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*