



CCTV and (In)dividuation

Heather Cameron¹

Abstract

This essay draws on work of Freud and Foucault to understand emerging converging aspects of visual surveillance and tracking technology. It discusses some of the general problems with video surveillance – due to its reliance on a flattened version of the visual realm, its partial view, and assumptions about human vision. It then moves on to show how CCTV has changed from the monitoring of flows to identifying individuals and functioning as the human interface for new databank applications, using Foucault's reflections on governmentality. The essay ends by detailing a controversial test of video surveillance and RFID tags which point out some new dangers for us to consider, and argues that we should resist the 'flat fantasy' offered by video surveillance.

Photographs and video images provide an apparently direct human interface to surveillance databases. Database records can be very detailed and useful but without photographs or video images it is much more difficult for a person to identify the target of the records. A passport number may identify a person quicker to a machine, but the photograph is the usual reference for the border patrol guard. Facial photography and video footage are preferred for human processing over other visual references like a fingerprint or iris scan. However, human matching capabilities between photos and people have been repeatedly shown to be lacking.

The work of Freud and Foucault can be used to understand emerging converging aspects of visual surveillance and tracking technology. In the following I will first discuss some of the general problems with video surveillance due to its reliance on a flattened version of the visual realm and assumptions about human vision. Second, I discuss how CCTV has changed from the monitoring of flows to identifying individuals and functioning as the human interface for new databank applications. Foucault's reflections on governmentality and producing and tracking of individuals will introduce this theme. I will end by detailing a controversial test of video surveillance and RFID tags which point out some new dangers for us to consider.

One risk with the self evidence of video surveillance is that one partial view will be taken as the True view. Even when the public has gained the media literacy to question the reliability of photographs to accurately depict a scene, video surveillance seems to have escaped this

¹ Centre for Technology and Society, Technical University of Berlin, <mailto:ameron@ztg.tu-berlin.de>

scrutiny. This may be due in part to that fact that video images appear to present a context, which is lacking in a photograph. One appears to see a chain of actions. Viewers then often infer intent or meaning to those actions without any further information being given. Video does not faithfully reproduce the world, despite its claims to do so. Video surveillance in CCTV systems differs from direct visual observation in many important ways including audio cues, three dimensionality, colour, time and frame. Video images do not tell a lasting truth, if they tell a truth at all. They identify a moment, not the depicted subject.

CCTV systems cannot identify an individual person. A CCTV operator can monitor a camera or watch a tape and attempt to identify someone from a photograph or from memory. This is more difficult than it sounds. The unreliability of people to identify someone by a photograph has led to increasing pairing up of biometric identification systems with photo or video identification systems. Rather than a photograph or video capture of the surface of the body (normally the face) as with photo identification, biometric cards are a token attached to the body itself – e.g. iris scans, fingerprints, voice prints. American prisons are using iris scans to make certain they are releasing the proper inmate after having released the wrong prisoner based on his borrowing another prisoners' identification card. This was not a forged card, but simply the authorities' mismatching of the photo on the identity card of the prisoner to be released with the (incorrect) prisoner who presented himself. This happened more than once. The US army is testing similar iris scan identification systems because a reliable photographic identification is impossible if the unknown person is cocooned in a chemical suit. Biometrics claim to be a more reliable identification method than photographs and provide another example of the drive to reduce access slippage. Anonymity is increasingly suspect and authorities and customer relationship managers are increasingly working towards more detailed information tied to particular individuals. Before networked CCTV people were more anonymous moving under the gaze of the cameras. They were being looked at but not tracked. New technology connects a person's name and database records to their body. Their anonymity is washed away revealing the ridged fingertips and spotted irises under the flat smooth surface of their image.

Photographs necessarily leave things out. Photos cut out a limited frame. They leave out the world as it is after or before their exposure. This time element is especially important as both human and computer matching capabilities decline with the increasing delay between the capture of an original identification photograph in a database (or recorded on an identification card) and the time of identification. While in theory facial geometry should not change so drastically to make the facial algorithm obsolete, tests have shown that the efficacy of facial identification software declines with the time gap between the original registration and later identifications.

Despite the marketing hype from security firms, there are even greater technical problems to reliably identify people under in field conditions who are moving and not actively co-operating with the video capture cameras. This is due to the need for bright even lighting, a specific angle of the face to the camera, and high resolution video capture to allow for a facial algorithm to be attained. If the face area captured is not large enough to create a high resolution image, i.e. if the person targeted is not close enough to the capture device, then the magnification of the facial image will distort it so that it cannot be reliably compared to a photograph in the database. There are many technical challenges to be overcome if the actual capabilities of the products in

the field are to come close to the marketing hype of the security firms. However, the problem is not solely a question of technical affordances. The greater problem is with the construction of vision and visibilities.

Theorists such as Martin Jay (1993) have drawn attention to a growing rejection of ocular centrism in continental thought. Here is not the place to detail the descent of vision as a metaphor for knowledge from the time of the Enlightenment. However, we can note that human visual perception, despite its pretensions to be objective, expels information and structures the visual field so as to make certain things visible and push others into invisibility. Deleuze draws attention to Foucault's discussion of truth regimes and how "each historical formation sees and reveals all it can within the conditions laid down for visibility, just as it says all it can within the conditions relating to statements." (Deleuze, 1988: 59) Deleuze points to the problem of how things can be opened up to sight (*ibid.*: 52-53). This is parallel to Foucault's discussions around tracing the breaks and ruptures and discontinuities that make a history. With vision the question becomes how machines "bring forth visibilities as flashes or shimmerings" (*ibid.*: 58). Our visual field is constructed and limited by the historical formation in which we find ourselves.

Freud demonstrated how our vision is influenced and constructed through unconscious beliefs and expectations. We do not see things which are in front of us and we believe ourselves to have seen things which we could not have. This slippage in human visual perception has been well documented through studies interested in eye witness testimony or criminal identification from photographs. It has repeatedly been shown that both are unreliable.

It is increasingly the case that identification from CCTV has high levels of error. Researchers in Leicester University recently completed a study confirming results from Bruce *et al.* (1999) and Kemp, Towell and Pike (1997) that there is a very low rate (15-30%) of successful identification of individuals from CCTV material (Davis and Thasen, 2000). Even close up CCTV images such as those collected from bank machines did not guarantee accurate identification. According to the Davis and Thasen study there was still a 13% error rate when the viewer had continuous access to the recording.

In part due to his awareness of the construction of the visual field, Freud drew attention to the problems and pretensions of vision in the detection of information. His therapy method of psychoanalysis seats the analyst behind and hence out of the view of the patient but within easy listening distance. This seating arrangement also releases the patient and the analyst from needing to control their faces and keeping eye contact with each other, so called 'face work'. By removing himself from the patient's view Freud argues he achieves two therapeutic effects: first, it dulls the effect of the analysand's voyeurism and second, it allows the analysand to express thoughts freely without seeing a reaction mirrored on Freud's face. Freud of course is not the first authority who wants to watch and not be watched himself. The medical inspecting gaze is turned on patients who should not look back. Freud goes on in his 'Zur Einleitung der Behandlung' to argue that despite setting up the couch and his chair this way, patients will turn to face him or otherwise resist the command not to make eye contact (472). Visual stimuli are often reduced (the analyst often works with his or her eyes closed) in psychoanalytic treatment. Freud argues that after human being evolved from moving on four legs to walking upright, vision

replaced smell as our dominant sense. Vision, accompanied by a sense of self-evidence, overwhelmed other human forms of perception and awareness, including the other senses and the unconscious to our detriment. Freud also cautions that vision is influenced by memory and what we expect to see. Because we only see what we expect to see, this misapprehension is reinforced instead of challenged and new information can only break through with great difficulty. This becomes relevant to discussions of what is actually happening when people witness events and helps to explain why eye witness testimony is so unreliable and open to suggestion.

CCTV operators are eye witnesses of a different sort as their 'witnessing' is mediated by cameras and screens. Psychoanalytic film theory draws attention to the similarity of the cinema experience and hypnosis. A cinema is usually darkened and other sensory experience minimised (i.e. reduced sound from outside, constant temperature, limited smells, comfortable seats) in order to allow the viewer to relax into an identification with the characters on the screen. Until recently the screen has only visually shown one story. CCTV operators in larger control rooms are usually confronted with a multitude of monitors which play simultaneously but do not provide any sound. With all the monitors they resemble editing suites or live broadcast trucks. Control rooms are not as dark as a cinema, but are designed to direct light to keep glare off the monitors. As a secure area, often also linked to emergency services, CCTV control rooms have stricter but similar entry controls to a commercial cinema. People are allowed into the viewing areas (control room or cinema) only with the proper id (pass or ticket).

Sometimes human fallibility is given as the reason why CCTV systems should be used as they are claimed to objectively record information. We have seen above how cameras construct the visual field. Monitoring CCTV cameras and reviewing tapes allows for human error. Everyone is vulnerable to unconscious influences that cause slips of the eye.

* * *

Governmentality (*Gouvernementalité*) is a word coined by Foucault to designate the 'conduct of conduct.' Governmentality is about how to govern: to govern oneself, to govern private relationships, to govern oneself in respect to institutions, and finally the relationship of the citizen to the state. Foucault gave a series of lectures in the late seventies and early eighties under the rubric 'The Government of one's self and others.' His lectures 'Omnes et Singulatim' (1981) explore the development of normative power and the relationships of authority by looking at the changes in the understanding of leadership from ancient Greek to modern Christian models. Ancient Greek understandings of leadership and politics were significantly different from later Judeo-Christian models. These Judeo-Christian models have evolved into the Western modern state that has in turn produced a certain type of subject and relationship to power. When examining visual surveillance it is useful to understand how certain supervisory relationships are created to exercise authority.

'Pastoral Power' is the name Foucault gives to certain forms of individuating and totalizing modern power structures, which form part of the normalizing and disciplinary society. In 'Omnes et Singulatim' Foucault identifies the introduction of the shepherd metaphor of leadership as the break between Greek and Hebraic and Christian texts. The leader modeled on

a shepherd was not at all common in Greek texts on governance, but it was the dominant metaphor in Hebraic and Christian texts. Foucault identifies five major changes from the Greek to Hebraic texts. First, the shepherd has power over a flock and not land. Second, the shepherd makes the flock, in the sense that he brings individual sheep together. Third, each sheep is individually looked after and is valuable as an individual. Fourth, the shepherd understands his rule as a duty, as a sense of devotion. This is different from the Greek texts which encourage the work in order to assure immortal glory. Fifth, the shepherd must keep watch and take care of his sheep.

The only thing a shepherd can do is keep watch over his sheep. Shepherds may sing to their flock or play them music but the verbal communication only goes one way. A model of leadership where the leader is human and the led are sheep would seem to make it impossible for the leader to fulfil her or his task of knowing details about the inner life of the followers. A metaphor which excludes dialogue between the leaders and the led then requires the leader to inspect and probe to get the necessary information rather than wait for it to be freely given.

Pastoral power was used to chart changes in power relationships in the emergence of the modern state, not describe the use of CCTV. However we can see how the general tendency mirrors relationships of control with surveillance technologies and it is useful to explore Deleuze's critique of pastoral power. Deleuze refers to pastoral power in his 'Postscript on Societies of Control' (1992) explaining how it is no longer useful to speak of individuals or numbers but of 'dividuals' and codes. Our society has moved from focusing on interiority and depth and the ability to lay bare that depth, to prioritising the surface and scanning. Dividuals are understood to be composites of various codes and group identifiers which can be structured and localized based on a particular piece of structuring information e.g. the postal code which indicates where one lives. At another time another piece of information may be the structuring factor. Societies of Control are not interested as much in the soul or what sins people have committed, but in behaviour and what future actions can be predicted. Deleuze shows how the processing of the internalized information has changed from confession to a priest to having your face or identity cards scanned for risk assessment as you pass unknowingly by.

For our purposes it is interesting to think about actors in addition to the state who are interested in turning undifferentiated groups into individuals with internalized values and then back into more manageable groups. For example private security, but increasingly the retail sector, are experimenting with a range of technologies to deepen and also quicken their knowledge of their existing and potential customers. There is also a lot of cross over from corporate to state functions (as far as this distinction still makes sense) including the application of Customer Relationship Management (CRM) techniques to 'fighting terrorists'.

Immediately after the events of 9/11 the CRM industry began to lobby for opportunities to sell their services to the government as a way of fighting terror. On 26th of February 2002, CRM industry executives including Tom Siebel of Siebel Systems Inc. appeared before the US House Subcommittee on Technology and Procurement Policy of the House Committee on Government Reform. He explained to legislators how publicly available information on one of the 9/11 suspects could have been brought together through CRM systems to build a composite picture

which would have caught the attention of law enforcement. As it was, different government agencies each knew something about the 9/11 suspect but each discrete piece did not in itself arouse suspicion and there was no way to link all the pieces up. The CRM executives argued that the data mining and warehousing techniques used to build composite pictures of customers from discrete bits of data to sell them more products and services, can be used to connect bits of information about individuals to find patterns which are claimed to constitute terrorist activity. The PATRIOT Act (2001) increased dramatically the ability of the US government to access databases of US Firms in order to gather information in the name of fighting terrorism. The PATRIOT Act has raised grave concerns about misuse, mistakes and privacy invasion. CRM shares pastoral power's focus on visual control, individuation, tracking and 'care'.

* * *

CCTV's capabilities have changed since its deployment in traffic and transit control. Rather than low resolution stationary cameras high on a concrete mast with a rudimentary zoom function which observed traffic flows, portable cameras now can be made to track moving objects in all light situations. Rather than monitoring an entire highway, CCTV systems are used to identify individual cars' license plates. Rather than taping a casino as insurance against staff or customer fraud, systems at the entrance can now scan for individual people unwelcome on the premises. Rather than watch an entire warehouse, CCTV can be used with other systems to track individual pallets of goods, and controversially single units of goods, like a package of razors. In this way the development of CCTV as a surveillance technology fits into the model of power offered by Foucault and improved by Deleuze of dividing groups into measurable units and then reassembling them for various purposes.

As it becomes possible to target smaller and smaller units – from rush hour to the individual car, from an entire casino to an individual player or from a warehouse to a pallet – more detailed sorting actions can be taken. However, as CCTV begins to play a role as the human interface to data systems some of its earlier functions have become untenable.

Public CCTV is rarely used by police to immediately react to crime but to prosecute and predict it. The point was repeatedly made by UK police officers at the Urbaneye expert conference that police officers had other priorities than reacting to CCTV nuisance calls for antisocial behaviour. The huge number of cameras in the UK and the broadcasting of these images on television have made petty crime and antisocial behaviour visible to the public who have expected those in authority to take action. This behaviour was not new. That the behaviour was recorded and broadcast made it impossible to ignore. Theorists such as Virilio refer to the speed of the image and the immediate forgetting that happens when one is overwhelmed by visual information. The CCTV image makes itself unforgettable through its constant replaying and archiving. Since the police cannot and will not spend their resources this way CCTV required an outsourcing to private security and monitoring firms who then had an interest in the expansion of their business.

Police use of CCTV is focussed on evidence collection after the fact, not just to investigate crimes depicted on the tape but to collect clues for other crimes committed in the area -- for example suspects arriving and parking their car or other movements linked to another

neighbouring crime. While the police are using CCTV increasingly after the fact, other actors are exploring how CCTV links into a system of predictive or preventative actions way beyond the established practice of making a video camera visible for deterrence.

The future of CCTV is mobile. Rather than erecting concrete masts and building cameras into fixed spots in the city, cameras will be deployed in hot spots with a clear task and then redeployed somewhere else when their task is completed. Critics have long argued that CCTV simply displaces crime. Mobile camera installations will allow the authorities to more actively pursue it.

One of the most talked about examples of predictive use of CCTV was the 'smart shelf' from Gillette that made headlines in the UK in 2003 when it was tested at Tesco. The Gillette smart shelf links a video camera to RFID (radio frequency identification) tags, floor sensors, PDAs in the hands of store detectives and monitors at checkout. RFID tags were put on the packaging on individual packages of Gillette razors which are small and expensive and therefore a target for shoplifters. In Tesco the packages with their radio tags were displayed on a so called smart shelf. If a customer removed a package of razors from the smart shelf the system would detect this through a proximity detector linked to the RFID chip and covertly take a photograph of the person. A photograph of the suspect would be sent to the PDA device of store detectives. On the way to the checkout the suspect's position could be tracked through the RFID tags on the razors by sensors on the floor and relayed to store detectives. If the person went to the checkout with the razors then another photo was taken for comparison and then the person was removed from the active list on the system. Otherwise, the person could be tracked through the store and observed to see if he or she tried to leave the premises without paying. This case aroused the interest and condemnation of many privacy groups due to the issues involved: covert surveillance, assumption of guilt and not to mention the future threat of further tracking outside the store. Activists feared that more advanced technology would expand the interrogation range of the tags now measured in centimeters to a distance that would allow the tracking of individual persons. Like cellular phones, some people are worried about the use of these chips as location devices. Natural scientists have long used RFID chips to track animals in the wild and even bees. People 'chip' their pets and Japanese school administrators in Osaka started a pilot project in the summer of 2004 to track school children's comings and goings through RFID chips in their backpacks and readers posted at the school gates.

RFID tags represent a move towards smaller and smaller units of tracking. These tags are also programmed with certain information which can be particular to each tag. As Foucault's flock was broken into individual trackable and predictable sheep and then regrouped at will, the development of these tags opens the possibility of a more detailed and intimate control. This makes Deleuze's point that the current historical framework is not interested in unique individuals confessing their truth but connected units being scanned for their code. Consumer research is interested in your deeply held beliefs, only so far as they predict your buying patterns or susceptibility to marketing campaigns. By tracking consumer behaviours stores hope to become better at tailoring their services and products to affluent consumers. Stores do not need to care what customers believe as long as they continue to consume their products. Customer information is irrelevant if it does not have an effect on purchasing behaviour.

We return again to the storage and classification of information: the ever-expanding database of personal details, some significant, some apparently insignificant until they are pooled together and tracked over time. The tracking of these moments into pools of data provide the environment for analysts to punch out their patterns, to reduce individual potential and difference to uniform groups predictable, governable and susceptible to selling. David Lyon refers to social sorting to describe the “classifying drive” of contemporary surveillance (Lyon, 2002: 14). The use of surveillance to classify and sort populations in order to target them for different treatment poses a different threat to that which can be sufficiently regulated by privacy legislation. The challenge is increasingly to confront different types of discrimination which may not even be immediately visible in its effects but influence how people can participate in public life.

Surveillance technologies can be, and are, resisted or defeated. RFID can be defeated by technology: shoplifters use specially shielded bags for example, or one could become a personal jamming station broadcasting at an intensity that would swamp the relatively weak signals of the RFID chips. Alas these are zero sum games. We can rest assured that further encryption and bans on jamming and blocker bags will come about forcing new levels of creativity in those trying to disrupt the technology.

This escalating spy vs. spy behaviour links us back to Foucault and his question coming out of his analysis of pastoral power: how can the growth of capabilities be disconnected from the growth of power relations? (Foucault 1984b: 48) Does offering technological solutions (privacy enhancing devices, counter surveillance techniques) to the problems of surveillance simply deepen our subjection? Choosing to address the problems of surveillance through technological fixes opens up some strategic options and shuts down others. This is also the case for looking at surveillance as a problem for privacy law or human rights. Each approach focuses in on a few elements, distorts others and pushes still others into invisibility outside its frame. In all of this we have to resist our own susceptibility to believe what we see and be seduced by our eyes into a flat fantasy.

References

- Baudelaire, C. (1964) *The Painter of Modern Life, and Other Essays* (trans. and ed. J. Mayne). London: Phaidon Press.
- Bruce, V. (1998) ‘Fleeting images of shade: Identifying people caught on video’, *The Psychologist* 11: 331-338.
- Davies, G. and S. Thasen (2000) ‘Closed-circuit television: How effective an identification aid?’ *British Journal of Psychology*, 91: 411-426.
- Dean, T. (2001) *Beyond Sexuality*. Chicago: University of Chicago Press.
- Dean, T and C. Lane (2001) *Homosexuality and Psychoanalysis*. Chicago: University of Chicago Press.
- Deleuze, G (1988) *Foucault*. (trans. S. Hand). Minneapolis: University of Minnesota Press.
- Deleuze, G (1992) ‘Postscript to Societies of Control’, *October*, 59: 3-7.

- Fischkin and Roy (2003) 'Enhancing RFID Privacy via Antenna Energy Analysis'. Paper presented to MIT RFID Privacy Workshop, 15 November. <http://www.rfidprivacy.org/agenda.php> [accessed 5 January, 2004].
- Foucault, M. (1981) "'Omnes et Singulatim": towards a critique of political reason'. *The Tanner Lectures on Human Values II*. Salt Lake City: University of Utah Press. 224–254.
- Foucault, M. (1984) 'What is Enlightenment: Was ist Aufklärung?' unpublished ms., (trans. C. Porter) in P. Rabinow (ed.), *The Foucault Reader*. New York: Pantheon.
- Foucault, M. (1991) 'Questions of Method', in *The Foucault Effect: Studies in Governmentality*. Burchell, Gordon, Miller (eds.) Chicago: University of Chicago Press.
- Freud, S. (1999) *Gesammelte Werke: Werke aus den Jahren 1909-1913*, Frankfurt: Fischer Verlag
- Jay, M. (1993) *Downcast Eyes: The Denigration of Vision in Twentieth Century French Thought*. Berkeley: University of California.
- Kemp, R., N. Towell, and G. Pike, (1997) 'When seeing should not be believing: photographs, credit cards and fraud', *Applied Cognitive Psychology* 11: 211-22.
- Lyon, David. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.
- Monahan, T. (2004) 'Counter Surveillance as Political Intervention?' Paper Presented to CCTV and Social Control conference, University of Sheffield, UK, 8-9 January 2004.