeforderten Bilder nicht aushändigen, da ansonsten Informationen über und Bilder von anderen Personen, die auf der Videokassette identifizierbar sind, preisgegeben würden. Es ist uns leider nicht möglich, deren Zustimmung zur Herausgabe der Bilder einzuholen. Außerdem ist uns unmöglich, die anderen Bildinformationen herauszulöschen. Ich verweise auf den Abschnitt 7 des* Data Protection Act 1998 *und insbesondere auf Abschnitt 7 (4) (11/2003).*

Obwohl in dem Abschnitt betont wird, dass dies

> *nicht so auszulegen sei, dass es den Betreiber von der Verpflichtung entbindet, soviel der angesuchten Information wie möglich weiterzuvermitteln, ohne dabei 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.
Es darf nur die gesetzlich vorgeschriebene Höchstsumme von £10 pro Anfrage verrechnet werden, obwohl das nicht alle zu wissen schienen:

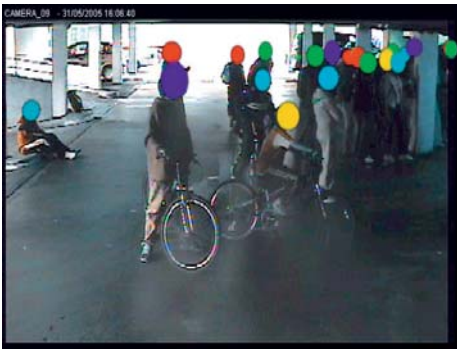
> *Wir gingen davon aus, dass die Kosten für die Nachbearbeitung des Videos von der ansuchenden Person übernommen werden, wobei wir diesen Punkt natürlich noch überprüfen werden. In der Zwischenzeit übermitteln wir Ihnen das Videoband mit den besten Grüßen von [Firmenname unkenntlich gemacht] – und zwar gebührenfrei. (07/2002)*

Die visuell provokanten und symbolisch aufgeladenen, unkenntlich gemachten Köpfe garantieren nicht unbedingt Anonymität. Das Ausschwärzen eines Gesichts kann unzureichend sein, wenn die Drittperson demjenigen, der die Bilder anfordert, bekannt ist. Nur ein CCTV-Betreiber hat die richtige Massnahme zum Schutz der Privatheit Dritter angewendet und die elegante Lösung gefunden den Antragsteller mit einer Negativmaske zu versehen („Schlüssellochmaske"), die alles ausser den erkennbaren Betroffenen abdeckte. (Es handelt sich dabei um ein vom Betreiber ohne Kommentar 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, wenn 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 relevanten Einzelbildern der Zeitrafferaufnahmen 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 – das eine war ein Brief einer jungen Angestelltengehilfin, die ihre Kündigung einreichte (besteht womöglich ein Zusammenhang mit dem Job, Köpfe auszuschneiden?), und das andere eine ironische Notiz:



Standbild aus *Faceless*, 2007

> *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, Bilder einzufordern, erheblich schwieriger.

> *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 Service 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 Informationen, über die wir verfügen, die nötige Relevanz für Sie 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 von Ihnen enthält. (11/2004)*

Weiters liegt seit der Einführung von Schwenks und Zoomfunktionen keine ausreichende Begründung für eine Datenanforderung vor, wenn man mit einer statischen Kamera etwa inmitten einer Menschenmenge gefilmt wurde.

> *[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 die Sensibilität der Öffentlichkeit in Bezug auf Datenrechte ansteigt, wird die Durchsetzung derselben immer schwieriger:

> *Ich verweise auf den Text „CCTV Systems and the Data Protection Act 1998 (DPA) Guidance Note on when the Act applies". Diesem Dokument zufolge fällt unser Videoüberwachungssystem 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 wegen nicht funktionierender technischer Ausstattung, gelöschter Bänder, verlorener Briefe oder reinen Ausflüchten brachte ein CCTV-Betreiber eine vernünftige Rechtfertigung hervor, warum er keine Bilder liefern 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)*

Im Schatten des Schattens

Man diskutiert über Effizienz, Kosten-Nutzen-Rechnung, Qualität der Ausführung, politische Legitimität und kulturelle Auswirkungen der CCTV-Systeme in Großbritannien. Während Videoüberwachung bei der Lösung einiger Fälle, die grosse Beachtung in den Medien fanden, eine wesentliche Rolle spielten (z. B. 1999 beim Fall des Londoner Nagelbombers oder 1993 im Mordfall von James Bulgur), 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 Videoüberwachungn 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.*
> (Gill, M. und Spriggs, A.: *Assessing the impact of CCTV,* Home Office Research, Development and Statistics Directorate, London 2005, S. 60–61)

Standbild aus *Faceless,* 2007

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, der Gespräche, der Bewegung. Vernetzte Datenbanken verdichten diese Spuren zu einem „Datenkörper", dessen Verhalten und Risiko Hauptgegenstand von Analysen sind (seitens der Wirtschaft und der Regierung). Die Sicherstellung eines „Datenkörpers" ist angeblich notwendig, um den menschlichen Körper zu schützen (entweder präventiv oder als forensisches Hilfsmittel). Wenn Ersteres nicht überzeugend 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 einseitige Blick jemals als Grundlage eines Sicherheitskonzeptes dienen, das vorgibt, die Betroffenen zu bevollmächtigen, sie zur Mitverantwortlung und Teilnahme aufzufordern?

Aus dem Englischen von Martina Bauer

Der vollständige Text des DPA (1998) ist zu beziehen über *www.opsi.gov.uk/ACTS/acts1998/19980029.htm*